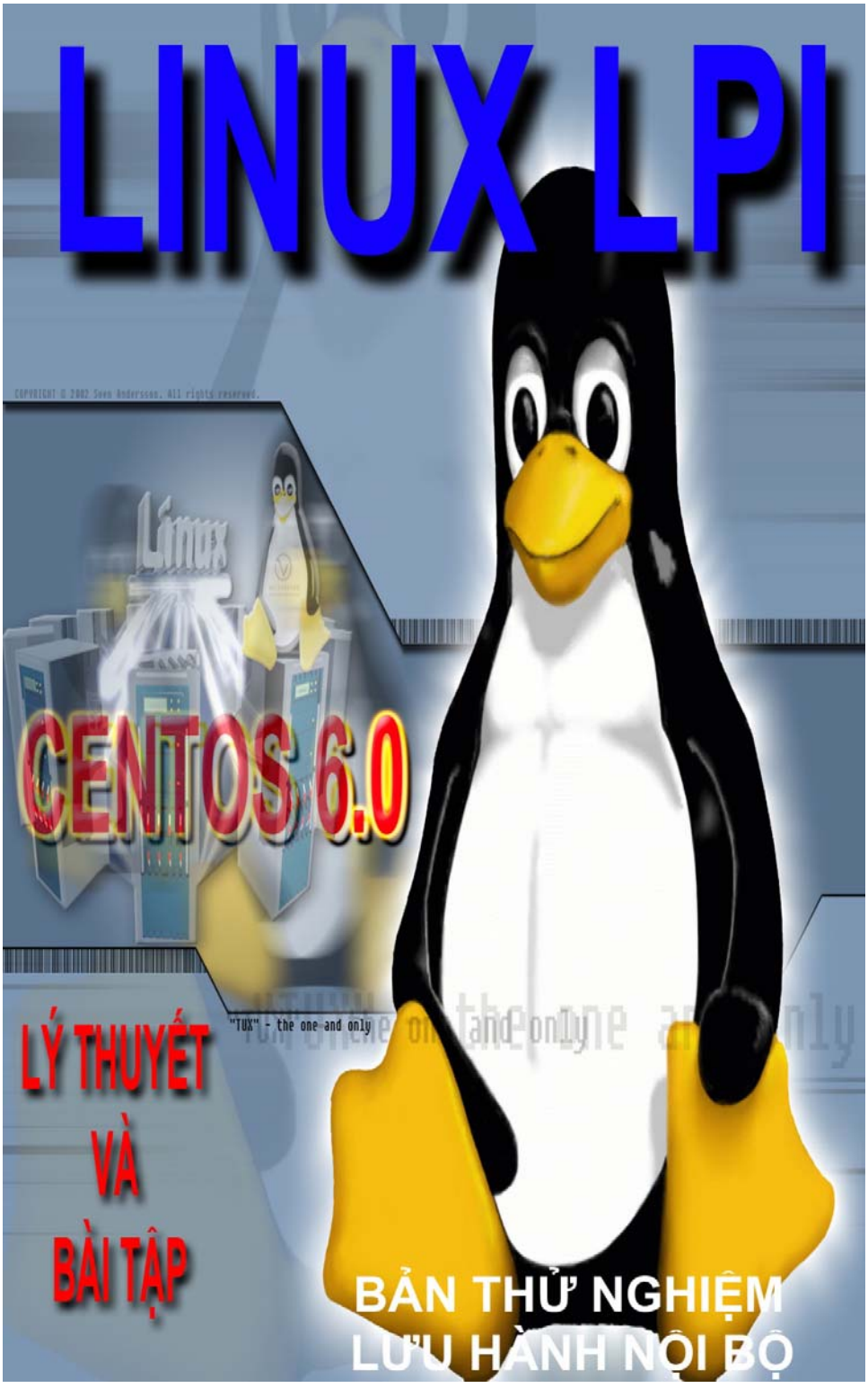
LINUX LPI


CENTOS 6.0
LÝ THUYẾT
VÀ
BÀI TẬP
"TUX" - the one and only
BẢN THỬ NGHIỆM
LƯU HÀNH NỘI BỘ

CHƯƠNG 1: GIỚI THIỆU CHUNG VỀ UNIX/LINUX

Nội dung:

- ❖ Lịch sử ra đời và phát triển của hệ điều hành Linux
- ❖ Vấn đề bản quyền và luật bản quyền phần mềm mã nguồn mở
- ❖ Các bản phân phối của Linux

TÓM TẮT

- Phần 1.1: Giới thiệu sơ lược về sự ra đời của hệ điều hành Unix/Linux.
- Phần 1.2:Trình bày tổng quan về giấy phép mã nguồn mở GPL.
- Phần 1.3: Giới thiệu tóm tắt các bản phân phối của hệ diều hành Linux gồm: Ubuntu, CentOS, Fedora core, Debian, Suse và Red Hat Enterprise.

1.1. LỊCH SỬ PHÁT TRIỂN CỦA UNIX/LINUX

Giữa năm 1960, AT&T Bell Laboratories và một số số trung tâm khác thực hiện dụ án Multics (Multiplexed Information and Computing Service). Sau một thời gian thực hiện, dự án tỏ ra không khả thi. Tuy vậy Ken Thompson, Dennis Ritchie … thuộc Bell Labs đã không bỏ cuộc. Thay vì xây dựng một HĐH làm nhiều việc một lúc như Multics, họ quyết định phát triển một HĐH đơn giản chỉ làm tốt một việc là chạy chương trình (run program). Peter Neumann đặt tên cho HĐH "đơn giản"này là Unix

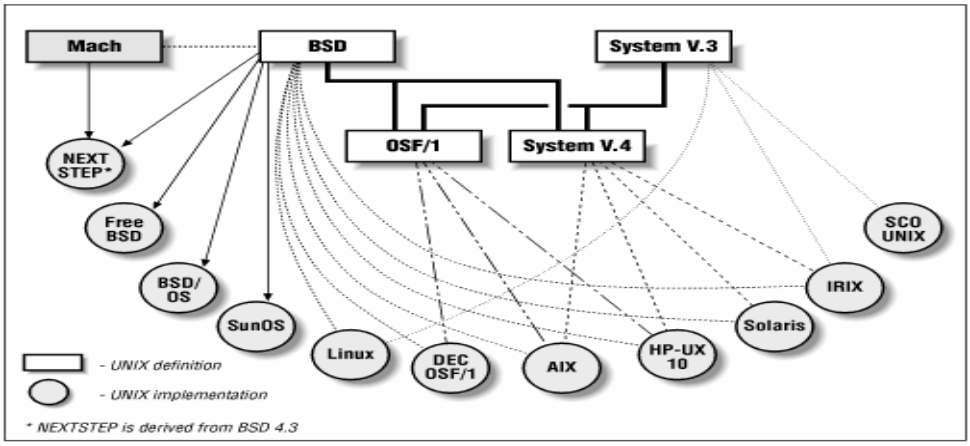
Khoảng 1977 bản quyền của UNIX được giải phóng và HĐH UNIX trở thành một thương phẩm. Hai dòng UNIX: System V của AT&T, Novell và Berkeley Software Distribution (BSD) của Đại học Berkeley.

Sau đó IEEE đã thiết lập chuẩn "An Industry-Recognized Operating Systems Interface Standard based on the UNIX Operating System." Kết quả cho ra đời POSIX.1 (cho giao diện C) và POSIX.2 (cho hệ thống lệnh trên Unix)

Năm 1991 Linus Torvalds bắt đầu xem xét Minix, một phiên bản của Unix với mục đích nghiên cứu cách tạo ra một hệ điều hành Unix chạy trên máy PC với bộ vi xử lý Intel 80386. Ngày 25/8/1991, Linus cho ra version 0.01 và thông báo trên comp.os.minix của Internet về dự định của mình về Linux. Vào tháng 1/1992, Linus cho ra version 0.12 với shell và C compiler. Linus không cần Minix nữa để recompile HDH của mình. Linus đặt tên HDH của mình là Linux. Năm 1994, phiên bản chính thức 1.0 được phát hành.

Linux là một HDH dạng UNIX (Unix-like Operating System) chạy trên PC với CPU Intel 80386 trở lên, hay các bộ vi xử lý trung tâm tương thích AMD, Cyrix. Linux ngày nay còn có thể chạy trên các máy Macintosh hoặc SUN Sparc. Linux thỏa mãn chuẩn POSIX.1.

Quá trình phát triển của Linux được tăng tốc bởi sự giúp đỡ của dự án GNU (GNU's Not Unix), đó là chương trình phát triển các Unix có khả năng chạy trên nhiều platform. Đến cuối 2001, phiên bản mới nhất của Linux kernel là 2.4.2-2, có khả năng điều khiển các máy đa bộ vi xử lý và rất nhiều các tính năng khác.



Hình 1.1 Sự hình thành và phát triển của HĐH Linux

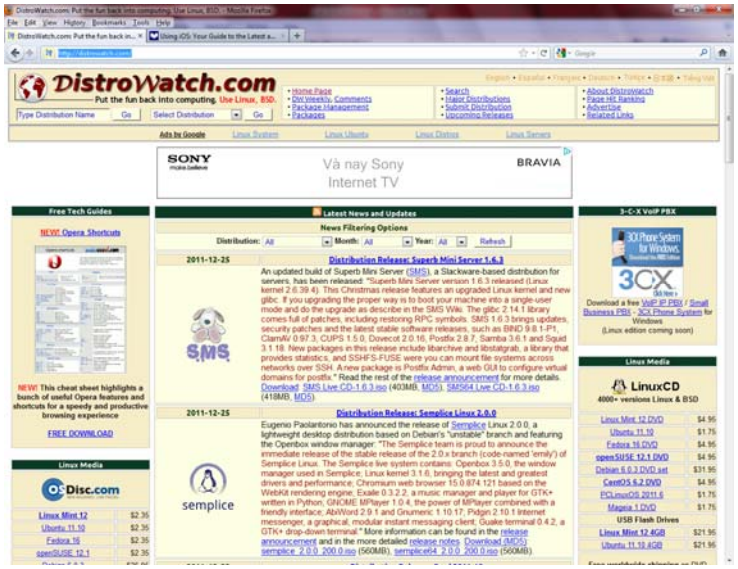
1.2. MÃ NGUỒN MỞ VÀ GPL

Các chương trình tuân theo GNU Copyleft or GPL (General Public License) có bản quyền như sau:

- Tác giả vẫn là sở hữu của chương trình của mình.
- Ai cũng được quyền bán copy của chương trình với giá bất kỳ mà không phải trả cho tác giả ban đầu.
- Người sở hữu chương trình tạo điều kiện cho người khác sao chép chương trình nguồn để phát triển tiếp chương trình

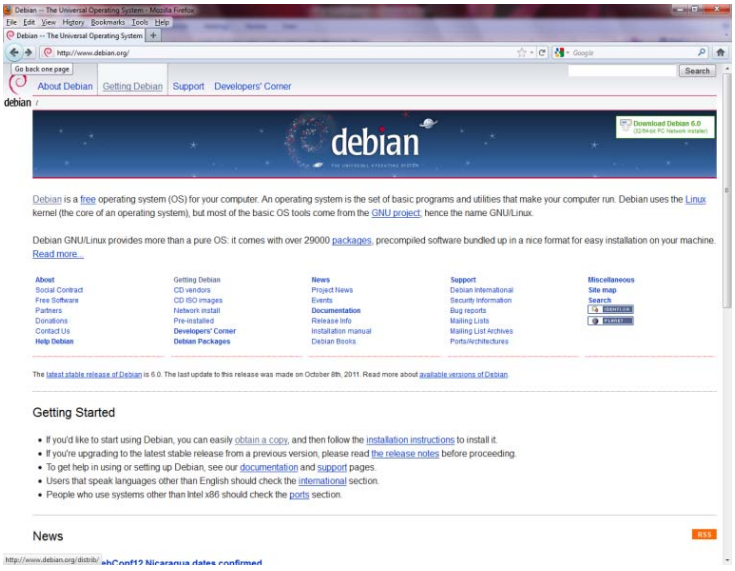
1.3. CÁC BẢN PHÂN PHỐI CỦA LINUX

Các phiên bản của HDH Linux được xác định bởi hệ thống số dạng X.YY.ZZ. Nếu YY là số chẵn, phiên bản ổn định. Nếu YY là số lẻ, phiên bản thử nghiệm. Các phân phối (distribution) của Linux quen biết là RedHat, Debian, SUSE, Slakware, Caldera,Ubuntu… Địa chỉ website giới thiệu các bản phân phối Linux: http://distrowatch.com/

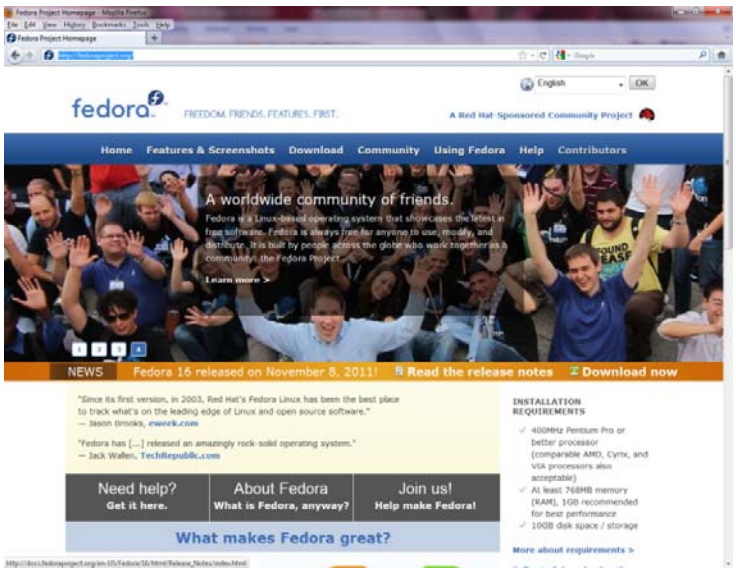


- DEBIAN: do dự án Debian xây dựng, là bản phân phối phần mềm tự do với sự cộng tác của các trình nguyện viên trên khắp thế giới. Kể từ lúc bắt đầu đến nay, hệ thống chính thức phát hành với tên gọi Debian GNU/Linux được xây dựng dựa trên nhân Linux với nhiều công cụ cơ bản của hệ điều hành lấy từ dự án GNU.

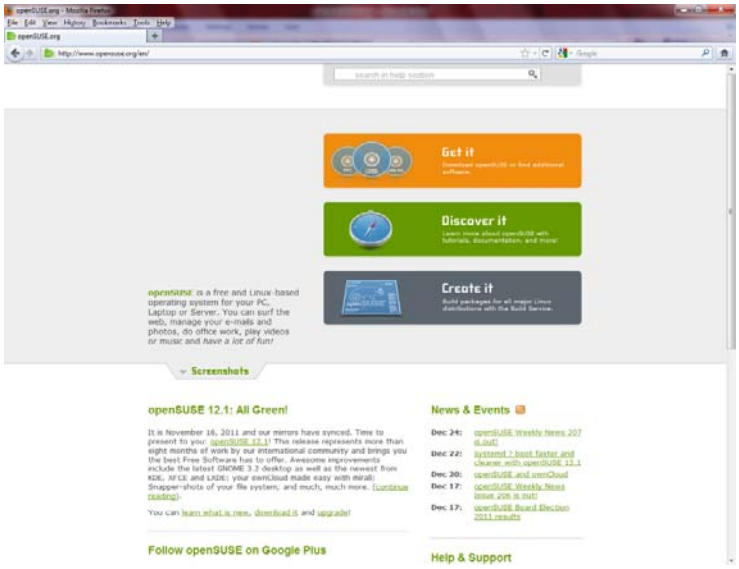
  Debian có tiếng về mối kết gắn chặc chẽ với triết lý Unix và phần mềm tự do. Nó cũng có tiếng về sự phong phú cho các chọn lựa, phiên bản phát hành hiện tại có hơn 15,490 gói phần mềm cho 11 kiến trúc máy tính, từ kiến trúc ARM thường gặp ở các hệ thống nhúng và kiến trúc mainframe s390 của IBM cho đến các kiến trúc thường gặp trên máy tính cá nhân hiện đại như x86 và PowerPC. Địa chỉ website: http://www.debian.org/



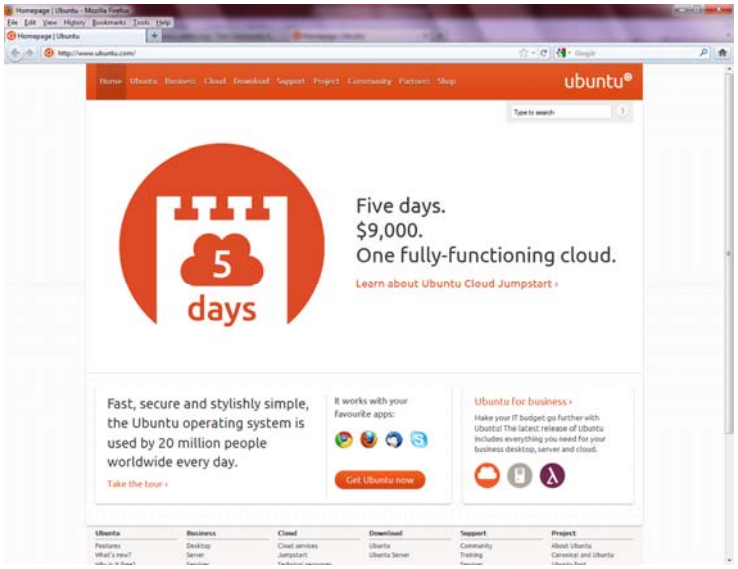
- FEDORA CORE: là một bản phân phối của Linux dựa trên RPM Package Manager, được phát triển dựa trên cộng đồng theo "Dự án Fedora (Fedora Project)" và được bảo trợ bởi RedHat. Dự án Fedora nhằm tới mục đích tạo ra một hệ điều hành mã nguồn mở hoàn chỉnh để sử dụng cho các mục dích tổng quát. Fedora được thiết kế để có thể dễ dàng cài đặt với chương trình cài đặt mang giao diện đồ họa. Các gói phần mềm bổ sung có thể tải xuống và cài đặt một cách dễ dàng với công cụ YUM. Các phiên bản mới hơn của Fedora có thể được phát hành 6 đến 9 tháng. Phiên bản hiện tại của Fedora là 16http://fedoraproject.org/



- SUSE: do hãng Nowel phát triển. SuSE có các phiên bản chính như: SuSE Linux Enterprise Server, openSuSE. Trong số các phiên bản trên, phiên bản x86-64 bit, PPC, IA64. Kiến trúc x86 bao gồm các loại bộ xử lý: Intel Pentum 1-4, Celeron, 32bit Xeon, Celeron D, AMD K6, Duỏn, Athlon, Athlon XP, Athlon MP, Sempron. Kiến trúc x86-64 bit bao gồm các bộ vi sử lý như: AMD Xeon, Xeon MP, Pentum 4 Extreme Edition, pentum D, processors based on AMD's AMD 64 & intel's EM64T.Có thể tham khảo các thông tin về OpenSuSE tại địa chỉ: http://www.opensuse.org.

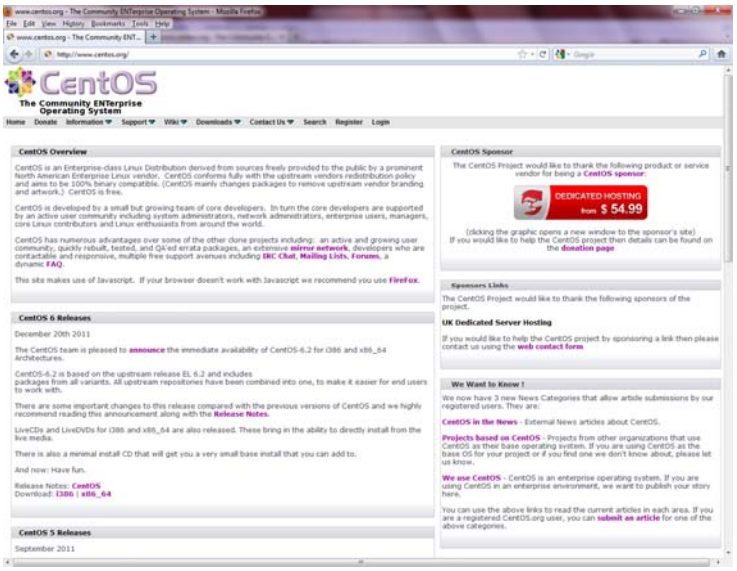


- UBUNTU: là bản phân phối của Linux chủ yếu dành cho máy tính để bàn dựa trên Debian GNU/Linux.Nó được tài trợ bởi Canonical LTD, tên của bản phân phối bắt nguồn từ quan niệm "ubuntu" của Nam Phi. Ubuntu hướng đến chỉ việc chỉ dùng phần mềm cho người dùng trung bình. Ubuntu có một cộng đồng người dùng năng động. Địa chỉ website: http://www.ubuntu.com/



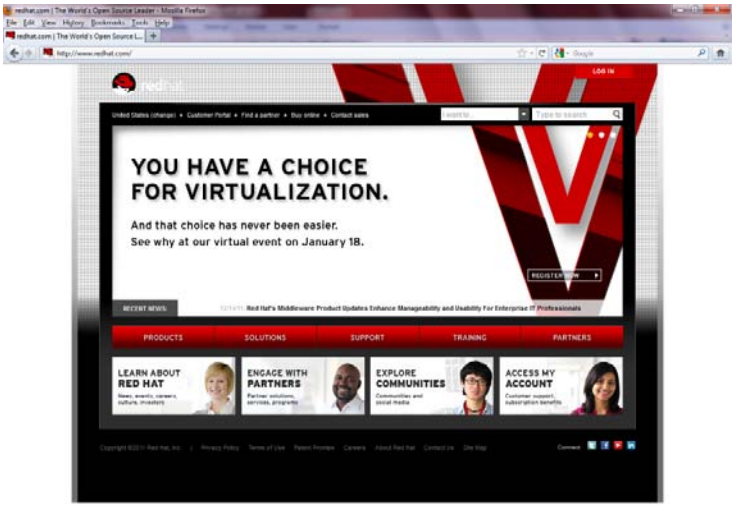
- CENTOS: Comminity Enterprise Operating System là bản được xây dựng dựa trên nền tảng của Red Hat Enterprise Linux, hỗ trợ dòng x86 (i586 và i386), dòng x86-64 (AMD64 và Intel EMT64), các cấu trúc IA64, Alpha, S390 và S390x. CentOS

chủ yếu cung cấp cho dòng server chuyên dụng, hiện nay CentOS cung cấp phiên bản 6.0http://www.centos.org/



- RED HAT ENTERPRISE: thường được gọi tắt là RHEL là một bản phân phối Linux mang tính thương mạii của RedHat. Mỗi phiên bản RHEL sẽ Redhat hỗ trợ trong vòng 7 năm kể từ ngày phát hành đầu tiên. Các phiên bản mới của RHEL sẽ xuất hiện sau mỗi 18 tháng. Hiện nay RedHat đã có phiên bản 6:
    - RHEL AS: dành cho các hệ thống lớn
    - RHEL ES: dành cho các hệ thống trung bình
    - RHEL ws: dành cho người dùng các nhân có nhu cầu cao
    - RHEL Desktop: dành cho người dùng cá nhân có nhu cầu thấp

Địa chỉ website:http://www.redhat.com/



1.4. CÂU HỎI ÔN TẬP

1. Trình bày tóm tắt quá trình phát triển của hệ điều hành Linux
2. Hãy cho biết sự giống và khác nhau giữa Linux và Unix
3. Anh chị hãy cho biết ưu, khuyết điểm của hệ điều hành Linux
4. Anh (chị) hãy cho biết các luật bản quyền được sử dụng trong thế giới mã nguồn mở ? So sánh các điểm giống và khác nhau giữa các luật đó ?
5. Anh (chị) hãy trình bày điểm khác biết giữa các bản phân phối của Linux ?
6. Anh (chị) hãy trình bày vai trò của hệ điều hành Linux trong thời đại ngày nay ?

CHƯƠNG 2: CÀI ĐẶT LINUX CENTOS6.0

Nội dung:

- ❖ Các bước cài đặt hệ điều hành Linux
- ❖ Phân chia partation ổ cứng cài Linux
- ❖ Trình khởi động Bootloader
- ❖ Quá trình đóng tắt và khởi động hệ thống Linux
- ❖ Cài đặt Linux chung với các hệ điều hành khác trên một máy.
- ❖ Sử dụng RPM
- ❖ Cài đặt phần mềm từ file nguồn
- ❖ Quản lý phần mềm bằng yum

TÓM TẮT

- Phần 2.1 giới thiệu các đặc điểm chính của bản phân phối hệ điều hành Linux CentOS6.0, giới thiệu các yêu cầu phần cứng tối thiểu chuẩn bị trước khi cài đặt hệ điều hành, và cách chia các partation cần thiết cho cài đặt Linux.
- Phần 2.2 giới thiệu các bước cài đặt bản phân phối Linux CentOS6.0.
- Phần 2.3 giới thiệu và hướng dẫn cách cài đặt phần mềm trên Linux bằng trình quản lý phần mềm RPM và trình tiện ích YUM.

2.1. CÀI ĐẶT LINUX CENTOS SERVER

2.1.1. GIỚI THIỆU CENTOS 6.0

Được công bố chính thức năm 2011. CentOS cung cấp một số đặc điểm sau:

- Cung cấp giao diện GNOME 2.20 bao gồm các chương trình thông dụng như Evolution mail client, có thể xem file đính kèm dạng pdf, cùng một số tính năng nâng cao khác.
- Giao diện KDE 3.5.8 cùng với các tính năng multimedia, đọc DVD đa dạng.
- Cung cấp giao diện quản lý mạng NetworkManager 0.7 hỗ trợ tính năng quản lý và thiết bị mạng không dây.
- Cấp chương trình PulseAudio là một chương trình quản lý sound card hiệu quả và có thể tương thích với hầu hết các hệ thống sound mới. Cùng với chương trình giải mã CodecBuddy có thể hỗ trợ thêm cho các chương trình nghe nhạc.
- Cung cấo ứng dụng văn phòng OpenOffice.org 3 với nhiều tính năng mới.
- Tích hợp thêm bộ nhận dạng cho các thiết bị Bluetooth.

- Hỗ trợ cho laptop bộ xử lý theo kiến trúc x86 và x86-64.
- CentOS sử dụng kernel phiên bản 2.6.25

2.1.2. YÊU CẦU PHẦN CỨNG:

- CPU 386 trở lên, BUS ISA,PCI,EISA
- Keyboard:US English 105 key. Hoặc các loại khác
- Mouse type
- Hard disk size: Nên có tối thiểu 1.8 GB song khuyến cáo nên có 3,5 GB
- RAM –tối thiểu 64M (RedHat 7.2) chọn Dùng thêm SWAP file nhờ một bộ nhớ ảo (Gấp đôi RAM value).
- Tuy vậy đối với những Kernel mới (2.6x) trở lên ta nên sử dụng cấu hình mạnh hơn như HDD tối thiểu 5GB, RAM 256 M.
- Lưu ý dung lượng SWAP (không gian hoán đổi bộ nhớ) cần hai lần lớn hơn dung lượng RAM.

2.1.3. PHÂN VÙNG ĐĨA CỨNG

Đĩa cứng được phân ra nhiều vùng khác nhau gọi là Partition. Mỗi partition sử dụng một hệ thống tập tin và lưu trữ dữ liệu. Các phân vùng cần thiết để cài đặt Linux.

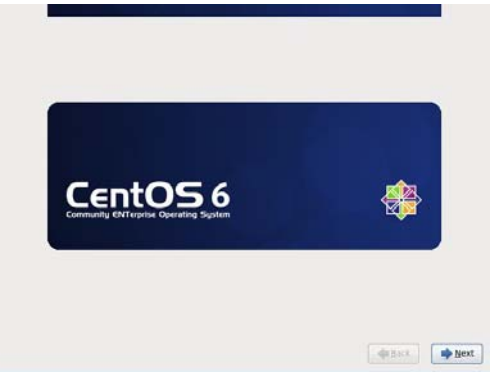
- Phân vùng / là phân vùng chính chứa các thư mục gốc của hệ thống.
- Phân vùng /boot chứa các boot loader, boot image của hệ điều hành.
- Phân vùng swap được dùng làm không gian hoán đổi dữ liệu khi phân vùng nhớ chính được sử dụng hết. Kích thước của phân vùng swap sử dụng tùy thuộc hệ thống mình sử dụng ít hay nhiều ứng dụng. Kích thước vùng swap được khuyến khích lớn hơn hay bằng dung lượng RAM.

2.2. CÁC BƯỚC CÀI ĐẶT

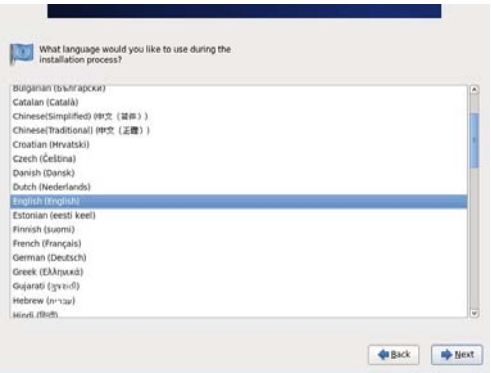
Khởi tạo cài đặt: chương trình hướng dẫn cài đặt trực tiếp từ CDROMcài đặt:

Chọn Skip trong hộp thoại Disk Found, để không kiểm đĩa CDROM trước khi cài đặt, sau đó hệ thống sẽ nạp chương trình anaconda để vào chết độ đồ họa.

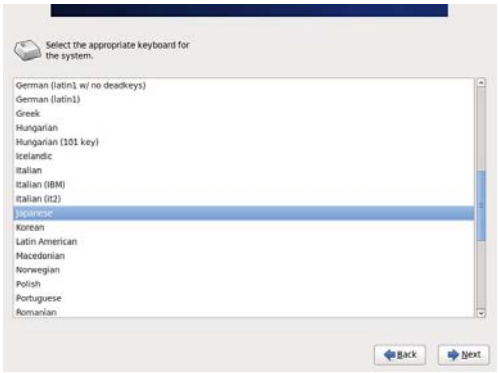
Click Next để tiếp tục



Chọn Next để qua bước kế tiếp. Chọn ngôn ngữ English làm ngôn ngữ hiển thị trong quá trình cài đặt, có thể chọn ngôn ngữ tiếng việt, chọn Next để tiếp tục bước kế tiếp:



Chọn kiểu Keyboard, nhấn Next để tiếp tục

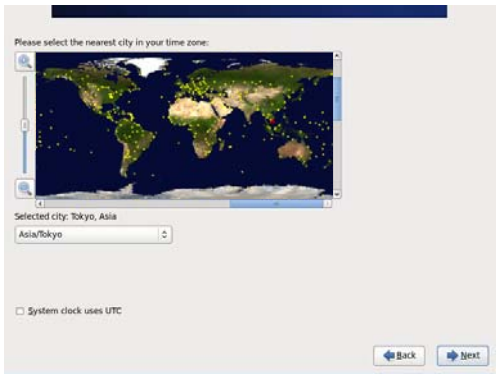


Chọn “"Basic Storage Devices”

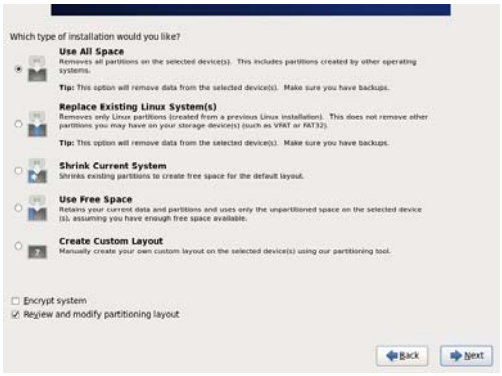
Click chọn “Re-initialize all”, nhân next để tiếp tục

Đặt Hostname cho máy tính

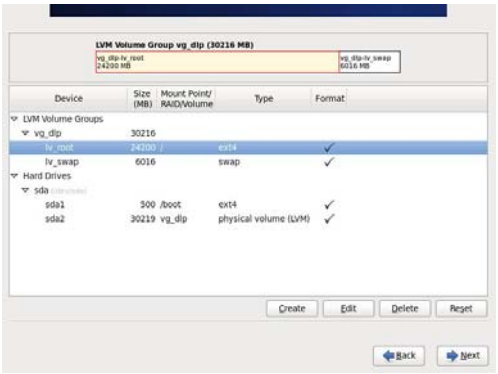
Chọn timezone



Chọn phương thức tổ chức Partition, chọn “create custom layout” nếu muốn tự tạo phân vùng, chọn Next để tiếp tục

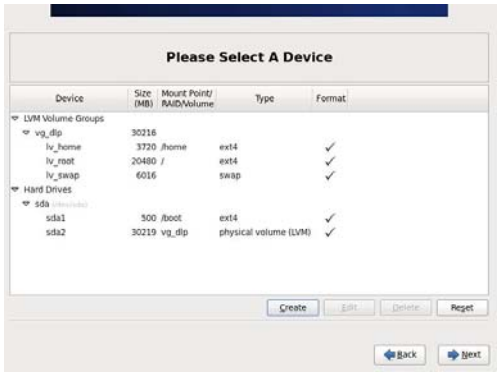


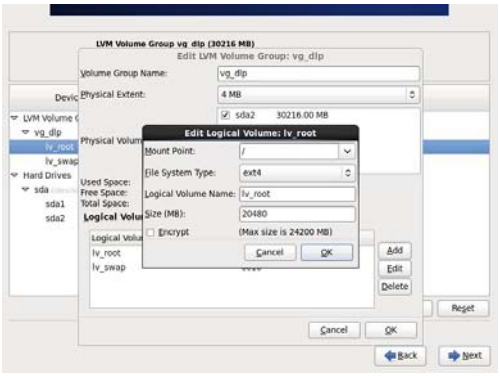
Chọn New để tạo phân vùng mới, ta cần tạo bốn phân vùng, phân vùng /, phân vùng /boot, phân vùng swap, phân vùng /home



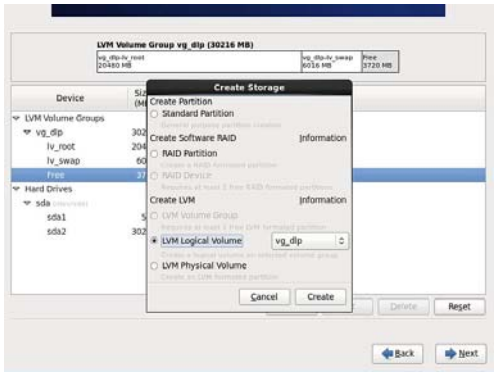
- Tạo phân vùng /boot với kích thước là 500MB, Mount Point ext4.
- Tạo phân vùng / với Mout Point là ext4, size là 20480MB.
- Tạo Swap 6000MB.
- Tạo phân vùng /home với kích thước khoảng 3700MB, mount point ext3.

Tạo phân vùng /boot với kích thước là 500MB, Mount Point ext4.

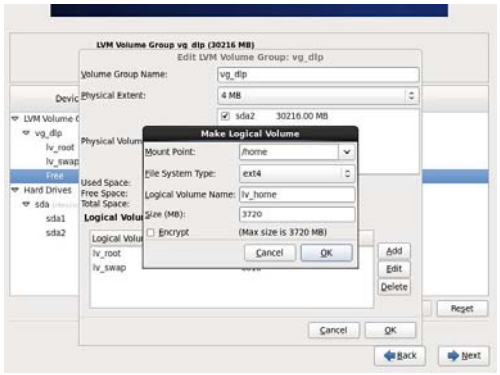




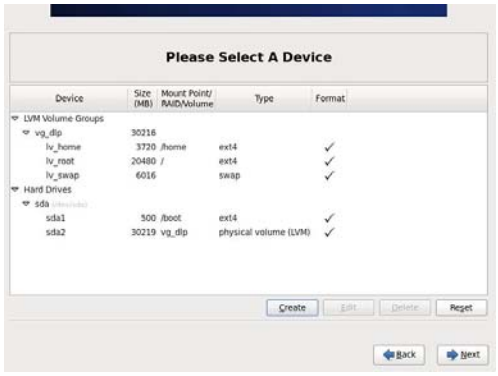
Click nút "Create" , Select "LVM Logical Volume" và Click "Create”



Tạo phần vùng /home



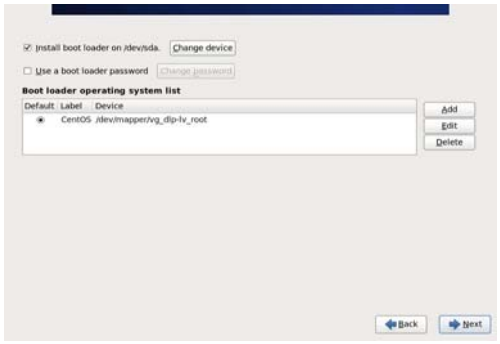
Sau khi tạo xong các phân vùng nhấn next để tiếp tục



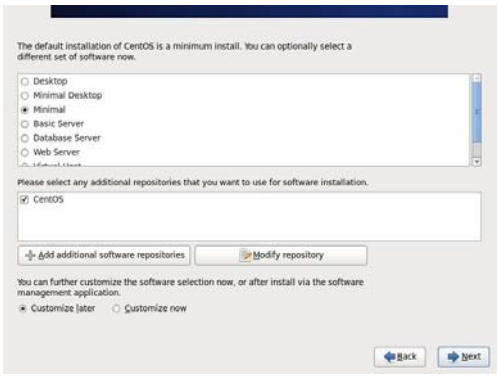
Clieck “Format” để định dạng ổ đĩa

Click 'Write Changes to Disk'

Chọn Next để tiếp tục. Chọn cài đặt Grub boot loader để quản lý boot loader hệ thống chọn Next để tiếp tục:

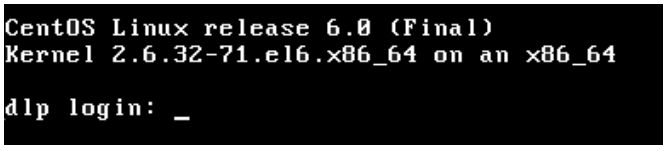


Lực chọn phần mềm để cài đặt. Select 'Minimal' và tiếp tục.



Quá trình cài đặt diễn ra trong vài phút.

Quá trình cài đặt hoàn tất nhấn nút “reboot” để khởi động hệ thống



2.3. CÀI ĐẶT PHẦN MỀM

2.3.1. QUẢN LÝ PHẦN MỀM RPM

RedHat Package Manager (RPM) là hệ thống quản lý package (gói phần mềm) được Linux hỗ trợ cho người dùng. RPM có một cơ sở dữ liệu chứa các thông tin của các package đã cài và các tập tin của chúng. Nhờ vậy, RPM cho phéptruy vấn các thông tin, cũng như xác thực các package trong hệ thống.

Trong quá trình nâng cấp package, RPM thao tác trên tập tin cấu hình rất cẩn thận, do vậy màkhông bao giờ bị mất các lựa chọn trước đó của mình. Trên phương diện các nhà phát triển, nó cho phép đóng gói chương trình nguồn của phần mềm thành các package dạng nguồn hoặc binary đưa tới người dùng.

2.3.2. CÀI ĐẶT PHẦN MỀM BẰNG RPM

Package RPM thường chứa các tập tin có dạng giống như "foo-1.0-1.i386.rpm". Tên tập tin này bao gồm tên package (foo), phiên bản (1.0), số hiệu phiên bản (1), kiến trúc sử dụng (i386).

- Cú pháp: # rpm –ivh tên-tập-tinRPM
- Ví dụ 2.3.1: #rmp –ivh foo-1.0-1.i386.rpm

  foo package foo-1.0-1 is already installed

Nếu muốn cài chồng lên package đã cài rồi dùng lệnh thêm tham số --replacepkgs

#rpm –ivh –—replacepkgs tên-tập-tin-package

- Ví dụ 2.3.2:# rpm -ivh --replacepkgs foo-1.0-1.i386.rpm

2.3.3. TRUY VẤN CÁC PHẦN MỀM

- Cú pháp:# rpm -q tên-package
- Ví dụ 2.3.3*:* # rpm -q sendmail

  sendmail.8-11.1

Thay vì xác định tên package,có thể sử dụng thêm một số tham số khác kết hợp với -q để xác định package màmuốn truy vấn.

-a	Truy vấn tất cả các package.
-f tập-tin	Truy vấn những package chứa tập-tin. Khi xác định tập tinphải chỉ rõ đường dẫn (ví dụ: /usr/bin/ls)
-p tên-tập-tin-package	Truy vấn package tên-tập-tin-package

-i	Xác định các thông tin về package bao gồm: tên, mô tả, phiên bản, kích thước, ngày tạo, ngày cài đặt, nhà sản xuất
-l	Hiển thị những tập tin trong package
-s	Hiển thị trạng thái của các tập tin trong package
-d	Hiển thị danh sách tập tin tài liệu cho package (ví dụ man, README, info file …)
--c	Hiển thị danh sách tập tin cấu hình

2.3.4. XUNG ĐỘT TẬP TIN PHẦN MỀM

Khicài package chứa tập tin trùng với tập tin đã tồn tại của package khác hoặc của bản cũ sẽ xảy ra lỗi.

- Ví dụ 2.3.4:# rpm -ivh foo-1.0-1.i386.rpm

  foo /usr/bin/foo conflicts with file from bar-1.0-1

Để bỏ qua lỗi này,có thể cài đè lên bằng cách sử dụng tùy chọn --replacefiles.

- Ví dụ 2.3.5:# rpm -ivh --replacefiles foo-1.0-1.i386.rpm

Một số package sử dụng các tập tin của các package khác. Trước khi cài package này,phải cài các package phụ thuộc, nếu không sẽ báo lỗi.

- Ví dụ 2.3.6:# rpm -ivh foo-1.0-1.i386.rpm

  failed dependencies:

  bar is needed by foo-1.0-1

Giải quyết trường hợp nàyphải cài các package được yêu cầu. Nếumuốn tiếp tục cài mà không cài các package khác thì dùng tùy chọn **--nodeps**. Tuy nhiên lúc này có thể package củacài có thể chạy không tốt.

2.3.5. LOẠI BỎ PHẦN MỀM ĐÃ CÀI ĐẶT TRONG HỆ THỐNG

- Cú pháp: #rpm -e <tên-package>
- Ví dụ 2.3.7:# rpm -e foo

  removing these packages would break dependencies:

  foo is needed by bar-1.0-1

Lưu ý là khi xóa chúng ta dùng tên-package chứ không dùng tên tập tin RPM.Nếu muốn xóa các package bỏ qua các lỗi,dùng thêm tham số **--nodeps**. Tuy nhiên nếu chương trìnhxóa có liên quan đến chương trình khác thì chương trình này sẽ hoạt động không được.

2.3.6. NÂNG CẤP PHẦN MỀM

- Cú pháp: # rpm –Uvh tên-tập-tinRPM
- Ví dụ 2.3.8:# rpm -Uvh foo-2.0-1.i386.rpm

Khi upgrade RPM sẽ xóa các phiên bản cũ của package.Có thể dùng lệnh này để cài đặt, khi đó sẽ không có phiên bản cũ nào bị xóa đi.

Khi RPM tự động nâng cấp với tập tin cấu hình,thấy chúng thường xuất hiện một thông báo như sau: saving /etc/foo.conf as /etc/foo.conf.rpm save. Điều này có nghĩa là khi tập tin cấu hình của phiên bản cũ không tương thích với phiên bản mới thì chúng lưu lại và tạo tập tin cấu hình mới.

Nâng cấp thực sự là sự kết hợp giữa Uninstall và Install. Vì thế khi upgrade cũng thường xảy ra các lỗi như khi Install và Uninstall và thêm một lỗi nữa là khiupgrade với phiên bản cũ hơn.

- Ví dụ 2.3.9# rpm -Uvh foo-1.0-1.i386.rpm
  foo package foo-2.0-1 (which is newer) is already installed
  Trong trường hợp nàythêm tham số --oldpackage
  # rpm -Uvh --oldpackage foo-1.0-1.i386.rpm

2.3.7. CÀI ĐẶT PHẦN MỀM FILE SOURCE *.tar, *.tgz

Ngoài các phần mềm được đóng gói dạng file nhị phân (file *.rpm) còn có các phần mềm được cung cấp dạng file source code như: *.tar hoặc *.tgz. Thông thường để cài đặt phần mềm này ta cần phải dựa vào trợ giúp của file giúp đỡ trong từng chương trình hoặc phần mềm, các file (README or INSTALL,) này nằm trong thư mục con của thư mục sau khi ta dùng lệnh tar để giải nén source. Để thực hiện việc cài đặt này ta thường làm các bước sau:

- **Bước 1:** Giải nén file tar

Ví dụ 2.3.10:#tar -xvzf linux-software-1.3.1.tar.gz

```
linux-software-1.3.1/
linux-software-1.3.1/plugins-scripts/
linux-software-1.3.1/linux-software-plugins.spec
[root@bigboy tmp]#
Tạo các thư mục con chứa các file cài đặt
[root@bigboy tmp]# ls
linux-software-1.3.1 linux-software-1.3.1.tar.gz
```

- **Bước 2:** Chuyển vào thư mục con và tham khảo các file INSTALL, README.

Ví dụ 2.3.11:# cd linux-software-1.3.1

```
[root@bigboy linux-software-1.3.1]# ls
COPYING install-sh missing plugins
depcomp LEGAL mkinstalldirs plugins-scripts
FAQ lib linux-software.spec README
Helper.pm Makefile.am linux-software.spec.in REQUIREMENTS
INSTALL Makefile.in NEWS subst.in
[root@bigboy linux-software-1.3.1]#
```

- **Bước 3:** Sau đó ta dựa vào chỉ dẫn trong file (INSTALL, README) để cài đặt phần mềm.

2.3.8. QUẢN LÝ PHẦN MỀM BẰNG YUM

Yum là tiện ích để quản lý phần mềm trên môi trường Linux. Với yum ta có thể cài đặt phần mềm trực tiếp từ hệ thống cục bộ hoặc cài đặt phần mềm trực tiếp từ Internet. Ngoài ra yum còn cho phép ta cập nhật phần mềm trong hệ thống, cài đặt cả nhóm các gói cho phần mềm, tự động phát hiện và kiểm tra các phần mềm cần thiết phải cài đặt. Với yum mọi việc cài đặt phần mềm trở nên đơn giản hơn.

2.3.9. CÀI ĐẶT PHẦN MỀM BẰNG YUM

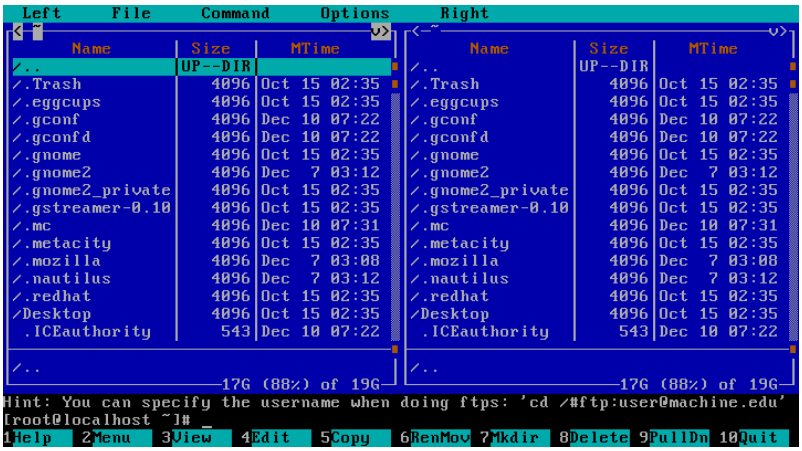
- Cú pháp:#su –c ‘yum install <tên phần mềm>hoặc #yum install <tên phần mềm>
- Ví dụ 2.3.12:#su –c ‘yum install mc’ hoặc lệnh #yum install mc

Trong đó mc là tên phần mềm cần cài đặt, tiếp theo chúng ta sẽ thực thi các bước sau:

```
[root@localhost ~]# su -c 'yum install mc'
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cuhk.edu.hk
 * extras: ftp.cuhk.edu.hk
 * updates: centosz4-msync-dvd.centos.org
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package mc.i386 1:4.6.1a-35.el5 set to be updated
--> Finished Dependency Resolution
```

```
Dependencies Resolved
================================================================
Package      Arch     Version      Repository       Size
================================================================
Installing:
mc             i386   1:4.6.1a-35.el5  base       2.1 M
Transaction Summary
================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 2.1 M
Is this ok [y/N]: y
Downloading Packages:
mc-4.6.1a-35.el5.i386.rpm              | 2.1 MB     00:07
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
Installing     : mc                     1/1
Installed:
mc.i386 1:4.6.1a-35.el5
Complete!
```

Hệ thống thông báo đã cài đặt hoàn tất phần mềm mc, ta có thể kiểm tra bằng cách chạy lệnh mc để kích hoạt chương trình.



2.3.10. **CẬP NHẬT PHẦN MỀM BẰNG YUM**

- Cú pháp:#su –c ‘yum update <tên phần mềm> hoặc #yum update <tên phần mềm>
- Ví dụ 2.3.13:#su –c ‘yum update bind’ hoặc lệnh #yum update bind.

Trong đó bind là phần mềm cần được update.

```
[root@localhost ~]# su -c 'yum install bind'
-->Running transaction check
-->Processing Dependency: bind = 30:9.3.6-16.P1.el5 for package:
caching-nameserver
-->Running transaction check
-->Package bind-utils.i386 30:9.3.6-16.P1.el5_7.1 set to be updated
-->Finished Dependency Resolution
Dependencies Resolved
================================================================================
Package        Arch        Version           Repository       Size
================================================================================
Updating:
bind       i386     30:9.3.6-16.P1.el5_7.1 updates          980 k
Updating for dependencies:
bind-chroot   i386    30:9.3.6-16.P1.el5_7.1   updates      46 k
bind-libs     i386    30:9.3.6-16.P1.el5_7.1   updates        862 k
bind-utils    i386    30:9.3.6-16.P1.el5_7.1   updates        173 k
caching-nameserver  i386  30:9.3.6-16.P1.el5_7.1 updates    62 k
Transaction Summary
================================================================================
Install       0 Package(s)
Upgrade       5 Package(s)
Total download size: 2.1 M
Is this ok [y/N]: y
Downloading Packages:
(1/5):bind-chroot-9.3.6-16.P1.el5_7.1.i386.rpm  |  46 kB     00:00
……..
(5/5): bind-9.3.6-16.P1.el5_7.1.i386.rpm        | 980 kB     00:11
--------------------------------------------------------------------------------
Total
101 kB/s | 2.1 MB     00:21
Running rpm_check_debug
Transaction Test Succeeded
Running Transaction
  Updating       : bind-libs                             1/10
```

```
  Updating       : bind                                    2/10
……..
  Cleanup        : bind                                    9/10
  Cleanup        : caching-nameserver                      10/10
Updated:
bind.i386 30:9.3.6-16.P1.el5_7.1
Dependency  Updated:    bind-chroot.i386  30:9.3.6-16.P1.el5_7.1  bind-
libs.i386  30:9.3.6-16.P1.el5_7.1  bind-utils.i386  30:9.3.6-16.P1.el5_7.1
caching-nameserver.i386 30:9.3.6-16.P1.el5_7.1
Complete!
```

2.3.11. **LOẠI BỎ PHẦN MỀM VỚI YUM**

- Cú pháp:#su –c ‘yum remove <tên phần mềm> hoặc #yum remove <tên phần mềm>
- Ví dụ 2.3.14#su –c ‘yum remove mc’ hoặc lệnh yum remove mc.

Trong đó mc là tên phần mềm.

```
[root@localhost ~]# su -c 'yum remove mc'
--> Running transaction check
---> Package mc.i386 1:4.6.1a-35.el5 set to be erased
--> Finished Dependency Resolution
Dependencies Resolved
================================================================
 Package     Arch     Version      Repository          Size
================================================================
Removing:
 mc          i386     1:4.6.1a-35.el5     installed   5.2 M
Transaction Summary
================================================================
Remove        1 Package(s)
Reinstall     0 Package(s)
Downgrade     0 Package(s)
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Erasing       : mc                1/1
```

```
Removed:
  mc.i386 1:4.6.1a-35.el5
Complete!
```

2.3.12. **TÌM PHẦN MỀM BẰNG YUM**

- Cú pháp:#su –c ‘yum list <tên phần mềm>’ hoặc lệnh yum list <tên phần mềm>
- Ví dụ 2.3.15:#su –c ‘yum list mc’ hoặc lệnh yum list mc

Trong đó mc là tên phần mềm cần tìm. Kết xuất của quá trình tìm kiếm sẽ cho ta biết phần mềm này có được cài đặt trong hệ thống hay còn trong bộ lưu trữ.

```
[root@localhost ~]# yum list mc
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cuhk.edu.hk
 * extras: ftp.cuhk.edu.hk
 * updates: centosz4-msync-dvd.centos.org
Installed Packages
mc.i386
1:4.6.1a-35.el5
installed
```

- Ví dụ 2.3.16:#su –c ‘yum search named’

```
[root@localhost ~]# su -c 'yum search named'
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cuhk.edu.hk
 * extras: ftp.cuhk.edu.hk
 * updates: centosz4-msync-dvd.centos.org
=================== Matched: named ====================
bind.i386 : The Berkeley Internet Name Domain (BIND) DNS (Domain Name
System) server.
bind-chroot.i386 : A chroot runtime environment for the ISC BIND DNS
server, named(8)
bind-sdb.i386 : The Berkeley Internet Name Domain (BIND) DNS (Domain
Name System) server with database backends.
caching-nameserver.i386 : Default BIND configuration files for a caching
nameserver
bind97.i386 : The Berkeley Internet Name Domain (BIND) DNS (Domain Name
System) server
```

```
bind97-chroot.i386 : A chroot runtime environment for the ISC BIND DNS
server, named(8)
c-ares.i386 : A library that performs asynchronous DNS operations
e4fsprogs.i386 : Utilities for managing the fourth extended (ext4)
filesystem
perl-Archive-Zip.noarch : Perl library for accessing Zip archives
pstack.i386 : Display stack trace of a running process
sqlite.i386 : Library that implements an embeddable SQL database engine
system-config-bind.noarch : The BIND DNS Configuration Tool.
```

- Ví dụ 2.3.17#su –c ‘yum provides bind’

```
[root@localhost ~]# su -c 'yum provides bind'
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cuhk.edu.hk
 * extras: ftp.cuhk.edu.hk
 * updates: centosz4-msync-dvd.centos.org
30:bind-9.3.6-16.P1.el5.i386 : The Berkeley Internet Name Domain (BIND)
DNS (Domain Name System) server.
Repo        : base
Matched from:
30:bind-9.3.6-16.P1.el5_7.1.i386 : The Berkeley Internet Name Domain
(BIND) DNS (Domain Name System) server.
Repo        : updates
Matched from:
30:bind-9.3.6-16.P1.el5_7.1.i386 : The Berkeley Internet Name Domain
(BIND) DNS (Domain Name System) server.
Repo        : installed
Matched from:
Other       : Provides-match: bind
```

Nếu chúng ta muốn tìm phần mềm ở dạng gần đúng, ví dụ như tìm tất cả các phần mềm bắt đầu bằng ký tự bin thì ta dùng mô tả bin*.

- Ví dụ 2.3.18:#su –c ‘yum list bin*’

```
[root@localhost ~]# su -c 'yum list bin\*'
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cuhk.edu.hk
 * extras: ftp.cuhk.edu.hk
 * updates: centosz4-msync-dvd.centos.org
```

```
Installed Packages
bind.i386                30:9.3.6-16.P1.el5_7.1        installed
bind-chroot.i386         30:9.3.6-16.P1.el5_7.1        installed
bind-libs.i386           30:9.3.6-16.P1.el5_7.1        installed
bind-utils.i386          30:9.3.6-16.P1.el5_7.1        installed
binutils.i386            2.17.50.0.6-14.el5            installed
Available Packages
bind-devel.i386          30:9.3.6-16.P1.el5_7.1        updates
bind-libbind-devel.i386  30:9.3.6-16.P1.el5_7.1        updates
bind-sdb.i386            30:9.3.6-16.P1.el5_7.1        updates
bind97.i386              32:9.7.0-6.P2.el5_7.4         updates
bind97-chroot.i386       32:9.7.0-6.P2.el5_7.4         updates
bind97-devel.i386        32:9.7.0-6.P2.el5_7.4         updates
bind97-libs.i386         32:9.7.0-6.P2.el5_7.4         updates
```

2.3.13. CẬP NHẬT HỆ THỐNG BẰNG YUM

Sử dụng tùy chọn update để cập nhật phần mềm cho hệ thống với phiên bản cập nhật mới nhất từ Internet.

- Ví dụ 2.3.19:#su –c ‘yum update’

```
[root@localhost ~]# su -c 'yum update'
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cuhk.edu.hk
 * extras: ftp.cuhk.edu.hk
 * updates: centosz4-msync-dvd.centos.org
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package NetworkManager.i386 1:0.7.0-13.el5 set to be updated
---> Package NetworkManager-glib.i386 1:0.7.0-13.el5 set to be updated
……..
---> Package authconfig-gtk.i386 0:5.3.21-7.el5 set to be updated
---> Package autofs.i386 1:5.0.1-0.rc2.156.el5_7.4 set to be updated
base/filelists                  | 2.9 MB     00:18
extras/filelists_db             | 215 kB     00:00
updates/filelists_db            | 1.6 MB     00:06
--> Finished Dependency Resolution
Dependencies Resolved
```

```
================================================================================
Package             Arch         Version       Repository        Size
================================================================================
Installing:
 kernel             i686    2.6.18-274.12.1.el5 updates     18 M
Updating:
 NetworkManager     i386    1:0.7.0-13.el5    base          1.0 M
 NetworkManager-glib  i386  1:0.7.0-13.el5    base          82 k
 NetworkManager-gnome i386  1:0.7.0-13.el5    base          327 k
 OpenIPMI             i386  2.0.16-11.el5_7.2 updates       158 k
 OpenIPMI-libs        i386  2.0.16-11.el5_7.2 updates       570 k
 SysVinit             i386  2.86-17.el5      base          113 k
 apr                  i386  1.2.7-11.el5_6.5  base          124 k
Installing for dependencies:
 perl-NetAddr-IP      i386  4.027-5.el5_6     base          109 k
Transaction Summary
================================================================================
Install       2 Package(s)
Upgrade     187 Package(s)
Total download size: 295 M
Is this ok [y/N]: y
```

2.4. CÂU HỎI ÔN TẬP:

1. Hãy cài đặt hệ điều hành CentOS6 dưới sự kiểm soát của máy ảo Vmware
2. Giải thích cách tổ chức phần vùng ổ cứng trong quá trình cài đặt hệ điều hành Linux
3. Hãy cấu hình các thiết bị sau khi cài đặt hệ điều hành Linux
4. Trong quá trình cài đặt hệ điều hành Linux cần tạo ra bao nhiêu phân vùng (partition) ổ đĩa.
5. Một ổ cứng (HDD) có thể tạo tối đa bao nhiêu phân vùng (partition).
6. Hãy cho biết các đặc điểm của bản phân phối CentOS6
7. Hãy cho biết các kiểu định dạng partition dùng cho hệ điều hành linux
8. Hãy giải thích boot sector và Master Boot Record là gì?
9. Trong quá trình cài đặt, mật khẩu của tài khoản root có chiều dài tối đa bao nhiêu ký tự?
10. Có thể cài đặt nhiều hệ điều hành (Linux và windows) trên cùng một máy hay không? Nếu được thì cài đặt như thế nào?

CHƯƠNG 3: QUẢN LÝ TÀI KHOẢN ADMINISTRATOR

Nội dung:

- ❖ Quản lý người dùng (user) trong Linux.
- ❖ Quản lý nhóm (group) trong Linux
- ❖ Thiết lập quyền hạn của người dùng lên file, chuyển đổi chủ sở hữu, nhóm sở hữu,…
- ❖ Quản lý người dùng và nhóm (user, group) bằng giao diện đồ họa.
- ❖ Làm quen với cơ chế tổ chức filesystem, các tập lệnh liên quan, quyền hạn truy cập file, quản lý filesystem.
- ❖ Làm quen với trình tiện ích quản lý phân vùng đĩa, sử dụng các thiết bị lưu trữ

TÓM TẮT

- Phần 3.1: Giới thiệu cách thức quản lý tài khoản người dùng trên Linux như: xem thông tin tài khoản người dùng, các thao tác quản trị người dùng và cách thiết lập quyền cho tài khoản người dùng.
- Phần 3.2: Giới thiệu và quản trị hệ thống Linux ở chế độ dòng lệnh với các thao tác lệnh cơ bản và cách thức quản trị các Run Level
- Phần 3.3: Giới thiệu và quản trị filesystem như mô tả chức năng và cấu trúc filesystem, các thao tác cơ bản trên filesystem, các thao tác trên thư mục và tập tin
- Phần 3.4: Quản trị đóng tắt hệ thống với các thao tác: các bước khởi động hệ thống, phục hồi mật khẩu cho tài khoản quản trị.
- Phần 3.5: Quản trị dịch vụ System Services như dịch vụ Xinetd, dịch vụ Telnet và bảo mật Telnet, dịch vụ SSH.

3.1. QUẢN LÝ NGƯỜI DÙNG

Trong hệ thống Linux, tài khoản này có tên là root. Đây là tài khoản có quyền cao nhất được sử dụng bởi người quản trị, giám sát hệ thống. Tuy nhiên chúng ta chỉ sử dụng tài khoản này vào các mục đích cấu hình, bảo trì hệ thống chứ không nên sử dụng vào mục đích hằng ngày.Cần tạo các tài khoản (account) cho người sử dụng thường nhất có thể được (đầu tiên là cho bản thân). Với những server quan trọng và có nhiều dịch vụ khác nhau,có thể tạo ra các superuser thích hợp cho từng dịch vụ để tránh dùng root cho các việc này. Ví dụ như superuser cho công tác backup chỉ cần chức năng đọc (read-only) mà không cần chức năng ghi.

Trong Linux, chúng ta có thể tạo tài khoản có tên khác nhưng có quyền của root, bằng cách tạo user có UserID bằng 0. Cần phân biệtđang login như root hay người sử dụng thường thông qua dấu nhắc của shell.

```
login: cntt
Password:******
Last login: Wed Mar 13 19:00:42 2002 from 172.29.8.3
[tdnhon@NetGroup tdnhon]$ su -
Password: ****
```

Dòng thứ tư với dấu $ cho thấyđang kết nối như một người sử dụng thường (cntt). Dòng cuối cùng với dấu # cho thấyđang thực hiện các lệnh với root.

3.1.1. THÔNG TIN VỀ NGƯỜI DÙNG

Mỗi tài khoản người dùng phải có một tên sử dụng (username) và mật khẩu (password) riêng. Tập tin /etc/passwd là tập tin chứa các thông tin về tài khoản người dùng của hệ thống.

Tên người dùng là chuỗi ký tự xác định duy nhất một người dùng. Người dùng sử dụng tên này khi đăng nhập cũng như truy xuất tài nguyên. Trong Linux tên người dùng có sự phân biệt giữa chữ hoa và thường. Thông thường, tên người dùng thường sử dụng chữ thường. Để dễ dàng trong việc quản lý người dùng, ngoài tên người dùng Linux còn sử dụng khái niệm định danh người dùng (user _ID). Mỗi người dùng có một con số định danh riêng.

Linux sử dụng số định danh để kiểm soát hoạt động của người dùng. Theo qui định chung, những người dùng có định danh là 0 là người dùng quản trị (root). Các số định danh từ 1-99 sử dụng cho các tài khoản hệ thống, định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 100

Tập tin /etc/passwd

Tập tin /etc/passwd đóng vai trò sống còn đối với một hệ thống Unix, Linux. Nó là cơ sở dữ liệu các tài khoản người dùng trên Linux và được lưu dưới dạng tập tin văn bản. Chúng ta thử xem qua nội dung của tập tin passwd:`#cat /etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
```

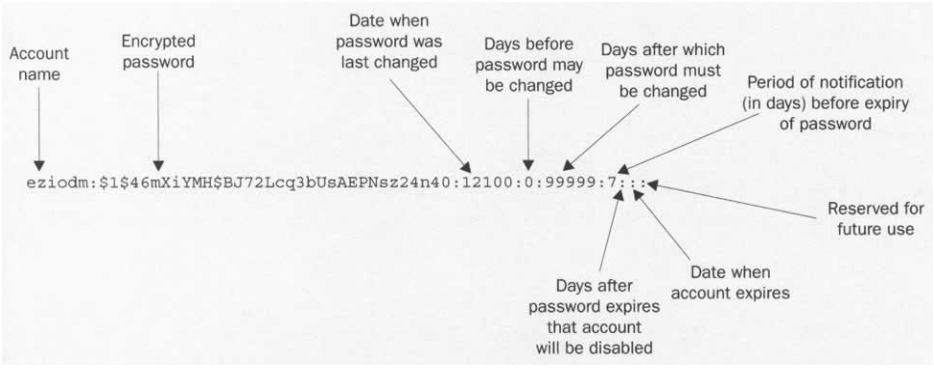
```
ftp:x:14:50:FTP User:/var/ftp:
nobody:x:99:99:Nobody:/:
nscd:x:28:28:NSCD Daemon:/:/bin/false
mailnull:x:47:47::/var/spool/mqueue:/dev/null
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/bin/false
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
nthung:x:525:526:nguyen tien hung:/home/nthung:/bin/bash
natan:x:526:527::/home/natan:/bin/bash
```

Mỗi tài khoản được lưu trong một dòng gồm 7 cột:

- Cột 1: Tên người sử dụng.
- Cột 2: Mã liên quan đến mật khẩu của tài khoản và "x" đối với Linux. Linux lưu mã này trong một tập tinkhác /etc/shadow mà chỉ có root mới có quyền đọc.
- Cột 3:4: Mã định danh tài khoản (user ID) và mã định danh nhóm (group ID).
- Cột 5: Tên đầy đủ của người sử dụng. Một số phần mềm phá password sử dụng dữ liệu của cột này đểthử đoán password.
- Cột 6: thư mục cá nhân (Home Directory)
- Cột 7: Chương trình sẽ chạy đầu tiên sau khi người dùng đăng nhập vào hệ thống.

Tập tin /etc/shadow

- Là nơi lưu trữ mật khẩu đã được mã hóa
- Cấu trúc tập tin /etc/shadow như sau:`#cat /etc/shadow`



- Tên tài khoản
- Mật khẩu đã mã hóa:
  - Bắt đầu bằng * biểu thị tài khoản đã bị vô hiệu hóa (disable)
  - Bắt đầu bằng !!, tài khoản tạm thời bị khóa (locked)
- Ngày đổi mật khẩu (tính từ 1/1/1970)
- Ngày có thể đổi mật khẩu (0 = bất kỳ lúc nào)

- Ngày phải đổi mật khẩu
- Ngày báo mật khẩu sắp hết hạn
- Số ngày sẽ vô hiệu hóa tài khoản nếu không đổi mật khẩu đúng hạn
- Ngày sẽ tự động vô hiệu hóa tài khoản
- Dự trữ để sử dụng sau này

3.1.2. CÁC THAO TÁC QUẢN TRỊ NGƯỜI DÙNG

Tạo tài khoản người dùng

a) Lệnh trợ giúp man

- Cú pháp lệnh: #man <lệnh>
- Ví dụ:#man useradd

```
USERADD(8)        System Management       Commands    USERADD(8)
NAME
       useradd - create a new user or update default new user
       information
SYNOPSIS
       useradd [options] LOGIN
       useradd -D
       useradd -D [options]
DESCRIPTION
       When invoked without the -D option, the useradd command creates
       a new user account using the values specified on the command
       line plus the default values from the system. Depending on
       command line options, the useradd command will update system
       files and may also create the new userÂ´s home directory and copy
       initial files.
       By default, a group will also be created for the new user (see
       -g, -N, -U, and USERGROUPS_ENAB).
OPTIONS
:
```

b) Tạo tài khoản người dùng

- Cú pháp:#useradd [-c lời_mô_tả_về_người_dùng] [-d thư_mục_cá_nhân] [-m] [-g nhóm_của_người_dùng] [tên_tài_khoản]

Trong đó: Tham số –m được sử dụng để tạo thư mục cá nhân nếu nó chưa tồn tại; và chỉ có root được phép sử dụng lệnh này

- Ví dụ 3.1.1:# useradd hocvien
- Kiểm tra hocvien trong /etc/passwd:

```
[root@localhost ~]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
……..
named:x:25:25:Named:/var/named:/sbin/nologin
hocvien:x:501:501::/home/hocvien:/bin/bash
```

- Kiểm tra hocvien trong /etc/shadow

```
[root@localhost ~]# vi /etc/shadow
root:$6$TJbnN.B1u2MnUkxE$axmsOdkqonFy.CbiJ6SsDwqXMp74J3oJ2/RGJ.eM/G3ww23ACJ
J67.LwYVBN6lFw6KF8x5rQ5J92NZJ1ZZUok0:15320:0:99999:7:::
……
named:!!:15325::::::
hocvien:!!:15326:0:99999:7:::
```

Tài khoản hocvien dang bi tạm khóa do chua đặt mật khẩu.

- Kiểm tra hocvien trong /etc/group

```
[root@localhost ~]# vi /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
……
gdm:x:42:
lhu:x:500:
named:x:25:
hocvien:x:501:
```

Đặt mật khẩu người dùng

- Cú pháp: #passwd <username>
- Ví dụ 3.1.2# passwd hocvien

```
[root@localhost ~]# passwd hocvien
Changing password for user hocvien.
New password:
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is a palindrome
Retype new password:
```

```
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

Vì vấn đề an ninh cho máy Linux và sự an toàn của toàn hệ thống mạng, việc chọn đúng password là rất quan trọng. Một password gọi là tốt nếu:

- **Có độ dài tối thiểu 6 ký tự.**
- **Phối hợp giữa chữ thường, chữ hoa, số và các ký tự đặc biệt.**
- **Không liên quan đến tên tuổi, ngày sinh … của bạn và người thân.**

- Kiểm tra hocvien trong /etc/showdow

```
[root@localhost ~]# vi /etc/shadow
root:$6$TJbnN.B1u2MnUkxE$axmsOdkqonFy.CbiJ6SsDwqXMp74J3oJ2/RGJ.eM/G3ww23ACJ
J67.LwYVBN6lFw6KF8x5rQ5J92NZJ1ZZUok0:15320:0:99999:7:::
bin:*:14924:0:99999:7:::
……..
named:!!:15325::::::
hocvien:$6$NQq/CPOt$yg6Y5E1ly3ES/ZfgImmG6vZNwVb6ZUbgbN/sVh8M2wviDh8aVJUTV0W
B80OB/phCEuMIqFJFBJYVf.qbwriaL1:15326:0:99999:7:::
```

Tài khoản hocvien đã được active và mật khẩu đã được mã hóa.

- Ví dụ 3.1.3: tạo user sv có home directory là /tmp/sv và có dòng mô tả “day la tai khoan dung de test”:

- Tạo tài khoản sinhvien: #useradd –c “day la tai khoan dung de test” –d /tmp/sv sv
- Kiểm tra user sv vừa tạo:

```
[root@localhost ~]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
……
named:x:25:25:Named:/var/named:/sbin/nologin
hocvien:x:501:501::/home/hocvien:/bin/bash
sv:x:502:502:day la tai khoan dung de test:/tmp/sv:/bin/bash
```

- Ví dụ 3.1.4: Tạo tài khoản hv1 có home directory là /tmp/hv1 và thuộc nhóm hocvien:

- Tạo tài khoản hv1:#useradd –d /tmp/hv1 –g hocvien hv1
- Kiểm tra hv1 trong /etc/passwd

```
[root@localhost ~]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
……..
hocvien:x:501:501::/home/hocvien:/bin/bash
```

```
sv:x:502:502:day la tai khoan dung de test:/tmp/sv:/bin/bash
test:x:503:503:day la tai khoan dung de test:/tmp/test:/bin/bash
hv1:x:504:501::/tmp/hv1:/bin/bash
```

- Kiểm tra hv1 trong /etc/group

```
[root@localhost ~]# vi /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
…….
hocvien:x:501:
sv:x:502:
test:x:503:
```

Thay đổi mật khẩu tài khoản người dùng

c) Thay đổi mật khẩu tài khoản root

```
[root@localhost ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

- Làm tương tự cho việc thay đổi mật khẩu các tài khoản khác như hocvien, hv1.

Thay đổi thông tin của tài khoản

- Xem cú pháp lệnh usermod

```
[root@localhost ~]# man usermod
USERMOD(8)         System Management Commands         USERMOD(8)
NAME
       usermod - modify a user account
SYNOPSIS
       usermod [options] LOGIN
DESCRIPTION
       The usermod command modifies the system account files to reflect
       the changes that are specified on the command line.
OPTIONS
       The options which apply to the usermod command are:
```

```
       -a, --append
           Add the user to the supplementary group(s). Use only with
           the -G option.
       -c, --comment COMMENT
           The new value of the userÂ´s password file comment field. It
           is normally modified using the chfn(1) utility.
       -d, --home HOME_DIR
           The userÂ´s new login directory.
```

- Cú pháp:#usermod [-c mô_tả_thông_tin_người_dùng] [-d thư_mục_cá_nhân] [-m] [-g nhóm_của_người_dùng] [tên_tài_khoản
- Ví dụ 3.1.5:Thêm tài khoản nvb vào nhóm admin
    - #usermod –g admin nvb
- Thay đổi home directory của hv1 là /home/hv1: `#usermod –d /home/hv1 hv1`
- Kiểm tra hv1 trong /etc/passwd

```
[root@localhost ~]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
…….
test:x:503:503:day la tai khoan dung de test:/tmp/test:/bin/bash
hv1:x:504:501::/home/hv1/:/bin/bash
```

- Thay đổi hv1 thuộc nhóm nhanvien: `#usermod –g  nhanvien  hv1`

```
[root@localhost ~]# usermod -g nhanvien hv1
[root@localhost ~]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
```

```
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-
autoipd:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
…….
test:x:503:503:day la tai khoan dung de test:/tmp/test:/bin/bash
hv1:x:504:504::/home/hv1/:/bin/bash
```

Tạm khóa tài khoản người dùng

- Khoá hv1: passwd -l hv1 (hay dùng lệnh usermod -L hv1)

```
[root@localhost ~]# passwd -l hv1
Locking password for user hv1.
passwd: Success
[root@localhost ~]#
```

- Kiểm tra hv1 trong /etc/shadow

```
[root@localhost ~]# vi /etc/shadow
root:$6$TJbnN.B1u2MnUkxE$axmsOdkqonFy.CbiJ6SsDwqXMp74J3oJ2/RGJ.eM/G3ww23ACJ
J67.LwYVBN6lFw6KF8x5rQ5J92NZJ1ZZUok0:15320:0:99999:7:::
bin:*:14924:0:99999:7:::
…….
test:!!:15326:0:99999:7:::
hv1:!!:15326:0:99999:7:::
```

- Mở khóa hv1: pass -u hv1 (hay dùng lệnh usermod -U hv1)

```
[root@localhost ~]# passwd -u hv1
Unlocking password for user hv1.
passwd: Success
[root@localhost ~]#
```

- Kiểm tra hv1 trong /etc/shadow

```
[root@localhost ~]# vi /etc/shadow
root:$6$TJbnN.B1u2MnUkxE$axmsOdkqonFy.CbiJ6SsDwqXMp74J3oJ2/RGJ.eM/G3ww23ACJ
J67.LwYVBN6lFw6KF8x5rQ5J92NZJ1ZZUok0:15320:0:99999:7:::
bin:*:14924:0:99999:7:::
……
test:!!:15326:0:99999:7:::
hv1::15326:0:99999:7:::
```

Hủy tài khoản

- Cú pháp:#userdel <option> [username]
- Ví dụ 3.1.6: xóa người dùng hocvien
  #userdel –r hocvien

3.1.3. QUẢN LÝ NHÓM NGƯỜI DÙNG

Thiết lập những người dùng có chung một số đặc điểm nào đó hay có chung quyền hạn trên tài nguyên vào chung một nhóm. Mỗi nhóm có một tên riêng và một định danh nhóm, một nhóm có thể có nhiều người dùng và người dùng có thể là thành viên của nhiều nhóm khác nhau. Tuy nhiên tại một thời điểm, một người dùng chỉ có thể là thành viên của một nhóm duy nhất.Thông tin về nhóm lưu tại tập tin /etc/group. Mỗi dòng định nghĩa một nhóm, các trường trên dòng cách nhau bằng dấu hai chấm ":". Nội dung của một dòng theo cú pháp sau:*<tên-nhóm>:<password-của-nhóm>:<định-danh-nhóm>:<các-user-thuộc-nhóm>*

Tạo nhóm người dùng

- Cú pháp của lệnh:#groupadd [tên-nhóm]
- Xem cú pháp lệnh:#man groupadd

```
[root@localhost ~]# man groupadd
GROUPADD(8)        System Management Commands          GROUPADD(8)
NAME
       groupadd - create a new group
SYNOPSIS
       groupadd [options] group
DESCRIPTION
       The groupadd command creates a new group account using the
       values specified on the command line plus the default values
       from the system. The new group will be entered into the system
       files as needed.
OPTIONS
       The options which apply to the groupadd command are:

       -f, --force
           This option causes the command to simply exit with success
           status if the specified group already exists. When used with
           -g, and the specified GID already exists, another (unique)
           GID is chosen (i.e.  -g is turned off).
       -g, --gid GID
           The numerical value of the groupÂ´s ID. This value must be
:
```

- Ví dụ 3.1.7: Tạo nhóm có tên sinhvien:

```
#[root@localhost~]# groupadd     sinhvien
```

- Kiểm tra nhóm sinhvien trong /etc/group

```
[root@localhost ~]# vi /etc/group
```

```
root:x:0:root
bin:x:1:root,bin,daemon
……..
sinhvien:x:505:
```

Thay đổi thông tin nhóm

- Cú pháp:usermod –g [tên-nhóm tên-tài-khoản]
- Xem cú pháp lệnh: man groupmod

```
[root@localhost ~]# man groupmod
GROUPMOD(8)         System Management Commands         GROUPMOD(8)
NAME
       groupmod - modify a group definition on the system
SYNOPSIS
       groupmod [options] GROUP
DESCRIPTION
       The groupmod command modifies the definition of the specified
       GROUP by modifying the appropriate entry in the group database.
OPTIONS
       The options which apply to the groupmod command are:
       -g, --gid GID
           The group ID of the given GROUP will be changed to GID.

           The value of GID must be a non-negative decimal integer.
           This value must be unique, unless the -o option is used.
           Values between 0 and 999 are typically reserved for system
           groups.
           Any files that have the old group ID and must continue to
           belong to GROUP, must have their group ID changed manually.
:
```

- Thay đổi tên nhóm sinhvien thanh nhóm nhom1

```
[root@localhost ~]# groupmod -n nhom1 sinhvien
```

- Kiểm tra nhom1 trong /etc/group

```
[root@localhost ~]# vi /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
……..
nhom1:x:505:
```

- Đổi ID của nhóm nhom1 thành 600

```
[root@localhost ~]# groupmod -g 600 nhom1
```

- Kiểm tra nhóm nhom1 trong /etc/group

```
[root@localhost ~]# vi /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
…….
nhom1:x:600:
```

Thêm người dùng vào nhóm

- Cú pháp: #usermod -g <users> <nhóm>
- Ví dụ 3.1.8: #usermod -g sinhvien nhom1

Hủy nhóm

- Cú pháp:#groupdel [tên-nhóm]
- Ví dụ 3.1.9 #groupdel sinhvien

3.1.4. CÁC THAO TÁC LOGIN VÀ LOGOUT

- Từ root đăng nhập vào hv1: #su – hv1
- Từ hv1 đăng nhập vào hocvien: $su – hocvien
- Thoát khỏi hocvien:$exit
- Thoát khỏi hv1:$exit
- Thoát khỏi root:#exit

```
[root@localhost ~]# su - hv1
[hv1@localhost ~]$  su - hocvien
Password:
[hocvien@localhost ~]$ exit
logout
[hv@localhost ~]$  exit
logout
[root@localhost ~]# su - hocvien
[hocvien@localhost ~]$ exit
logout
[root@localhost ~]# exit
```

3.2. GIAO DIỆN DÒNG LỆNH

3.2.1. ĐĂNG NHẬP VỚI GIAO DIỆN DÒNG LỆNH

Giao diện dòng lệnh (text) chủ yếu để cung cấp cho người dùng quản trị. Điểm mạnh của hệ thống Linux là ở đặc điểm này, ở giao diện text cho phép người quản trị có toàn quyền quản trị hệ thống, thực hiện bất kỳ tác vụ nào, giao diện text cung cấp nhiều thuận lợi cho người quản trị, giúp quản trị hệ thống hiệu quả hơn, nhanh hơn, và an toàn hơn.

Nhập username và mật khẩu để đăng nhập giao diện Text.

Có hai chế độ dấu nhắc lệnh:

- Dấu nhắc $ dùng cho người dùng thông thường
- Dấu nhắc # dùng cho người dùng quản trị (root)
- Cách sử dụng lệnh trên giao diện Text theo cấu trúc:<command prompt> command <option><parameter>

Trong đó:

- Command prompt là dấu nhắc lệnh
- Command là tên lệnh
- Option là các tùy chọn của lệnh
- Parameter là tham số dòng lệnh

Ví dụ 3.2.1 `[root@localhost ~]# ls -a -l /etc`

```
[root@localhost ~]# ls -a -l /etc
total 4008
drwxr-xr-x 105 root root   12288 Dec 10 08:29 .
drwxr-xr-x  23 root root    4096 Dec 10 07:22 ..
-rw-r--r--   1 root root   15288 May 25  2008 a2ps.cfg
-rw-r--r--   1 root root    2562 May 25  2008 a2ps-site.cfg
drwxr-xr-x   4 root root    4096 Oct 15 02:02 acpi
-rw-r--r--   1 root root      45 Dec  7 03:13 adjtime
drwxr-xr-x   4 root root    4096 Oct 15 01:59 alchemist
-rw-r--r--   1 root root    1512 Apr 25  2005 aliases
-rw-r-----   1 root smmsp  12288 Dec 10 07:22 aliases.db
……
```

3.2.2. CÁC LỆNH CƠ BẢN

Xem danh sách các xử lý của hệ thống

```
[root@localhost ~]# top
top - 19:55:56 up 8 min,  2 users,  load average: 0.00, 0.00, 0.00
Tasks: 103 total,   1 running, 102 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.3%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:    511572k total,   188724k used,   322848k free,    19364k buffers
Swap:  1048568k total,        0k used,  1048568k free,    85216k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2088 root      20   0 11144 3160 2544 S  0.3  0.6   0:00.10 sshd
 2122 root      20   0  2632 1108  880 R  0.3  0.2   0:00.06 top
    1 root      20   0  2828 1376 1184 S  0.0  0.3   0:01.77 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
```

Xem danh sách các xử lý của hệ thống, thực hiện ở chế độ background:

```
[root@localhost ~]# top &
[1] 2124
```

Điều khiển job

a) Liệt kê những jobs đang chạy

```
[root@localhost ~]# jobs
[1]+  Stopped                 top
```

b) Chuyển một job đang chạy từ chế độ foreground sang chế độ background

```
[root@localhost ~]# bg 1
[1]+ top &
[1]+  Stopped                 top
```

c) Chuyển một job đang chạy từ chế độ background sang chế độ foreground

```
[root@localhost ~]# fg 1
top
```

```
top - 19:58:01 up 10 min,  2 users,  load average: 0.00, 0.00, 0.00
Tasks: 103 total,   1 running, 102 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:    511572k total,   188840k used,   322732k free,    19412k buffers
Swap:  1048568k total,        0k used,  1048568k free,    85216k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      20   0  2828 1376 1184 S  0.0  0.3   0:01.77 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    6 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events/0
    7 root      20   0     0    0    0 S  0.0  0.0   0:00.00 cpuset
    8 root      20   0     0    0    0 S  0.0  0.0   0:00.00 khelper
```

Lệnh về biến môi trường

a) Xem danh sách các biến môi trường: end (hay printenv)

```
[root@localhost ~]# env
HOSTNAME=localhost.localdomain
SELINUX_ROLE_REQUESTED=
TERM=vt100
SHELL=/bin/bash
HISTSIZE=1000
SSH_CLIENT=172.16.29.165 49423 22
SELINUX_USE_CURRENT_RANGE=
QTDIR=/usr/lib/qt-3.3
QTINC=/usr/lib/qt-3.3/include
SSH_TTY=/dev/pts/0
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;
01:cd=40;33;01:or=40;31;01:mi=01;05;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;
c=01;36:*.mid=01;36:*.midi=01;36:*.mka=01;36:*.mp3=01;36:*.mpc=01;36:*.ogg=
01;36:*.ra=01;36:*.wav=01;36:*.axa=01;36:*.oga=01;36:*.spx=01;36:*.xspf=01;
36:
MAIL=/var/spool/mail/root
PATH=/usr/lib/qt-
3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/
bin
PWD=/root
```

```
LANG=en_US.UTF-8
SELINUX_LEVEL_REQUESTED=
SSH_ASKPASS=/usr/libexec/openssh/gnome-ssh-askpass
HISTCONTROL=ignoredups
SHLVL=1
HOME=/root
LOGNAME=root
QTLIB=/usr/lib/qt-3.3/lib
CVS_RSH=ssh
SSH_CONNECTION=172.16.29.165 49423 172.16.29.151 22
LESSOPEN=|/usr/bin/lesspipe.sh %s
G_BROKEN_FILENAMES=1
_=/bin/env
```

b) Cài đặt biến môi trường rpm=”Redhat Package Manager”:

```
[root@localhost~]#export rpm=” Redhat Package Manager”
```

c) Kiểm tra biến môi trường vừa đặt

```
[root@localhost ~]# env
HOSTNAME=localhost.localdomain
SELINUX_ROLE_REQUESTED=
TERM=vt100
SHELL=/bin/bash
HISTSIZE=1000
SSH_CLIENT=172.16.29.165 49423 22
SELINUX_USE_CURRENT_RANGE=
QTDIR=/usr/lib/qt-3.3
QTINC=/usr/lib/qt-3.3/include
SSH_TTY=/dev/pts/0
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;
01:cd=40;33;01:or=40;31;01:mi=01;05;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;
c=01;36:*.mid=01;36:*.midi=01;36:*.mka=01;36:*.mp3=01;36:*.mpc=01;36:*.ogg=
01;36:*.ra=01;36:*.wav=01;36:*.axa=01;36:*.oga=01;36:*.spx=01;36:*.xspf=01;
36:
MAIL=/var/spool/mail/root
PATH=/usr/lib/qt-
3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/
bin
rpm= Redhat Package Manager
```

d) Gỡ bỏ biến môi trường rpm:

```
[root@localhost ~]#unset rpm
```

e) Một số lệnh thường dùng khác trong Linux

Tên lệnh	Cú pháp	Ý nghĩa
Date	$date	Hiển thị ngày hệ thống
who	#who	Hiển thị danh sách các tài khoản đang đặp nhập vào hệ thống
tty	#tty	Xác đinh tập tin tty mà mình đang login vào
cal	$cal	Xem lịch hệ thống
head	$head <filename>	Xem nội dung tập tin đầu tập tin
tail	$tail <filename>	Xem nội dung cuối tập tin
hostname	$hostname	Xem và đổi tên máy
passwd	$passwd <username>	Đổi mật khẩu của user
ls	ls <filename>	Liệt kê thuộc tính của file và thư mục
cd	cd <directory>	Di chuyển thư mục
man	$man <lệnh>	Trợ giúp

3.2.3. CÁC RUN LEVEL

Sau khi khởi động, hệ thống tự động nạp chương trình /sbin/init để kiểm tra hệ thống tập tin. Sau đó đọc file /etc/inittab để xác định mức hoạt động (runlevel). Các Linux runlevel nhu sau:

Runlevel	Thư mục lưu script	Mô tả module hoạt động
0	/etc/rc.d/rc0.d	Chế độ tắt hệ thống
1	/etc/rc.d/rc1.d	Chế độ đơn người dùng, cho phép hiệu quả chỉnh sự cố hệ thống
2	/etc/rc.d/rc2.d	Chế độ text cho đa người dùng không hỗ trợ NFS
3	/etc/rc.d/rc3.d	Chế độ text cho đa người dùng, hỗ trợ đầy đủ
4	/etc/rc.d/rc4.d	Không sử dụng
5	/etc/rc.d/rc5.d	Sử dụng cho nhiều người dùng, cung cấp giao diện đồ họa

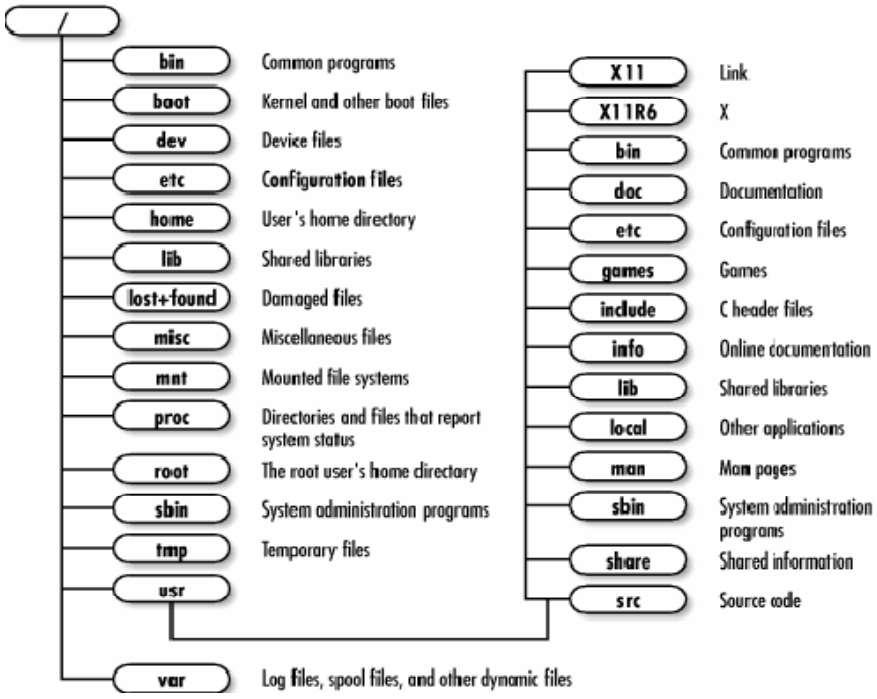
6	/etc/rc.d/rc6.d	Reboot hệ thống

Để thay đổi mức run level bằng cách cấu hình tập tin /etc/inittab, thay đổi thông số runlevel một trong các giá trị từ 0 đến 6 như trong bản trên hoặc dùng lệnh $init<runlevel>

3.3. HỆ THỐNG TẬP TIN

Linux hỗ trợ rất nhiều loại hệ thống tập tin như: ext2, ext3, MS-DOS, proc. Hệ thống tập tin cơ bản của Linux là ext2 và ext3 (hiện tại là ext4).Bên cạnh đó, Linux còn hỗ trợ vfat cho phép đặt tên tập tin dài đối với những tập tin MS-DOS và những partition FAT32. Proc là một hệ thống tập tin ảo (/proc) nghĩa là không dành dung lượng đĩa phân phối cho nó. Ngoài ra còn có những hệ thống tập tin khác như iso9660, UMSDOS, Network File System (NFS).

3.3.1. CẤU TRÚC THƯ MỤC HỆ THỐNG



Khái niệm tập tin trong Linux được chia làm 3 loại chính:

- Tập tin chứa dữ liệu bình thường.
- Tập tin thư mục.
- Tập tin thiết bị.

Ngoài ra Linux còn dùng các Link và Pipe như là các tập tin đặc biệt. Xem cấu trúc tập tin hệ thống:

```
[root@localhost ~]# ls -l /
total 98
dr-xr-xr-x.   2 root root  4096 Dec 12 18:40 bin
dr-xr-xr-x.   5 root root  1024 Dec 11 19:54 boot
drwxr-xr-x.   2 root root  4096 Nov 11  2010 cgroup
drwxr-xr-x.  18 root root  3680 Dec 18 19:47 dev
drwxr-xr-x. 115 root root 12288 Dec 18 19:47 etc
drwxr-xr-x.   8 root root  4096 Dec 13 15:09 home
dr-xr-xr-x.  18 root root 12288 Dec 18 14:18 lib
drwx------.   2 root root 16384 Dec 11 19:37 lost+found
drwxr-xr-x.   3 root root  4096 Dec 13 15:19 media
drwxr-xr-x.   2 root root     0 Dec 18 19:47 misc
drwxr-xr-x.   2 root root  4096 Nov 11  2010 mnt
drwxr-xr-x.   2 root root     0 Dec 18 19:47 net
drwxr-xr-x.   2 root root  4096 Nov 11  2010 opt
dr-xr-xr-x. 116 root root     0 Dec 18 19:47 proc
dr-xr-x---.   5 root root  4096 Dec 13 17:11 root
dr-xr-xr-x.   2 root root 12288 Dec 13 15:24 sbin
drwxr-xr-x.   7 root root     0 Dec 18 19:47 selinux
drwxr-xr-x.   2 root root  4096 Nov 11  2010 srv
drwxr-xr-x.  13 root root     0 Dec 18 19:47 sys
drwxrwxrwt.   8 root root  4096 Dec 18 19:47 tmp
drwxr-xr-x.  12 root root  4096 Dec 11 19:38 usr
drwxr-xr-x.  23 root root  4096 Dec 11 19:53 var
```

Đối với Linux, không có khái niệm các ổ đĩa. Toàn bộ các thư mục và tập tin được mount và tạo thành một hệ thống tập tin thống nhất, bắt đầu từ gốc '/'.

Cấu trúc logic của hệ thống file được tạo từ việc ánh xạ các cấu trúc vật lý được tạo ra khi ta cài đặt hệ thống, các thư mục nào không được tạo ra trong quá tình cài đặt thì hệ thống sẽ tự động tạo ra. Các thư mục cơ bản của Linux gồm:

Thư mục	**Chức năng**
/bin, /sbin	Chứa các tập tin nhị phân hỗ trợ cho việc boot và thực thi các lệnh cần thiết
/boot	Chứa linux kernel, file ảnh hỗ trợ load hệ điều hành
/lib	Chứa các thư viện chia sẻ cho các tập tin nhị phân trong thư mục /bin và /sbin, chứa kernel module
/usr/local	Chứa các thư viện, các phần mềm để chia sẽ cho các máy khác trong mạng
/tmp	Chứa các file tạm
/dev	Chứa các tập tin thiết bị (như CDROM, floppy, HDD), và một số file đặc

	biệt khác.
/etc	Chứa các tập tin cấu hình hệ thống
/home	Chứa các thư mục lưu trữ home directory của người dùng
/root	Lưu trữ home directory của root
/usr	Lưu trữ tập tin của các chương trình đã được cài đặt trong hệ thống
/var	Lưu trữ log file, hàng đợi của các chương trình ứng dụng, mailbox của người dùng.
/mnt	Chứa các mount point của các thiết bị được trong hệ thống
/proc	Còn gọi là system file, lưu trữ thông tin về kernel

3.3.2. CÁC THAO TÁC TRÊN FILESYSTEM

Mount và Umount Filesystem

Mount là hình thức gắn kết thiết bị vào một thư mục trong filesystem của Linux, còn gọi là mount point, sau khi mount hoàn tất việc sao chép dữ liệu giữa hệ thống và mount point, tương tự như sao chép dữ liệu giữa hệ thống và thiết bị. Ta có thể mount vào hệ thống các loại thiết bị sau: hda, sda, CDROM, đĩa mềm, usb.

Mount thủ công

- Cú pháp:#mount <tên thiết bị><điểm mount>

Trong đó

- Tên thiết bị: là thiết bị vật lý như: /dev/cdrom (CDROM), /dev/fd0 (đĩa mềm), đĩa cứng /dev/hda1, /dev/sda,…
- Điểm mount là vị trí thư mục, trong cây thư mục, mà bạn muốn mount vào.
- Tùy chọn của Mount:

-v	: cho biết chi tiết
-w	: mount hệ thống tập tin với quyền đọc và ghi
-r	:mount hệ thống tập tin với quyền đọc
-tloại –fs	: xác định hệ thống tập tin đang mount: ext2, ext3,…
-a	: mount tất cả hệ thống tập tin khai báo trong /etc/fstab.
-oremount <fs>	: chỉ định việc mount lại 1 filesystem nào đó

- Ví dụ 3.3.1: các loại mout thiết bị
    - Gắn kết cdrom: #mount /dev/cdrom /mnt/cdrom
    - Gắn kết một hệ thống tập tin: #mount /dev/hda6 /mnt/source
    - Remount filesystem: #mount –o remount /home

Mount tự động

Tập tin /etc/fstab liệt kê các hệ thống cần được mount tự động. Mỗi dòng một hệ thống tập tin tương ứng với một gắn kết. Các cột trong mỗi dòng phân cách nhau bằng khoảng trắng hoặc khoảng tab.

```
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/var              /var                    ext3    defaults        1 2
LABEL=/home             /home                   ext3    defaults        1 2
LABEL=/boot             /boot                   ext3    defaults        1 2
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
LABEL=SWAP-sda5         swap                    swap    defaults        0 0
```

- Cột 1: chỉ ra thiết bị hoặc hệ thống tập tin cần mount
- Cột 2: xác định mount point cho hệ thống tập tin. Đối với các hệ thống tập tin đặc biệt như swap, chúng ta dùng chữ node, có tác dụng làm cho tập tin swap hoạt động như nhìn vào cây thư mục không thấy.
- Cột 3: chỉ ra loại filesystem như: vfat, ext2, ext3,…
- Cột 4: các tùy chọn phân cách nhau bởi dấu phẩy
- Cột 5: xác định thời gian để lệnh dump sao chép hệ thống tập tin. Nếu trường này trống, dump sẽ giả định rằng hệ thống tập tin này không cần backup
- Cột 6: khai báo lệnh fsck biết thứ tự kiểm tra các file hệ thống tập tin khi khởi động hệ thống. Hệ thống tập tin gốc (/) phải có giá trị 1. Tất cả hệ thống tập tin khác phải có giá trị 2. Nếu không khai báo, khi khởi động máy sẽ không kiểm tra tính thống nhất của tập tin.

Umount hệ thống tập tin

Sau khi làm quen với việc gắn những hệ thống tập tin vào cây thư mục Linux, chúng ta có thể loại bỏ một filesystem bằng lệnh umount.

- Cú pháp:#umount <device_name><mount_point>

Lệnh umount có các dạng:

- #umount <thiết bị><điểm mount>: loại bỏ cụ thể một filesystem
- #umount -a: loại bỏ tất cả các filesystem đang mount
- Ví dụ 3.3.2: Loại bỏ tất cả các filesystem đang mount

  #umount -a

3.3.3. CÁC THAO TÁC TRÊN THƯ MỤC

Đường dẫn tuyệt đối

Đường dẫn tuyệt đối là đường dẫn đầy đủ bắt đầu từ thư mục gốc (/) của thư mục. Đường dẫn tuyệt đối là đường dẫn bắt đầu từ thư mục gốc.

- Ví dụ 3.3.3 /home/hv, /usr/local/vd. Txt

Đường dẫn tương đối

Trong một số trường hợp sử dụng các tập tin và thư mục là con của thư mục đang làm việc lúc đó ta sử dụng đường dẫn tương đối. Đường dẫn tương đối là bắt đầu từ thư mục hiện hành. Dấu ". " Chỉ thư mục hiện hành và dấu ".. " chỉ thư mục cha của thư mục hiện hành.

- Ví dụ 3.3.4: $cd.. :Quay về thư mục cha của thư mục hiện hành

Một số lệnh thao tác trên thư mục

a) Lệnh cd: Thay đổi thư mục hiện hành hay di chuyển thư mục
   - Cú pháp: #cd [thư mục]
   - Ví dụ 3.3.5 #cd /etc

b) Lệnh mkdir:Tạo thư mục mới
   - Cú pháp: #mkdir [thư mục]
   - Ví dụ 3.3.6 #mkdir /home/dulieu

c) Lệnh ls: Liệt kê nội dung trong thư mục.
   - Cú pháp:$ls [tùy chọn] [thư mục]

     $ls -x : hiển thị trên nhiều cột

$ls -l : hiển thị chi tiết các thông tin của tập tin

$ls -a :hiển thị tất cả các tập tin kể cả tập tin ẩn

- Ví dụ 3.3.7:$ls -l /etc

```
[root@localhost ~]# ls -l /etc
total 3980
-rw-r--r--  1 root root   15288 May 25  2008 a2ps.cfg
-rw-r--r--  1 root root    2562 May 25  2008 a2ps-site.cfg
drwxr-xr-x  4 root root    4096 Oct 15 02:02 acpi
-rw-r--r--  1 root root      45 Dec  7 03:13 adjtime
drwxr-xr-x  4 root root    4096 Oct 15 01:59 alchemist
-rw-r--r--  1 root root    1512 Apr 25  2005 aliases
.................................................
```

Ý nghĩa các cột từ trái sang phải:

- Cột 1: ký tự đầu tiên "-" chỉ tập tin thường, d chỉ thư mục, l chỉ link và phía sau có dấu -> chỉ tới tập tin thật. Các ký tự còn lại chỉ truy xuất
- Cột thứ 2: chỉ số liên kết đến tập tin này.
- Cột thứ 3, 4: người sở hữu và nhóm sở hữu
- Cột thứ 5: kích thước của tập tin, thư mục
- Cột thứ 6: chỉ ngày giờ chỉnh sửa cuối cùng
- Cột thứ 7: tên tập tin, thư mục

d) Lệnh rmdir: Lệnh rmdir cho phép xóa thư mục rỗng

- Cú pháp:$rmdir [tùy chọn] [thư mục]
- Ví dụ 3.3.8:$rmdir /home/dulieu
- Ví dụ 3.3.9:$cd /home

3.3.4. GIỚI THIỆU TẬP TIN

Các kiểu tập tin

Trên Linux hỗ trợ các kiểu tập tin sau đây:

"-"Tập tin bình thường (file)

"d" Tập tin thư mục (directory)

"b" Thiết bị khối (block device)

"c" Thiết bị ký tự (character device)

"l"Liên kết (link)

“p”Ống (FIFO)

“s”Khe kết nối (socket)

“. ” Tập tin ẩn

Kiểu tập tin không phân biệt bằng phần mở rộng của tên tập tin. Ta có thể xem kiểu tập tin bằng lệnhls -l:

- Ví dụ 3.3.10$ls -l abc

```
-rw-r--r-- 1 root root 0 Jan 19 19:09 abc
```

Giải thích:

Ký tự đầu tiên giúp ta xác định kiểu tập tin

- Tập tin bình thường: ký tự " –"
- Thư mục: ký tự "d"
- Thiết bị khối: ký tự "b"
- Thiết bị ký tự: ký tự "c"
- Liên kết: ký tự "l"
- Ống: ký tự "p"
- Khe kết nối: ký tự " s"
- Tập tin ẩn ". "

Các thao tác trên tập tin

a) Lệnh cat:

Dùng để hiển thị nội dung của tập tin dạng văn bản. Để xem tạp tin chúng ta ta chọn tên tập tin làm tham số.

- Cú pháp: $cat>filename hoặc $cat >>filename

Trong trường hợp này chúng ta sử dụng dấu ">" hay ">>" để theo sau. Nếu tập tin cần tạo đã tồn tại, dâu">" sẽ xóa nội dung của tập tin và ghi nội dung mới vào. Đấu ">>" sẽ ghi nối tiếp nội dung mới vào nội dung cũ của tập tin.

- Ví dụ 3.3.11:$cat > thotinh. txt[ENTER]

```
>toi yeu em den nay chung co the
>toi yeu em am tham khong hy vong
[Ctrl + d: để kết thúc]
```

b) Lệnh more:

Lệnh more cho phép xem nội dng tập tin theo từng trang màn hình.

- Cú pháp: $more <tên tập tin>
- Ví dụ 3.3.12: $more /etc/inittab

c) Lệnh cp:

Lệnh cp cho phép sao chép tập tin

- Cú pháp: $cp <tên tập tin nguồn> <tên tập tin đích>
- Ví dụ 3.3.13:$cp /etc/passwd $HOME/passwd

d) Lệnh mv:

Lệnh mv di chuyển vị trí của tập tin, có thể sử dụng lệnh mv để đổi tên tập tin.

- Cú pháp:$mv <tên tập tin cũ> <tên tập tin mới>
- Ví dụ 3.3.14:$mv $HOME/passwd $HOME/matkhau

e) Lệnh rm:

Lệnh rm cho phép xóa tập tin, thư mục

- Cú pháp:$rm [tùy chọn] <tên tập tin|thư mục>
- Các tùy chọn hay dùng:
  -r:xóa thư mục và tất cả các tập tin và thư mục con
  -l:xác nhận lại trước khi xóa

f) Lệnh locate:

Sử dụng lệnh locate tìm kiếm đơn giản, thực thi nhanh. Ví dụ tìm các file có tên bắt đầu bằng chuỗi *"test"* và kết thúc bởi 1 số từ 0-9

```
[root@localhost ~]# locate test[0-9]
/usr/share/doc/m2crypto-0.16/demo/CipherSaber/cstest1.cs1
/usr/share/doc/pygtk2-2.10.1/examples/glade/test2.glade
/usr/share/tcl8.4/tcltest2.2
/usr/share/tcl8.4/tcltest2.2/constraints.tcl
/usr/share/tcl8.4/tcltest2.2/files.tcl
/usr/share/tcl8.4/tcltest2.2/pkgIndex.tcl
/usr/share/tcl8.4/tcltest2.2/tcltest.tcl
/usr/share/tcl8.4/tcltest2.2/testresults.tcl
```

g) Lệnh find:Cho phép tìm kiếm tập tin thỏa mãn điều kiện

- Cú pháp: $find [thư mục]–name <tên tập tin>

```
[root@localhost ~]# find / -name named
/var/named
/var/named/chroot/var/named
/var/named/chroot/var/run/named
/var/run/named
/usr/sbin/named
/usr/share/doc/bind-9.3.6/sample/var/named
```

```
/usr/share/logwatch/scripts/services/named
/etc/sysconfig/named
/etc/rc.d/init.d/named
/etc/logrotate.d/named
```

h) Lệnh grep:Tìm kiếm chuỗi ký tự trong tập tin ta sử dụng

- Cú pháp:$grep "biểu thức tìm kiếm" <tên tập tin>
- Ví dụ 3.3.15: grep 'root' /etc/passwd

```
[root@localhost ~]# grep 'root' /etc/passwd
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
```

i) Lệnh touch:

Hỗ trợ việc tạo và thay đổi nội dung tập tin

- Cú pháp:[root@localhost ~]#touch [tùy chọn] <tên tập tin>
- Ví dụ 3.3.16: [root@localhost ~]#touch file1. txt file2. txt (tạo hai tập tin file1. txt và file2. txt)

3.3.5. CÁC THAO TÁC THIẾT LẬP QUYỀN TRUY CẬP CHO NGƯỜI DÙNG

Quyền người dùng

Tất cả các tập tin và thư mục của Linux đều có người sở hữu và quyền truy cập và có thể thay đổi các tính chất này. Quyền của tập tin còn cho phép xác định tập tin có phải là một chương trình (application) hay không.

- Ví dụ 3.3.17[root@localhost ~]#ls –l

  -rw-r—r— 1 fido users 163 Dec 7 14: 31 myfile

- Linux cho phép người sử dụng xác định các quyền đọc (read), viết (write) và thực thi (execute) cho từng đối tượng. Có ba dạng đối tượng:
  - **Người sở hữu (the owner)**
  - **Nhóm sở hữu (the group owner)**
  - **Người khác ("other users" hay everyone else).**

Kí tự	r	w	x	r	w	x	r	w	x
Loại tập tin	Owner			Group owner			Other users		

- Quyền hạn truy cập còn có thể biểu diễn dưới dạng số có giá trị tương ứng như sau:

Quyền	Giá trị
Read permission	4
Write permission	2
Execute permission	1

- Ví dụ 3.3.18:Thiết lập quyền read và excute là: 4+1 =5 và read, write và excute: 4+2+1=7

Tổ hợp của ba quyền trên có giá trị từ 0 đến 7.

```
0 or ---: Không có quyền
1 or --x: execute
2 or -w-: write-only (race)
3 or -wr: write và execute
4 or r--: read-only
5 or r-x: read và execute
6 or rw-: read và write
7 or rwx: read, write và execute
```

Như vậy khi cấp quyền trên một tập tin/thư mục, có thể dùng số thập phân gồm ba con số. **Số đầu tiên miêu tả quyền của sở hữu, số thứ hai cho nhóm và số thứ ba cho những người còn lại**.

Các lệnh phân quyền chmd, chown, chgrp

a) Lệnh chmod

Đây là lệnh được sử dụng cấp phép quyền truy cập của tập tin hay thư mục. Chỉ có chủ sở hữu và superuser mới có quyền thực hiện các lệnh này.

- Cú pháp:chmod [nhóm-người-dùng] [thao-tác] [quyền-hạn] [tên-tập-tin].

Nhóm người dùng	Thao tác	Quyền
u user	+ Thêm quyền	r read
g group	• Xóa quyền	w write
o others	= gán quyền bằng	x excute

- Ví dụ 3.3.19: Cấp quyền cho tập tin myfile

Quyền	Lệnh
-wrxr-xr-x	$chmod 755 myfile
-r-xr--r --	$chmod 522 myfile
-rwxrwxrwx	$chmod 777 myfile

b) Lệnh chown

Lệnh chown dùng để thay đổi người sở hữu trên tập tin, thư mục

- Cú pháp:[root@localhost ~]#chown [tên-user:tên-nhóm] [tên-tập-tin/thư-mục] hoặc $chown –R [tên-user:tên-nhóm] [thư-mục]
- Ví dụ 3.3.20**[root@localhost ~]#**chown -R sv1:sinhvien mfile

Dòng lệnh cuối cùng với tùy chọn –R (recursive) cho phép thay đổi người sở hữu của thư mục và tất cả các thư mục con của nó.

c) Lệnh chgrp

Lệnh chgrp dùng để thay đổi nhóm sở hữu của một tập tin, thư mục

- Cú pháp: [root@localhost ~]#chgrp [nhóm-sở-hữu] [tên-tập-tin/thư-mục]
- Ví dụ 3.3.21: **[root@localhost ~]#**chgrp hocvien myfile

3.3.6. CHUẨN CHUYỂN HƯỚNG TRONG LINUX

Chuyển hướng là hình thức thay đổi luồng dữ liệu của cách nhập, xuất và lỗi chuẩn. Khi sử dụng chuyển hướng, nhập chuẩn có thể nhận dữ liệu từ tập tin thay vì bàn phím, xuất và lỗi chuẩn có thể xuất ra tập tin hay máy in. Có ba loại chuyển hướng

Chuyển hướng nhập

Theo quy ước thì các lệnh lấy dữ liệu từ thiết bị nhập chuẩn (bàn phím). Để lệnh lấy dữ liệu từ tập tin chúng ta dùng ky hiệu "<"

- Cú pháp: [root@localhost ~]#lệnh < <tập tin>
- Dấu "<" chỉ hướng chuyển dữ liệu.
- Ví dụ 3.3.22: [root@localhost ~]#cat < abc. txt hay $cat 0< abc. txt

Chuyển hướng xuất

Kết quả của lệnh thông thường được hiển thị ra màn hình. Để xuất kết quả này ra tập tin ta dùng dấu ">"

- Cú pháp:$lệnh > <tên tập tin>
- Ví dụ 3.3.23: liệt kê nội dung thư mục và chuyển kết quả ra tập tin

  $ls -l > ketqua. txt

Để chèn dữ liệu vào cuối tập tin ta dùng dâu ">>" thay cho dấu ">"

- Cú pháp:$lệnh >> <tập tin>
- Ví dụ 3.3.24:$cat a. txt >> b. txt

Đường ống - PIPE

Linux cung cấp cơ chế đường ống cho phép ta có thể đẩy dữ liệu xuất của lệnh này làm dữ liệu nhập của lệnh khác xử lý.

- Ví dụ 3.3.25: $ls -l | more

Kết quả của lệnh ls không xuất ra màn hình mà chuyển cho lệnh more xử lý như dữ liệu đầu vào.

3.3.7. LƯU TRỮ TẬP TIN VÀ THƯ MỤC

Lệnh gzip và gunzip

Gzip dùng để nén tập tin, còn guzip dùng để giải nén các tập tin đã nén.

- Cú pháp:$gzip [tùy chọn]<tên tập tin> hoặc $gunzip [tùy chọn]<tên tập tin>

Gzip tạo tập tin nén với phần mở rộng. gz

- Các tùy chọn dùng cho gunzip và gzip:
  - *-c :chuyển các thông tin ra màn hình*
  - *-d :giải nén, gzip –d tương đượng gunzip*
  - *-h :Hiển thị giúp đỡ*
- Ví dụ 3. 1:$gzip /etc/passwdvà $gunzip /etc/passwd. gz

Lệnh tar

Lệnh này dùng để gom và bung những tập tin /thư mục. Nó sẽ tạo ra một tập tin có phần mở rộng. tar

- Cú pháp:#tar [tùy chọn] <tập tin đích><tập tin nguồn|thư mục nguồn…>
- Tùy chọn:
  - *-cvf :gom tập tin|thư mục*
  - *-xvf :bung tập tin|thư mục*

Tập tin đích :tập tin. tar sẽ được tạo ra

Tập tin nguồn|thư mục nguồn: những tập tin hoặc thư mục cần gom.

- Ví dụ 3. 2:lệnh nén và giải nén với tar

```
#tar    -cvf   /home/backup. tar    /etc/passwd   /etc/group
#tar    -xvf   /home/backup. Tar
```

3.3.8. KHỞI ĐỘNG HỆ THỐNG

Các bước khởi động hệ thống

- Bước 1: khi một máy PC bắt đầu khởi động, bộ xử lý sẽ tìm đến cuối vùng bộ nhớ hệ thống của BIOS và thực hiện các chỉ thị ở đó.
- Bước 2: BIOS sẽ kiểm tra hệ thống, tìm và kiểm tra các thiết bị và tìm kiếm đĩa chức trình khởi động. Thông thường, BIOS sẽ kiểm tra ổ đĩa mềm, hoặc CDROM xem có thể khởi động từ chúng hay không, rồi đến đĩa cứng. Thứ tự của việc kiểm tra các ổ đĩa phụ thuộc vào các cấu hình trong BIOS.
- Bước 3: khi kiểm tra ổ đĩa cứng, BIOS sẽ tìm đến MBR và nạp vào vùng nhớ hoạt động chuyển quyền điều khiển của nó.
- Bước 4: MBR chứa các chỉ dẫn cho biết cách nạp trình quản lý khởi động GRUB/LILO chi Linux hay NTLDR cho windows NT/2000. MBR sau khi nạp trình khởi động, sẽ chuyển quyền điều khiển cho trình quản lý hoạt động.
- Bước 5: boot loader tìm kiếm boot partition và đọc thông tin cấu hình trong grub.conf và hiển thị Operating Systems kernel có sẵn trong hệ thống để cho phép chúng ta lựa chọn OS kernel boot.
- Ví dụ về grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:You have a /boot partition.This means that
#all kernel and initrd paths are relative to /boot/, eg.
#root (hd0,0)
#kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.18-238.el5)
```

```
      root (hd0,0)
      kernel /vmlinuz-2.6.18-238.el5 ro root=/dev/VolGroup00/LogVol00 rhgb
quiet
      initrd /initrd-2.6.18-238.el5.img
```

- Bước 6: sau khi chọn kernel boot trong file cấu hình của boot loader, hệ thống tự động nạp chương trinh /sbin/init để kiểm tra hệ thống tập tin. Sau đó đọc file /etc/inittab để xác định mức hoạt động (runlevel). Các Linux runlevel.

Runlevel	Thư mục lưu script	Mô tả module hoạt động
0	/etc/rc.d/rc0.d	Chế độ tắt hệ thống
1	/etc/rc.d/rc1.d	Chế độ đơn người dùng, cho phép hiệu quả chỉnh sự cố hệ thống
2	/etc/rc.d/rc2.d	Chế độ text cho đa người dùng không hỗ trợ NFS
3	/etc/rc.d/rc3.d	Chế độ text cho đa người dùng, hỗ trợ đầy đủ
4	/etc/rc.d/rc4.d	Không sử dụng
5	/etc/rc.d/rc5.d	Sử dụng cho nhiều người dùng, cung cấp giao diện đồ họa
6	/etc/rc.d/rc6.d	Reboot hệ thống

- Bước 7: sau khi xác định runlevel thông qua khai báo initdefault, chương trình /sbin/init sẽ thực thi các file startup script được đặt trong các thư mục con của thư mục /etc/rc.d script chỉ định cho từng renlevel 0→6 để xác định thư mục chứa file script chỉ định cho từng runlevel như: /etc/rc.d/rc0.d → /etc/rc.d/rc6.d. File script trong thư mục /etc/rc.d/rc3.d/

Lưu ý: tập tin bằng đầu bằng từ khóa "S" có nghĩa tập tin này sẽ được thực thi lúc khởi động hệ thống, ngược lại tập tin bắt đầu bằng từ khóa "K" nghĩa là tập tin đó được thực thi sau khi hệ thống shutdown, số theo sau các từ khóa "S" và "K" để chỉ định trình tự khởi động script, kế tiếp là tên file script cho từng dịch vụ.

- Bước 8: Nếu như ở Bước 4 runlevel 3 được chọn thì hệ thống sẽ chạy chương trình login để yêu cầu đăng nhập cho từng user trước khi sử dụng hệ thống, nếu runlevel 5 được chọn thì hệ thống load X teminal GUI aplication để yêu cầu đăng nhập cho từng người dùng.
- Để xem các thông tin chi tiết về quá trình khởi động hệ thống ta dùng lệnh #dmesg|less.

Bảo mật cho grub

Để đặt mật khẩu cho GRUB ta chỉ cần mở file /etc/grub/grub.conf để mô tả thêm thông tin password <ký tự mật khẩu>

Nếu ta tạo mật khẩu ở dạng mã hóa thì ta mô tả dòng:Password –md5 PASSWORD

Sau đó tạo mật khẩu mã hóa bằng lệnh md5scrypt

- Ví dụ 3.3.26: Chạy shell grub và nhập mật khẩu:

```
Grub> md5crypt
Password: **********
Encrypted:$1$U$jkxFefdxWH6vppCUSl
b
```

- Sau đó cắt và dán mật khẩu đã được mã hóa trên vào dòng khai báo trong file cấu hình:

Tắt và khởi động hệ thống

- Để shutdown hệ thống ta thực hiện lệnh sau:

```
#init 0                  :khởi động hệ thống ngay lập tức
#shutdown   -hy   t      :hệ thống sẽ shutdown sau t giây
#halt :tương tự như init 0
#poweroff
```

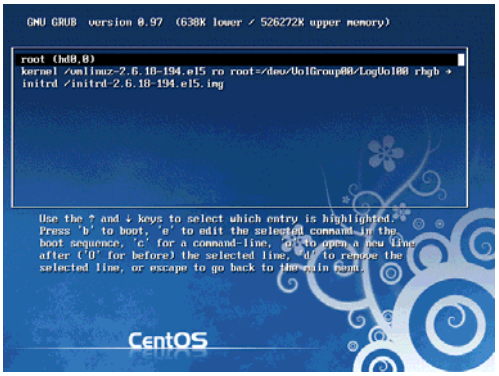
- Để reboot hệ thống ta thực hiện những một trong những lệnh sau:

```
#init 6
#reboot
#shutdown   -ry   10     :hệ thống khởi động lại trong 10 giây
```

Phục hồi mật khẩu cho người dùng quản trị

Để phụ hồi mật khẩu cho người dùng quản trị, ta thực hiện theo các bước sau:

- Khởi động lại máy Linux
- Khi GRUB Screen hiển thị chọn phím e để thay đổi thông tin boot loader (nếu boot loader có mật khẩu thì nhập mật khẩu vào)



- Chọn mục kernel /boot/vnlinux-2.6.18……Sau đó chọn phím e để thay đổi thông tin mục này, thêm từ khóa –s để vào chế độ đơn người dùng (single user) sau đó chọn phím Enter
- Nhấn phím b để tiếp tục khởi động, sau đó thực hiện lệnh passwd để thay đổi mật khẩu của người dùng root

```
Remounting root filesystem in read-write mode:          [  OK  ]
Mounting local filesystems:                             [  OK  ]
Enabling local filesystem quotas:                       [  OK  ]
Enabling /etc/fstab swaps:                              [  OK  ]
sh-3.2# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
sh-3.2# _
```

- Dùng lệnh init 6 để khởi động lại hệ thống

3.4. QUẢN TRỊ SYSTEM SERVICES

3.4.1. XINETD

Cấu hình xinetd

Mỗi dịch vụ Internet đều gắn liền với một cổng chẳng hạn như: smtp – 25, pop3 – 110, dns-53... Việc phân bổ này do một tổ chức qui định.

Xinetd là một Internet server daemon. Xinetd quản lý tập trung tất cả các dịch vụ Internet. Xinetd quản lý mỗi dịch vụ tương ứng với một cổng(port). Xinetd lắng nghe và khi nhận được một yêu cầu kết nối từ các chương trình client, nó sẽ đưa yêu cầu đến dịch vụ tương ứng xử lý. Và sau đó, Xinetd vẫn tiếp tục lắng nghe những yêu cầu kết nối khác. Khi hệ điều hành được khởi động, Xinetd được khởi tạo ngay lúc này bởi script /etc/rc.d/init.d/xinetd. Khi Xinetd được

khởi tạo, nó sẽ đọc thông tin từ tập tin cấu hình /etc/xinetd.conf và sẽ dẫn đến thư mục /etc/xinetd - nơi lưu tất cả những dịch vụ mà Xinetd quản lý. Trong thư mục /etc/xinetd, thông tin cấu hình của mỗi địch vụ được lưu trong một tập tin có tên trùng với tên dịch vụ đó.

- Ví dụ 3.4.1:Nội dung tập tin của dịch vụ telnet

```
service telnet
{
disable = yes
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
}
```

- Ý nghĩa các tùy chọn trong tập tin /etc/xinetd/telnet

Tên	Ý nghĩa
Disable	Tạm đình chỉ dịch vụ này. Có 2 giá trị: yes và no
Socket_type	Loại socket. Trong trường hợp này là stream, stream là một loại socket cho những kết nối connection-oriented chẳng hạn tcp
Wailt	Thường chỉ liên quan đến những kết nối có loại socket là datagram. Giá trị của nó có thể là nowailt, diều này có nghĩa là xinetd sẽ tiếp tục nhận và xử lý những yêu cầu khác trong lúc xử lý kết nối này. Hoặc có thể wailt nghĩa là tại một thời điểm xinetd chỉ có thể xử lý một kết nối tại một cổng chỉ định.
User	Chỉ ra user chạy dịch vụ này. Thông thường là root
Server	Chỉ ra đường dẫn đầy đủ đến nơi quản lý dịch vụ

Tập tin /etc/services

Khi xinetd được khởi tạo nó sẽ truy cập đến tập tin /etc/services để tìm cổng tương ứng với từng dịch vụ. Nội dung của tập tin này như sau:

```
echo        7/tcp
echo        7/udp
discard     9/tcp             sink null
discard     9/udp       sink null
systat      11/tcp      users
systat      11/udp      users
```

```
daytime     13/tcp
daytime     13/udp
qotd        17/tcp      quote
qotd        17/udp      quote
msp         18/tcp      # message send protocol
msp         18/udp      # message send protocol
chargen     19/tcp      ttytst            source
chargen     19/udp      ttytst            source
ftp-data    20/tcp
ftp-data    20/udp
ftp         21/tcp
ftp         21/udp      fsp fspd
ssh         22/tcp      # SSH Remote Login Protocol
ssh         22/udp      # SSH Remote Login Protocol
telnet      23/tcp
telnet      23/udp
smtp        25/tcp      mail
smtp        25/udp      mail
time        37/tcp      timserver
time        37/udp      timserver
rlp         39/tcp      resource # resource location
rlp         39/udp      resource # resource location
nameserver 42/tcp       name # IEN 116
nameserver 42/udp       name # IEN 116
```

Mỗi dòng trong tập tin mô tả cho một dịch vụ, bao gồm những cột sau:

- *Cột 1: tên của dịch vụ.*
- *Cột 2: số cổng và giao thức mà dịch vụ này hoạt động.*
- *Cột 3: danh sách những tên gọi khác của dịch vụ này.*

3.4.2. CẤU HÌNH TELNET

Trước khi cấu hình telnet, chúng ta phải cài đặt telnet trước. Có nhiều cách cấu hình telnet server, sau đây là hai cách cấu hình cơ bản nhất:

Cách 1:

- Dựa vào tập tin cấu hình khi cài đặt xong trong thư mục /etc/xinetd.d sẽ xuất hiện tập tin telnet. Tập tin này lưu những thông tin cấu hình về dịch vụ telnet.

```
service telnet
{
disable = yes
flags = REUSE
socket_type = stream
```

```
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
}
```

nếu disable = NO thì TELNET server được khởi động, ngược lại nếu disable = yes thì TELNET server không được khởi động.

- Khởi động xinetd bằng lệnh:

```
#/etc/rc.d/init.d/xinetd start
#/etc/rc.d/init.d/xinetd stop
```

Hoặc dùng lệnh:

```
# service xinetd start
# service xinetd stop
# service xinetd restart
```

Cách 2: Cấu hình telnet Server bằng dòng lệnh

- Dùng lệnh chkconfig để active telnet:

```
# chkconfig telnet on
```

- Kiểm tra telnet thông qua lệnh:

```
#netstat -a|grep telnet
tcp 0 0 *:telnet *:* LISTEN
```

- Kiểm tra telnet có được đặt như dịch vụ hệ thống:

```
# chkconfig --list | grep telnet
 telnet: on
```

Tạm ngưng hoạt động telnet server dùng lệnh

```
# chkconfig telnet off
```

3.4.3. **BẢO MẬT DỊCH VỤ TELNET**

Cho phép Telnet Server hoạt động trên TCP PORT khác

Như ta đã biết Telnet Traffic không được mã hóa do đó nếu ta cho telnet server hoạt động trên tcp port 23 thì không được an toàn vì thế ta có thể đặt telnet server hoạt động trên tcp port khác 23. để làm điều này ta thực hiện các bước sau:

- Bước 1. Mở tập tin /etc/services và thêm dòng.

```
stelnet 7777/tcp
```

- Bước 2. Chép file telnet thành file stelnet.

```
# cp /etc/xinetd.d/telnet /etc/xinetd.d/stelnet
```

- Bước 3. Thay đổi một số thông tin trong file /etc/xinetd.d/stelnet

```
service stelnet
{
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
disable = no
port = 7777
}
```

- Bước 4. Kích hoạt stelnet thông qua lệnh chkconfig

```
# chkconfig stelnet on
```

- Bước 5. Kiểm tra hoạt động stelnet thông qua lệnh netstat.

```
# netstat -an | grep 777
tcp 0 0 0.0.0.0:7777 0.0.0.0:* LISTEN
```

- Ta có thể logon vào stelnet server thông qua lệnh:

```
# telnet 192.168.1.100 7777
```

Cho phép một số địa chỉ truy xuất telnet

Hiệu chỉnh thông số only_from để cho phép một số host hoặc network truy xuất vào TELNET Server.

```
service telnet
{
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
disable = no
only_from = 192.168.1.100 127.0.0.1 192.168.1.200
}
```

3.4.4. SECURE REMOTE ACCESS – SSH (SECURE SHELL)

Chương trình telnet trong Linux cho phép người dùng đăng nhập vào hệ thống Linux từ xa. Khuyết điểm của chương trình này là tên người dùng và mật khẩu gởi qua mạng không được mã hóa. Do đó, nó rất dễ bị những người khác nắm giữ và sẽ là mối nguy hiểm cho hệ thống.

Phần mềm Secure Remote Access là một sự hỗ trợ mới của Linux nhằm khắc phục nhược điểm của telnet. Nó cho phépđăng nhập vào hệ thống Linux từ xa và mật khẩu sẽ được mã hóa. Vì thế, nó an toàn hơn telnet.

Cài đặt SSH server

```
[root@localhost ~]# yum -y install openssh
--> Running transaction check
--> Processing Dependency: openssh = 5.3p1-20.el6 for package: openssh-
server-5.3p1-20.el6.i686
---> Package openssh.i686 0:5.3p1-52.el6_1.2 set to be updated
--> Running transaction check
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
 Package         Arch       Version           Repository     Size
================================================================================
Updating:
 openssh        i686       5.3p1-52.el6_1.2   updates       235 k
Updating for dependencies:
……….
Transaction Summary
================================================================================
Install       0 Package(s)
Upgrade       4 Package(s)
Total download size: 939 k
Downloading Packages:
(1/4): openssh-5.3p1-52.el6_1.2.i686.rpm                | 235 kB     00:00
(2/4): openssh-askpass-5.3p1-52.el6_1.2.i686.rpm        |  49 kB     00:00
(3/4): openssh-clients-5.3p1-52.el6_1.2.i686.rpm        | 360 kB     00:00
--------------------------------------------------------------------------------
Total                                          1.8 MB/s | 939 kB     00:00
warning: rpmts_HdrFromFdno: Header V3 RSA/SHA1 Signature, key ID c105b9de:
NOKEY
updates/gpgkey                                          | 3.3 kB     00:00
...
```

```
Importing GPG key 0xC105B9DE "CentOS-6 Key (CentOS 6 Official Signing Key)
<centos-6-key@centos.org>" from /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating       : openssh-5.3p1-52.el6_1.2.i686            1/8
  Updating       : openssh-clients-5.3p1-52.el6_1.2.i686    2/8
……
  Cleanup        : openssh-clients-5.3p1-20.el6.i686        7/8
  Cleanup        : openssh-5.3p1-20.el6.i686                8/8
Updated:
  openssh.i686 0:5.3p1-52.el6_1.2
Dependency Updated:
  openssh-askpass.i686 0:5.3p1-52.el6_1.2
  openssh-clients.i686 0:5.3p1-52.el6_1.2
  openssh-server.i686 0:5.3p1-52.el6_1.2
Complete!
```

Hoặc cài đặt openssh từ file nhị phân như sau:

- Cài đặt SSH Server ta dùng lệnh: #rpm –ivh openssh-server.*.rpm

Khởi tạo SSH Server

Dùng lệnh sau: `#/etc/init.d/sshd start/stop/restart`

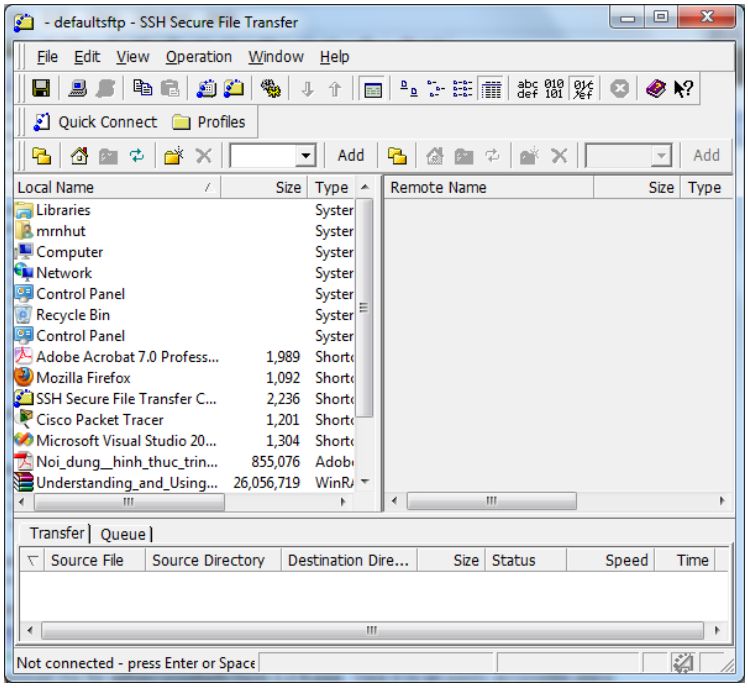
Hoặc khởi động ssh mỗi khi hệ thống khởi động bằng lệnh: `#chkconfig  sshd on`

Sử dụng SSH Client trên Linux

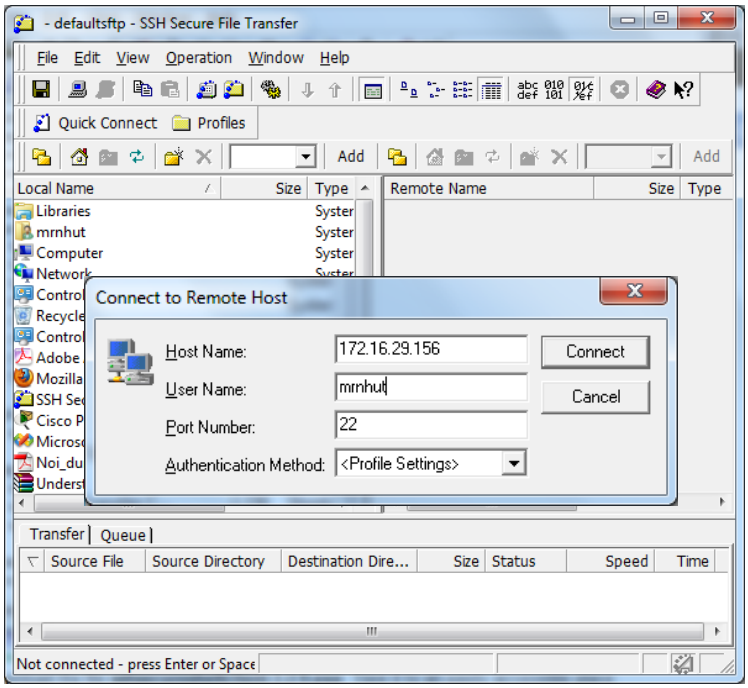
- Cú pháp:#ssh [tùy_chọn] [tên/IP_máy] [tùy_chọn] [lệnh]
- Ví dụ 3.4.2: `#ssh –l root 10.8.1.1`

Sử dụng SSH client trên Windows

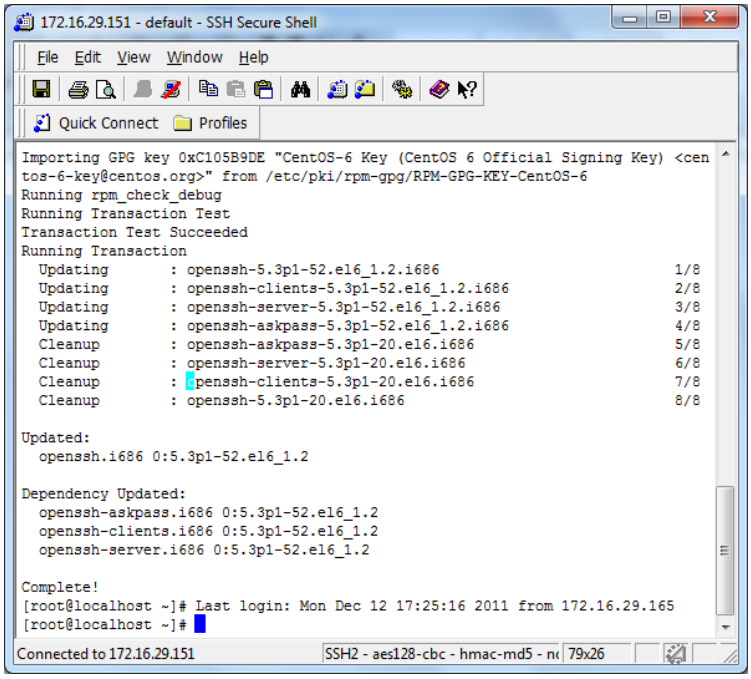
SSH client for Windows được thiết kế để cho phép người dùng có thể sử dụng/quản trị Unix/Linux từ hệ điều hành Windows. Ta có thể download phần mềm này từ site: http://www.ssh.com/support/downloads/ hoặc tải phần mềm sshsecureshellclient-3.2.9.exe hoặc mới hơn giành cho Windows. Phần mềm này hỗ trợ cho người dùng có thể làm việc từ xa, cung cấp dịch vụ sftp. Màn hình "SSH Client for Windows" như:



Click chuột vào nút "Quick Connect" sau đó nhập địa chỉ IP của máy SSH Server như hình sau:



Nhấn nút "new terminal windows" để đăng nhập giao diện dòng lệnh



3.5. CÂU HỎI ÔN TẬP

Đăng nhập vào hệ thống Linux và thực hiện các yêu cầu sau:

1. Hãy tạo các nhóm và người dùng sau
    a. Giamdoc(gd1, gd2)
    b. Nhansu(ns1, ns2)
    c. Kinhdoanh(kd1, kd2)
2. Thư mục home dir của người dùng được đặt tại /home/
3. Tạo thư mục /public, cấp quyền sao cho mọi người dùng được toàn quyền ghi dữ liệu, nhưng dữ liệu của người nào thì người đó mới được quyền thay đổi.
4. Cho phép mỗi người dùng được lưu tối đa 1GB trong home dir của mình.
5. Cho biết có bao nhiêu người dùng có UID=0, GID=0. Dùng vi ghi nhận danh sách những người dùng này vào tập tin /baitap/dsuser.
6. So sánh GID của từng người dùng root, bin, daemon trong tập tin /etc/passwd với GID của những nhóm root, bin, daemon trong tập tin /etc/group. Có nhận xét gì về tên của người dùng và tên của nhóm?
7. Tạo các nhóm sau: **hocvien, admin, user.**
    a. Trong nhóm hocvien tạo các người dùng:
        i. hv1 có mật khẩu 123456
        ii. hv2 có mật khẩu 123456

iii. hv3 có mật khẩu 123456

b. Trong nhóm admin tạo các người dùng:
   i. admin1 có mật khẩu 123456
   ii. admin2 có mật khẩu 123456

c. Trong nhóm user tạo các người dùng:
   i. user1 có mật khẩu 123456
   ii. user2 có mật khẩu 123456

8. Có nhận xét gì về những UID của các người dùng vừa tạo.
9. Cấp cho người dùng admin1 và admin2 có quyền quản trị hệ thống như người dùng root.
10. Hủy người dùng hv3 trong nhóm hocvien.
11. Chỉnh sửa thông tin trong phần mô tả (description) của người dùng admin1 và admin2 là "Người dùng quan tri he thong" để phân biệt với những người dùng khác trong hệ thống.
12. Chuyển người dùng user1 trong nhóm user sang nhóm hocvien.
13. Khóa user1 và user2, sau đó kích hoạt cho user được quyền logon vào hệ thống.
14. Chép file /etc/passwd thành file /data/dsuser.
15. Cấp quyền hạn cho tập tin /data/dsuser như sau: chủ sở hữu có quyền đọc, ghi; nhóm sở hữu có quyền đọc; những người khác không có quyền truy cập.
16. Cấp quyền hạn cho thư mục /baitap như sau: người sở hữu có quyền đọc, ghi, thực thi; nhóm sở hữu có quyền đọc, thực thi; những người khác không có quyền truy cập.
17. Tạo quyền hạn mặc định cho tập tin như sau: người sở hữu có quyền đọc, ghi; nhóm sở hữu có quyền đọc; những người khác không có quyền. Thử tạo tập tin, thư mục và so sánh quyền hạn mặc định với những tập tin và thư mục trước khi đặt lại quyền hạn mặc định.
18. Thay đổi chủ sở hữu và nhóm sở hữu của tập tin /data/dsuser thành người dùng user1 và nhóm user.
19. Đăng nhập vào Xwindow bằng người dùng quản trị, sao đó dùng công cụ quản lý user trên môi trường đồ họa để thực hiện các công việc sau:
20. Tạo các nhóm sau: hocvien, admin, user.
21. Trong nhóm hocvien tạo các người dùng:
    a. Tung có mật khẩu 123456
    b. Thuy có mật khẩu 123456
    c. Thanh có mật khẩu 123456
22. Trong nhóm admin tạo các người dùng:
    a. Adm1 có mật khẩu 123456

b. ADM2 có mật khẩu 123456

23. Trong nhóm user tạo các người dùng:
    a. U1 có mật khẩu 123456
    b. u2 có mật khẩu 123456
24. Xem và thay đổi các thuộc tính liên quan đến người dùng.
25. Thay đổi nhóm cho người dùng thanh sang nhóm user.
26. Giới hạn ngày sử dụng tài khoản là 2 tháng.
27. Tạm khóa tài khoản u2.
28. Giới hạn thời gian sử dụng mật khẩu.

3.6. HƯỚNG DẪN ÔN TẬP

1) Để chép file /etc/passwd thành file /data/dsuser dùng lệnh cp /etc/passwd /data/dsuser.
2) Để cấp quyền hạn cho tập tin /data/dsuser sao cho: người sở hữu có quyền đọc, ghi; nhóm có quyền đọc; những người khác không có quyền gì cả. Ta dùng lệnh chmod 640 /data/dsuser.
3) Để cấp ấp quyền hạn cho thư mục /baitap sao cho: chủ sở hữu có quyền đọc, ghi, thực thi; nhóm có quyền đọc, thực thi; những người khác không có quyền gì cả. ta dùng lệnh chmod 750 /baitap.
4) Để tạo quyền hạn mặc định cho tập tin sao cho: chủ sở hữu có quyền đọc, ghi; nhóm có quyền đọc; những người khác không có quyền, ta dùng lệnh umask 020. ta tạo file để kiểm tra bằng lệnh touch /data/test.txt, tiếp theo dùng lệnh ls -al /data/test.txt để xem quyền hạn.
5) Dùng lệnh chown user1 /data/dsuser để thay đổi chủ sở hữu và nhóm sở hữu của tập tin /data/dsuser thành người dùng user1. dùng lệnh chgrp user /data/dsuser.

CHƯƠNG 4: QUẢN LÝ DỊCH VỤ MẠNG INTRANET

Nội dung:

- ❖ Các bước cấu hình mạng căn bản
- ❖ Cấu hình cấp phát IP động DHCP

TÓM TẮT

- Phần 4.1: Trình bày các thao tác cấu hình mạng căn bản như: đặt tên máy, quản trị địa chỉ IP, cách thiết lập IP Alias.
- Phần 4.2: Giới thiệu dịch vụ cấp phát IP động (DHCP) gồm: cấu hình DHCP Server và quản lý cấp phát IP cho Client
-

4.1. CẤU HÌNH MẠNG CĂN BẢN

4.1.1. ĐẶT TÊN MÁY

Lệnh hostname cho phép xem và thay đổi tên máy tính (hay thường gọi là hostname).

- Cú pháp:#hostname

Thông tin về tên máy tính được lưu trong tập tin /etc/hosts, cú pháp của file này như sau:

<Địa chỉ ip><hostname ><domainname của hostname>

Khi muốn tên máy được đặt cố định một tên nào đó và tên này sẽ không thay đổi khi ta khởi động lại hệ thống thì ta thay đổi thông số HOSTNAME trong file /etc/sysconfig/network.

```
NETWORKING=yes
HOSTNAME=Server
```

4.1.2. XEM ĐỊA CHỈ IP

Xem thông tin địa chỉ IP của PC ta dùng lệnh ifconfig.

- Cú pháp: #interface<tùy chọn>
- Ví dụ 4.1.1# ifconfig –a

```
[root@localhost ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:CE:68:CF
          inet addr:172.16.29.134  Bcast:172.16.29.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16293 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13247645 (12.6 MiB)  TX bytes:933088 (911.2 KiB)
```

```
          Interrupt:67 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:9240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3120051 (2.9 MiB)  TX bytes:3120051 (2.9 MiB)
```

4.1.3. THAY ĐỔI ĐỊA CHỈ IP

- Cú pháp:#ifconfig <interface_name><IP_address> netmask <netmask_address> up
- Ví dụ 4.1.2:# ifconfig eth0 10.0.0.1 netmask 255.255.255.0 up

Lưu ý: Khi dùng lệnh này thay đổi địa chỉ IP chỉ tạm thời và sẽ bị mất khi hệ thống reboot lại. Nếu muốn thay đổi địa chỉ IP và lưu lại dài lâu thì phải cấu hình mạng trong file /etc/sysconfig/network-scripts/ifcfg-eth0 bằng địa chỉ IP tĩnh

```
DEVICE=eth0
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
IPADDR=172.29.14.150
NETMASK=255.255.255.224
NETWORK=172.29.14.128
BROADCAST=172.29.14.159
HWADDR=00:0C:29:6D:F0:3D
```

Nếu đặt địa chỉ IP động thì:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Sau đó ta dùng lệnh: #ifdown eth0, #ifup eth0 để khởi động lại trạng thái card mạng.

4.1.4. TẠO IP ALIAS

Phương thức tạo nhiều địa chỉ IP trên một card mạng được gọi là IP alias. Alias phải có tên dạng <parent-interface-name>:X, trong đó X là subinterface number. Để tạo Alias IP ta thực hiện theo cách sau:

- Tạo tập tin parent-interface-name:X bằng cách copy file /etc/sysconfig/network-scripts/ifcfg-eth0 thành file /etc/sysconfig/network-scripts/ifcfg-eth0:X (trong đó X là số thứ tự của subinterface)
- Thay đổi thông tin cấu hình mạng trong file ifcfg-eth0:X.

```
DEVICE=eth0:0
ONBOOT=yes
BOOTPROTO=static
IPADDR=172.29.14.151
NETMASK=255.255.255.224
GATEWAY=172.29.129
```

- Dùng lệnh `#service network restart`

4.1.5. THAY ĐỔI DEFAULT GATEWAY

Dùng lệnh route để mô tả, cập nhật địa chỉ default gateway. Ví dụ, ta dùng địa chỉ 172.29.14.150 là default gateway cho hệ thống nội bộ, ta làm như sau:

- Ví dụ 4.1.3:#route add default gw 172.29.14.150

Ta có thể dùng lệnh route add để chỉ định nhiều default gateway:

- Ví dụ 4.1.4#route add -net 10.0.0.0 netmask 255.0.0.0 gw 192.168.1.254 eth0

4.2. CẤP PHÁT IP ĐỘNG (DHCP)

- DHCP cấp cho máy trạm những thông tin mạng trong đó có địa chỉ IP.
- DHCP là một công cụ hữu ích trong việc quản trị những mạng lớn hay mạng có những người dùngdi động.
- DHCP Server: Là máy cấp phát địa chỉ IP cho những máy tính khác trong mạng. Tiến trình của DHCP service là dhcpd.
- DHCP client: Máy nhận địa chỉ IP và những thông tin khác về mạng từ DHCP Server.

4.2.1. CẤU HÌNH DHCP SERVER

Cài đặt phần mềm dhcp

```
[root@localhost ~]# yum -y install dhcp
Setting up Install Process
Resolving Dependencies
--> Running transaction check
```

```
---> Package dhcp.i686 12:4.1.1-19.P1.el6_1.1 set to be updated
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
 Package    Arch  Version     Repository        Size
================================================================================
Installing:
 Dhcp i686  12:4.1.1-19.P1.el6_1.1  updates  894 k
Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)
Total size: 894 k
Installed size: 2.1 M
Running Transaction
  Installing   : 12:dhcp-4.1.1-19.P1.el6_1.1.i686           1/1
Installed:
  dhcp.i686 12:4.1.1-19.P1.el6_1.1
Complete!
```

- Để cấu hình DHCP Server cần phải cài đặt package dhcpd*.rpm bằng RPM hoặc YUM.
- Để cấu hình DHCPcần phải có tập tin cấu hình /etc/dhcpd.conf và chỉnh sửa tập tin này.
- Ví dụ 4.2.1 về nội dung cấu hình chính của tập tin dhcpd.conf

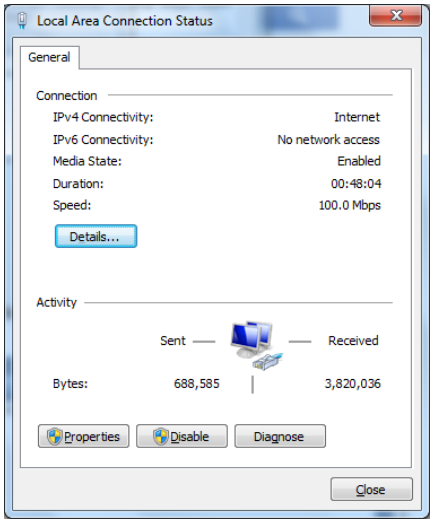
```
ddns-update-style interim; / ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "serverlinux.vn";
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
}
```

4.2.2. **KHỞI ĐỘNG DỊCH VỤ DHCP**

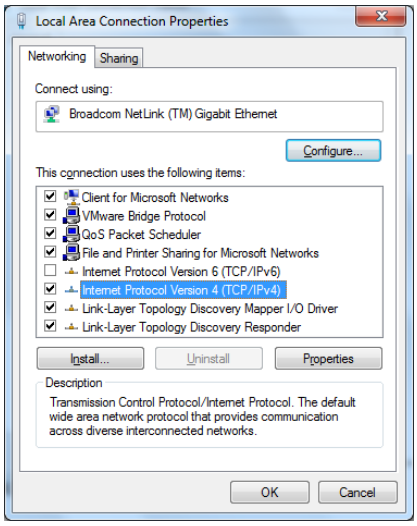
```
Cú pháp:#service dhcpd restart
```

4.2.3. **KIỂM TRA CẤP PHÁT IP CHO CLIENT TRÊN WINDOWS 7**

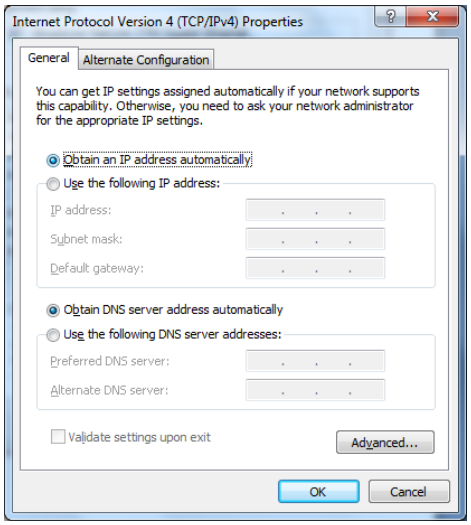
Trên Windows 7 vào Control Panel → vào Local Area Connection có giao diện như bên dưới:



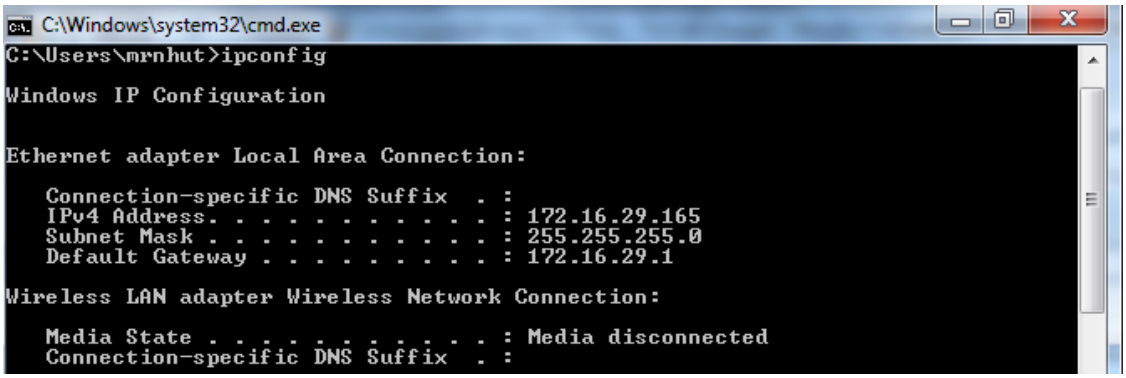
Click chọn nút “Properties”



Click chọn “Internet Protocol Version 4 (TCP/Ipv4) → click nút “Properties” .



Click chọn "Obtain an IP address automatically" để chọn yêu cầu phát IP động→click OK
Sau đó vào RUN, gõ cmd và gõ lệnh ipconfig để kiểm tra việc cấp phát IP từ DHCP server



4.3. CẤU HÌNH CHIA SẺ TÀI NGUYÊN (SAMBA, NFS)

4.3.1. CẤU HÌNH CHIA SẺ SAMBA

Cài đặt samba

```
[root@localhost ~]# yum -y install samba
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package samba.i686 0:3.5.6-86.el6_1.4 set to be updated
……..
  Updating    : libsmbclient-3.5.6-86.el6_1.4.i686           5/9
  Cleanup     : samba-client-3.5.4-68.el6.i686               6/9
  Cleanup     : samba-common-3.5.4-68.el6.i686               7/9
  Cleanup     : libsmbclient-3.5.4-68.el6.i686               8/9
  Cleanup     : samba-winbind-clients-3.5.4-68.el6.i686      9/9
Installed:
  samba.i686 0:3.5.6-86.el6_1.4
Dependency Updated:
  libsmbclient.i686 0:3.5.6-86.el6_1.4   samba-client.i686 0:3.5.6-
86.el6_1.4   samba-common.i686 0:3.5.6-86.el6_1.4  samba-winbind-
clients.i686 0:3.5.6-86.el6_1.4
Complete!
```

Hoặc cài đặt phần mềm samba ở dạng file nhị phân sử dụng RPM

```
[root@localhost ~]#libsmbclient-3.5.6-86.el6_1.4.i686.rpm
[root@localhost ~]#samba-3.5.6-86.el6_1.4.i686.rpm
[root@localhost ~]#samba-client-3.5.6-86.el6_1.4.i686.rpm
```

```
[root@localhost ~]#samba-client-3.5.6-86.el6_1.4.i686.rpm
[root@localhost ~]#samba-common-3.5.6-86.el6_1.4.i686.rpm
[root@localhost ~]#samba-winbind-clients-3.5.6-86.el6_1.4.i686.rpm
```

Cấu hình samba chia sẽ thư mục /home/share

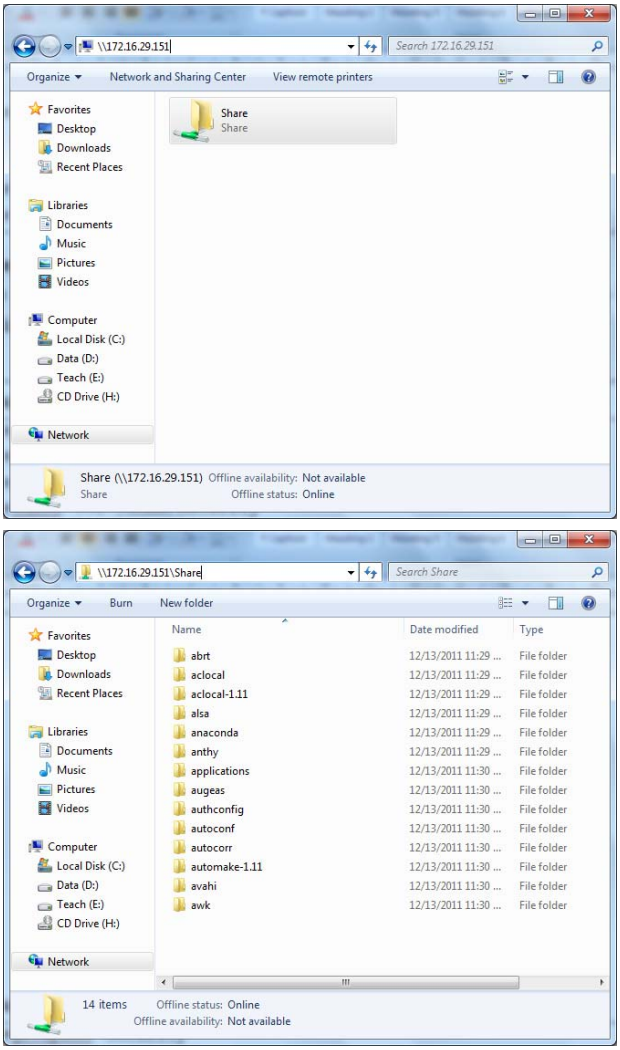
```
[root@linux ~]#mkdir /home/share
[root@linux ~]#chmod 777 /home/share
[root@linux ~]#vi /etc/samba/smb.conf
# Thay đổi dòng gần dòng 58: Thêm vào
unix charset = UTF-8
dos charset = CP932
# Thay đổi dòng 75: (Windows' default)
workgroup = WORKGROUP
# Thay đổi dòng 81: khai báo dãy địa chỉ ip
hosts allow = 127.16.   192.168.          # line 102: change (no auth)
security = share              # add at the bottom
[Share]                  # any name you like
   path = /home/share               # shared directory
   writable = yes             # writable
   guest ok = yes             # guest OK
   guest only = yes                 # guest only
   create mode = 0777               # fully accessed
   directory mode = 0777      # fully accessed
   share modes = yes                # warn if some people access to a file
```

Khởi động lại dịch vụ samba

```
[root@linux ~]# /etc/rc.d/init.d/smb start
Starting SMB services:                             [ OK  ]

[root@linux ~]# /etc/rc.d/init.d/nmb start
Starting NMB services:                             [  OK  ]

[root@linux ~]#chkconfig smb on
[root@linux ~]#chkconfig nmb on
```

Truy cập thư mục /home/share từ Windows

Trong windows vào cmd gõ đường dẫn \\<ip>. Ví dụ máy chia sẽ samba có địa chỉ ip là 172.16.29.151 thì truy cập như hình bên dưới:



Cấu hình giới hạn truy cập samba

```
[root@linux ~]#groupadd security          #Tạo nhóm security
[root@linux ~]#mkdir /home/baomat   #Tạo thư mục security
[root@linux ~]#chgrp security /home/baomat
[root@linux ~]#chmod 770 /home/ baomat
[root@linux ~]#vi /etc/samba/smb.conf
# Thay đổi dòng 102
security = user               # add at the last line
[Security]              # any name you like
   path = /home/data                #chia sẽ thư mục /home/security
   writable = yes             #Thư mục cho phép ghi
   create mode = 0770
   directory mode = 0770      #Cấp quyền truy cập thư mục
```

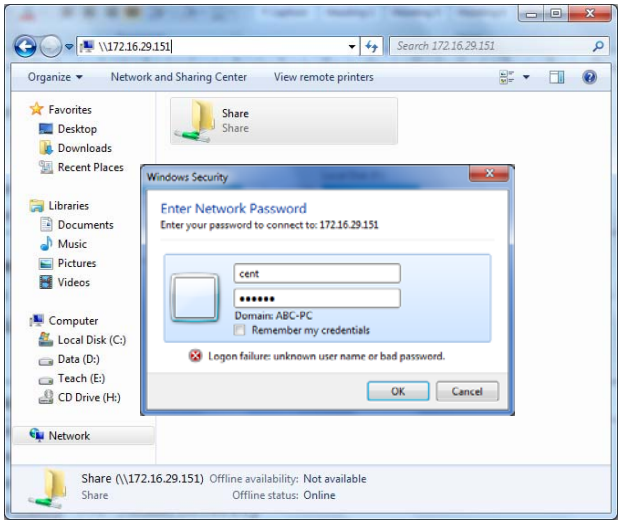
```
   share modes = yes
   guest ok = no                # guest không được phép truy cập
   valid users = @security      # chỉ cho phép nhóm security
```

khởi động lại samba

```
[root@linux ~]#/etc/rc.d/init.d/smb restart
Shutting down SMB services:          [  OK  ]
Starting SMB services:                     [  OK  ]

[root@linux ~]#smbpasswd -a cent     # Thêm user vào Samba
New SMB password:                    # nhập vào password
Retype new SMB password:             # nhập lại password
Added user cent.

[root@linux ~]#vi /etc/group
security:x:502:cent                          # Thêm vào hoặc điền đầy đủ thông
tin
```

Truy cập thư mục /home/data từ Windows

Trong windows vào cmd gõ đường dẫn \\<ip>. Ví dụ máy chia sẽ samba có địa chỉ ip là 172.16.29.151 thì truy cập như hình bên dưới:



Cài đặt và cấu hình Xinetd and SWAT

```
[root@linux ~]#yum -y install xinetd samba-swat
[root@linux ~]#vi /etc/xinetd.d/swat
# Chỉnh sửa dòng 10: add IP address you permit
```

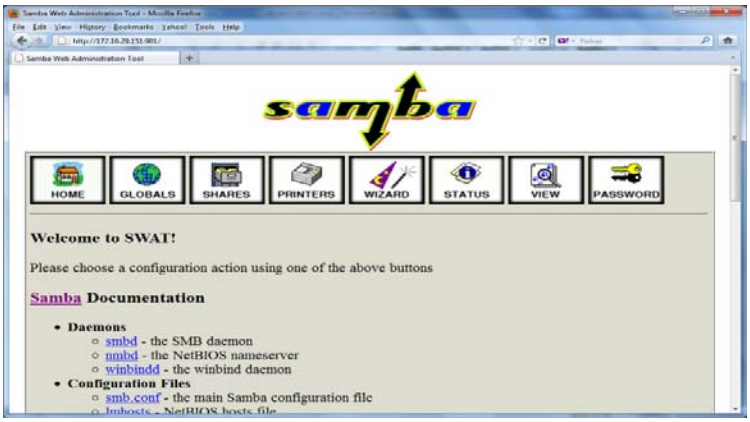
```
only_from = 127.0.0.1   192.168.1.0/24
# Chỉnh sửa dòng 14
disable = no
```

Khởi động lại xinetd

```
[root@linux ~]#/etc/rc.d/init.d/xinetd start
Starting xinetd:        [  OK  ]
[root@linux ~]#chkconfig      xinetd      on
```

Cấu hình samba thông qua SWAT

Truy cập vào swat bằng cách gõ địa chỉ http://(server's hostname or IP address):901vào trình duyệt. Sau đó đăng nhập vào hệ thống với user và mật khẩu.



4.3.2. CẤU HÌNH CHIA SẼ NFS

Cấu hình nfs server

```
[root@linux ~]# yum -y install nfs-utils
[root@linux ~]#vi /etc/idmapd.conf
# Thay đổi dòng 5: uncomment and change to your domain name
Domain = serverlinux
```

Cấu hình tập tin exports

```
[root@linux ~]# vi /etc/exports
# write like below *note
/home 192.168.1.0/24(rw,sync)
```

Trong đó:

- /home #Thư mục chia sẽ
- 192.168.1.0/24 #Dãy địa chỉ mạng cho phép truy cập NFS
- rw #Cho phép write
- sync #Đồng bộ hóa từ client đến server synchronize

Khởi động rpcbind

```
[root@linux ~]# /etc/rc.d/init.d/rpcbind start
Starting rpcbind:                    [  OK  ]
```

Khởi động nfslock

```
[root@linux ~]# /etc/rc.d/init.d/nfslock start
Starting NFS statd:                  [  OK  ]
```

Khởi động nfs

```
[root@linux etc]# /etc/init.d/nfs restart
Shutting down NFS mountd:                                  [  OK  ]
Shutting down NFS daemon:                                  [  OK  ]
Shutting down NFS quotas:                                  [  OK  ]
Shutting down NFS services:                                [  OK  ]
Starting NFS services:                                     [  OK  ]
Starting NFS quotas:                                       [  OK  ]
Starting NFS daemon:                                       [  OK  ]
Starting NFS mountd:                                       [  OK  ]
```

Các dịch vụ khởi động lúc khởi động hệ thống

```
[root@linux ~]# chkconfig rpcbind on
[root@linux ~]# chkconfig nfslock on
[root@linux ~]# chkconfig nfs on
```

Cấu hình nfs client

```
[root@linux ~]# yum -y install nfs-utils  #Cài đặt phần mềm
[root@linux ~]#vi /etc/idmapd.conf
#Thay đổi dòng 5: uncomment và thay đổi tên domain
Domain = serverlinux.vn
```

Khởi động rpcbind, rpcidmapd, nfslock,netfs

```
[root@linux ~]#/etc/rc.d/init.d/rpcbind start
Starting rpcbind:                              [  OK  ]

[root@linux ~]#/etc/rc.d/init.d/rpcidmapd start
Starting RPC idmapd: RPC: Registered udp transport module.
RPC: Registered tcp transport module.
RPC: Registered tcp NFSv4.1 backchannel transport module.   [ OK ]

[root@linux ~]#/etc/rc.d/init.d/nfslock start
Starting NFS statd:                        [  OK  ]

[root@linux ~]#/etc/rc.d/init.d/netfs start
Mounting other filesystems:         [  OK  ]

#khởi động lúc hệ thống khởi động
[root@linux ~]#chkconfig      rpcbind     on
[root@linux ~]#chkconfig      rpcidmapd   on
[root@linux ~]#chkconfig      nfslock     on
[root@linux ~]#chkconfig      netfs             on
```

Mount thư mục /home từ client

```
[root@linux ~]#mount -t nfs   dns1.serverlinux.vn:/home     /home
[root@linux ~]#df -h                 #Kiểm tra thư mục
Filesystem              Size  Used  Avail Use%  Mounted on
/dev/mapper/VolGroup-lv_root  18G   864M  16G   6%    /
Tmpfs             499M  0     499M  0%    /dev/shm
/dev/vda1               485M  47M   413M  11%   /boot
dns1.serverlinux.vn:/home                 18G   864M  16G   6%    /home
```

Khai báo mount point trong /etc/fstab

```
[root@linux ~]#vi /etc/fstab
# Thêm vào dòng cuối cùng của tập tin /etc/fstab
/dev/mapper/VolGroup-lv_root  /           ext4        defaults    1 1
UUID=2078630e-e84a-49e7-af68-55f0bde8d6c3 /boot ext4  defaults    1 2
tmpfs             /dev/shm    tmpfs       defaults    0 0
devpts                  /dev/pts    devpts gid=5,mode=620   0 0
sysfs             /sys        sysfs       defaults    0 0
proc              /proc       proc        defaults    0 0
dns1.serverlinux.vn:/home     /home       nfs         defaults    1 1
```

4.4. CÂU HỎI ÔN TẬP

4.4.1. BÀI TẬP CẤU HÌNH MẠNG

Đăng nhập vào hệ thống bằng người dùng root và thực hiện các yêu sau:

1) Xem tên máy, sau đó đổi tên thành linuxserver1.
2) Xem thông tin về địa chỉ mạng của card eth0 và lo
3) Xem trạng thái vật lý card mạng.
4) Đặt địa chỉ mạng có thông tin sau:
    a. IP: 10.10.10.10
    b. SM: 255.0.0.0
    c. GW: 10.10.10.1
    d. DNS: 10.100.100.254
5) Kiểm tra máy cục bộ có liên thông với máy 10.10.10.1.
6) Thay đổi địa chỉ ip trên thành địa 192.168.100.1/24, gw: 192.168.100.10
7) Để thiết lập địa chỉ IP cho một máy Linux ta sử dụng lệnh nào trong các lệnh nào?
8) Để xem trạng thái các port đang mở của một máy Linuxta sử dụng lệnh nào trong các lệnh nào?
9) Để xem các thông tin về bảng routing trong hệ thống Linux ta sử dụng lệnh nào trong các lệnh nào?
10) Để thiết lập địa chỉ IP cho card mạng eth0 dùng lệnh ifconfig, ta phải thực hiện lệnh nào?
11) Để tạm thời stop một card mạng ta dùng lệnh nào?
12) Giả sử ta muốn thêm vào bảng routing một đường dẫn mới: qua mạng 192.168.10.0/24 thì phải qua gateway 172.16.10.140 ta làm cách nào?
13) Khai báo default gw 172.16.8.2 cho 1 máy Linux làm gw ta dùng lệnh nào?
14) Để xem tải của hệ thống Linux ta dùng lệnh nào?
15) Tập tin nào trong Linux định nghĩa các port cho các dịch vụ chạy trong nó?
16) Dịch vụ SMTP chạy ở port nào?
17) Dịch vụ www chạy ở port nào?
18) Dịch vụ nào cho phép ta truyền file qua mạng?
19) Làm thế nào để login từ xa qua mạng vào một máy Linux?

4.4.2. BÀI TẬP CẤU HÌNH ALIAS, GATEWAY

1) Đăng nhập vào hệ thống bằng người dùng root và thực hiện các yêu cầu sau:

2) Tạo IP Alias cho card mạng eth0 với:
    - Tên interface eth0:0
    - IP address: 192.168.100.100
    - Netmask: 255.255.255.0
    - GW: 192.168.100.1
    - DNS: 192.168.100.1
3) Chỉ định địa chỉ 192.168.100.10 là default route cho hệ thống.
4) Xem thông tin bảng định tuyến và xác định gateway.
5) Xác định các cổng ứng dụng đang hoạt động trên máy nội bộ.

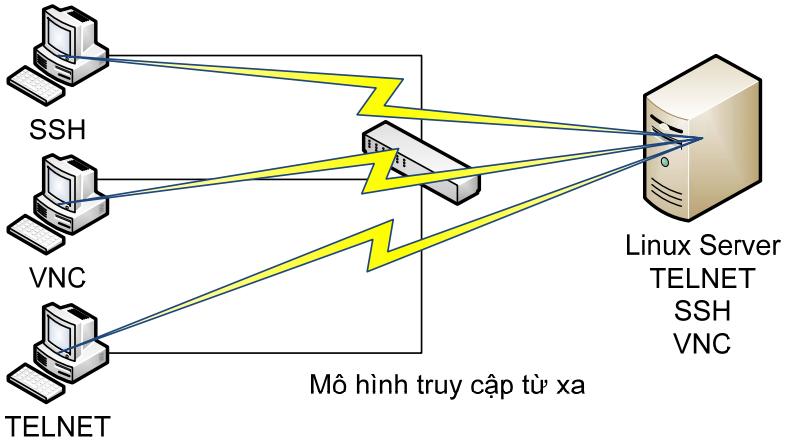
4.4.3. **HƯỚNG DẪN ÔN TẬP**

1. Để chép file /etc/passwd thành file /data/dsuser dùng lệnh cp /etc/passwd /data/dsuser.
2. Để cấp quyền hạn cho tập tin /data/dsuser sao cho: người sở hữu có quyền đọc, ghi; nhóm có quyền đọc; những người khác không có quyền gì cả. Ta dùng lệnh chmod 640 /data/dsuser.
3. Để cấp ấp quyền hạn cho thư mục /baitap sao cho: chủ sở hữu có quyền đọc, ghi, thực thi; nhóm có quyền đọc, thực thi; những người khác không có quyền gì cả. ta dùng lệnh chmod 750 /baitap.
4. Để tạo quyền hạn mặc định cho tập tin sao cho: chủ sở hữu có quyền đọc, ghi; nhóm có quyền đọc; những người khác không có quyền, ta dùng lệnh umask 020. ta tạo file để kiểm tra bằng lệnh touch /data/test.txt, tiếp theo dùng lệnh ls -al /data/test.txt để xem quyền hạn.
5. Dùng lệnh chown user1 /data/dsuser để thay đổi chủ sở hữu và nhóm sở hữu của tập tin /data/dsuser thành người dùng user1. dùng lệnh chgrp user /data/dsuser.

4.4.4. **BÀI TẬP CẤU HÌNH TELNET, SSH**

Đăng nhập vào hệ thống bằng người dùng root và thực hiện các yêu cầu sau:

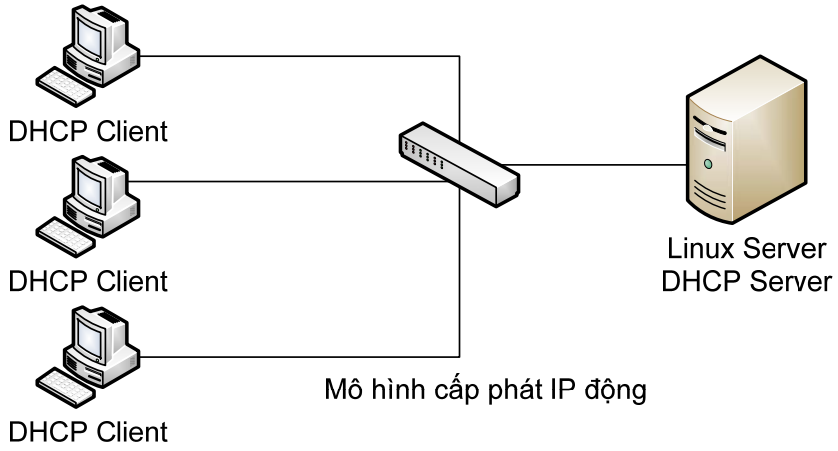
1) Cho phép mọi người có thể truy cập server qua dịch vụ TELNET.
2) Cho phép mọi người truy cập từ xa máy chủ qua dịch vụ SSH



4.4.5. BÀI TẬP CẤU HÌNH DHCP

Hãy đăng nhập vào máy chủ Linux và thực hiện các yêu cầu sau:

1) Thiết lập DHCP server theo các yêu cầu sau:
   - Scope: 192.168.100.50 – 192.168.100.100
   - SM: 255.255.255.0
   - GW: 192.168.100.1
   - DNS: 192.168.100.10
   - Domain: t3h.edu.vn
2) Kiểm tra cổng ứng dụng của DHCP.
3) Xem thông tin thống kê địa chỉ IP đã cấp phát.



4) Hãy cấu hình Linux làm router mềm
5) Thiết lập cơ chế quản lý từ xa cho người quản trị root bằng ssh
6) Thiết lập DHCP server cho máy chủ linux để cấp ip động cho máy chủ cục bộ

CHƯƠNG 05: QUẢN LÝ DỊCH VỤ MẠNG INTERNET

Nội dung

- ❖ Giới thiệu và hướng dẫn cấu hình dịch vụ DNS Server
- ❖ Giới thiệu và hướng dẫn cấu hình dịch vụ Web Server
- ❖

TÓM TẮT

- Phần 5.1: Giới thiệu và hướng dẫn cấu hình dịch vụ mạng DNS bao gồm các thao tác như: Cơ sở dữ liệu của DNS, phân giải tên máy tính thành địa chỉ IP, phân giải địa chỉ IP thành tên máy tính, cấu hình DNS server ngang qua các file, khởi động DNS, kiểm tra cấu hình DNS server, cấu hình slave name server và cấu hình master name server.
- Phần 5.3: Giới thiệu và hướng dẫn cấu hình dịch vụ mạng web server bao gồm các thao tác như: Giới thiệu Web Server, cấu hình Apache cơ bản, cấu hình chứng thực, cấu hình VirtualHost.
-

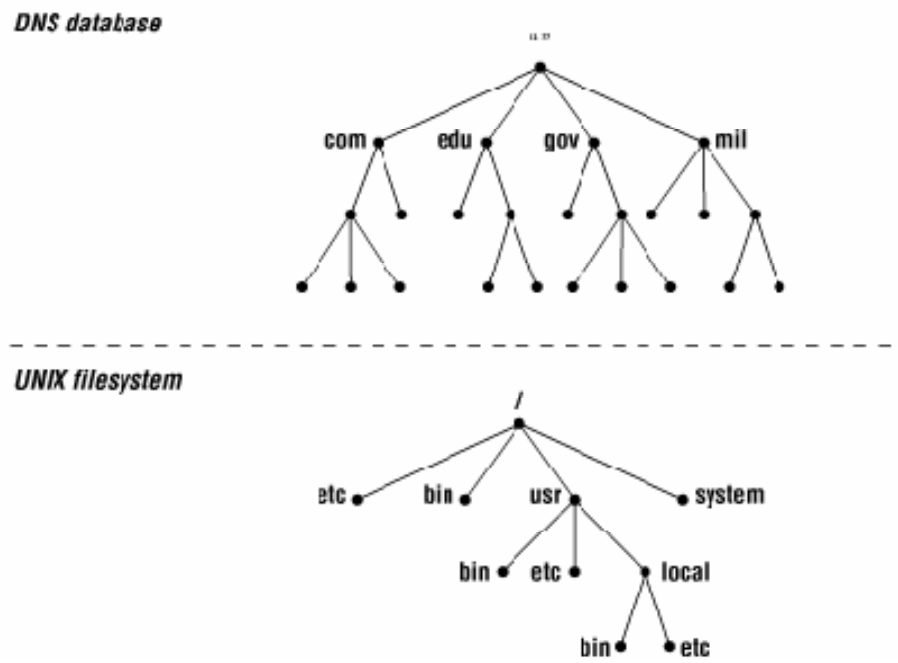
5.1. DỊCH VỤ DNS

5.1.1. GIỚI THIỆU DNS

Mỗi máy tính trong mạng muốn giao tiếp với nhau cần phải biết rõ địa chỉ IP của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ IP này rất là khó khăn. Mỗi máy tính ngoài địa chỉ IP ra còn có một tên máy còn gọi là Computer Name. Đối với con người việc nhớ tên máy dù sao cũng dễ dàng hơn vì chúng có tính trực quan và gợi nhớ hơn địa chỉ IP. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính.

Dịch vụ DNS hoạt động theo mô hình Client-Server: Phần Server gọi là máy chủ phục vụ tên hay còn gọi là Name server, còn phần Client là chương trình trình yêu cầu phân giải tên hay còn gọi là Resolver. Name server chứa các thông tin CSDL của DNS, còn Resolver đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (query) và gửi chúng qua đến Name server.

Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (replication) và lưu tạm (caching). Một hostname trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm. Ví dụ hostname serverlinux.com trong đó serverlinux là tên máy và com là tên vùng. Domain name phân bổ theo cơ chế phân cấp tương tự như sự phân cấp của hệ thống tập tin Unix/Linux.



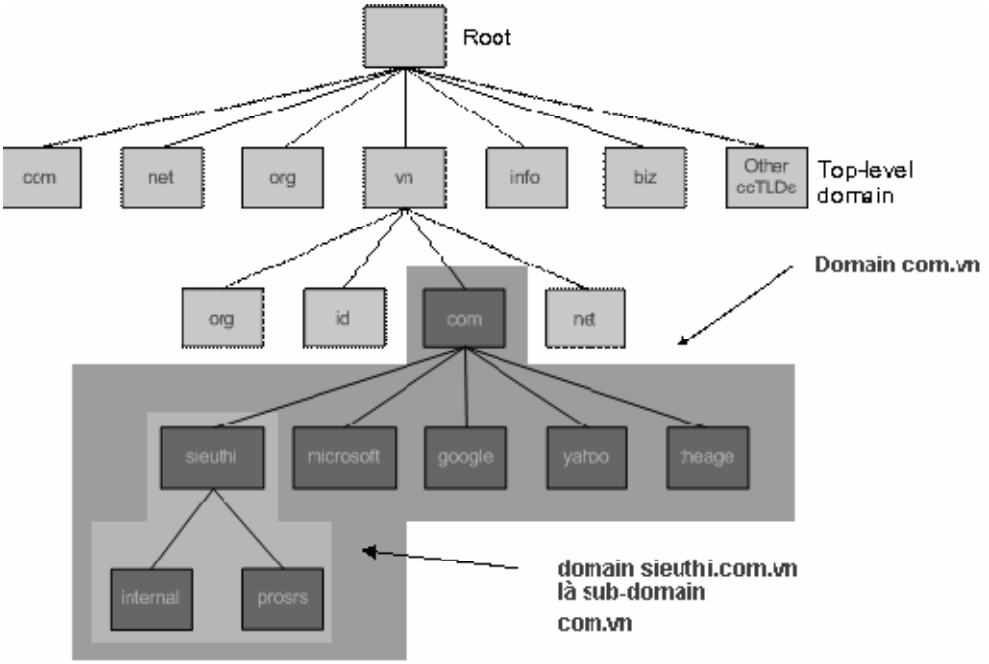
Cơ sở dữ liệu (CSDL) của DNS là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của một cây con. Mỗi cây con là một phân vùng con trong toàn bộ CSDL DNS gọi là một miền (domain). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (subdomain).

Mỗi domain có một tên (domain name). Tên domain chỉ ra vị trí của nó trong CSDL DNS. Trong DNS tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm. Tên nhãn bên phải trong mỗi domain name được gọi là top-level domain. Trong ví dụ trước serverlinux.com, vậy com là top-level domain. Bảng sau đây liệt kê top-level domain.

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Bên cạnh đó, mỗi quốc gia cũng có một top-level domain. Ví dụ top-leveldomain của Việt Nam là.vn, Mỹ là.us, Nhật Bản là.jp,... Mỗi quốc gia khác nhau có cơ chế tổ chức phân cấp domain khác nhau.

- Ví dụ 5.1.1: Tổ chức domain của Việt Nam:

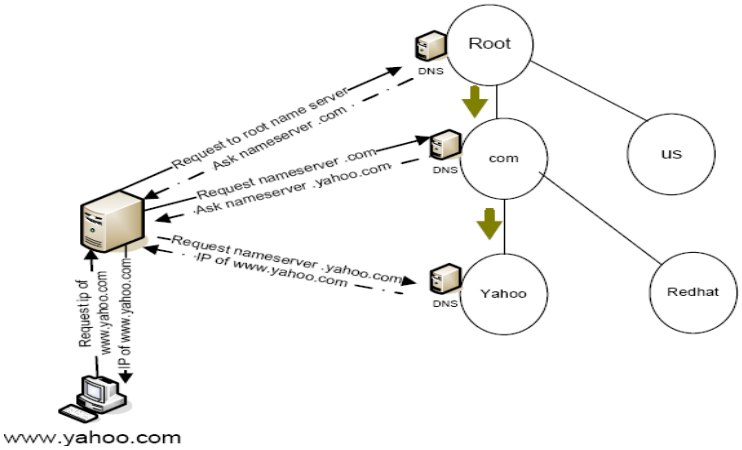


5.1.2. CƠ CHẾ PHÂN GIẢI TÊN

Phân giải tên thành IP

Root Name Server: Là máy chủ quản lý các name server ở mức top-level domain. Khi có truy vấn về một tên miền nào đó thì root name server phải cung cấp tên và địa chỉ IP của name server quản lý top-level domain (Thực tế là hầu hết các root server cũng chính là máy chủ quản lý top-level domain) và đến lượt các nameserver của top-level domain cung cấp danh sách các name server có quyền trên các second-level domain mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

Nếu mọi root name server trên mạng Internet không liên lạc được thì mọi yêu cầu phân giải đều không thực hiện được. Mô hình sau đây mô tả quá trình phân giải www.yahoo.com trên mạng Internet



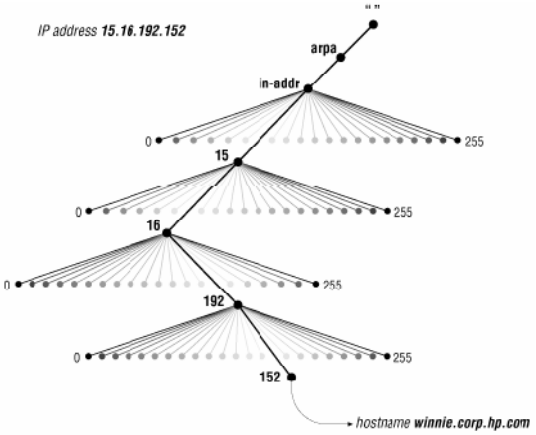
Client sẽ gửi yêu cầu cần phân giải địa chỉ IP của máy tính có tên www.yahoo.com đến name server cục bộ.Khi nhận yêu cầu từ resolver, Name server cục bộ sẽ phân tích tên này và xét xem tên miền này có do mình quản lý hay không. Nếu như tên miền do server cục bộ quản lý, nó sẽ trả lời địa chỉ IP của tên máy đó ngay cho resolver. Ngược lại, server cục bộ sẽ truy vấn đến một root name server gần nhất mà nó biết được. Root name server sẽ trả lời địa chỉ IP của name server quản lý miền.com, Máy chủ name server cục bộ lại hỏi tiếp name server quản lý miền.com và được tham chiếu đến máy chủ quản lý miền.yahoo.com. Name server cục bộ truy vấn máy chủ quản lý miền yahoo.com và nhận được câu trả lời www.yahoo.com tương ứng ip cụ thể.

Phân giải IP thành tên

Ánh xạ địa chỉ IP thành tên máy tính được dùng để diễn dịch các tập tin log cho dễ đọc hơn. Nó còn dùng trong một số trường hợp chứng thực trên hệ thống UNIX (kiểm tra các tập tin.rhost hay host.equiv). Trong không gian tên miền đã nói ở trên dữ liệu -bao gồm cả địa chỉ IP- được lập chỉ mục theo tên miền. Do đó với một tên miền đã cho việc tìm ra địa chỉ IP khá dễ dàng.

Để có thể phân giải tên máy tính của một địa chỉ IP, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ IP. Phần không gian này có tên miền là in-addr.arpa.

Mỗi nút trong miền in-addr.arpa có một tên nhãn là chỉ số thập phân của địa chỉ IP. Ví dụ miền in-addr.arpa có thể có 256 subdomain, tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi subdomain lại có 256 subdomain con nữa ứng với byte thứ hai. Cứ như thế và đến byte thứ tư có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ IP tương ứng.



Lưu ý khi đọc tên miền địa chỉ IP sẽ xuất hiện theo thứ tự ngược. Ví dụ nếu địa chỉ IP của máy winnie.corp.hp.com là 15.16.192.152, khi ánh xạ vào miền in-addr.arpa sẽ là 152.192.16.15.in-addr.arpa.

5.1.3. CÁC LOẠI RECORD

SOA(Start of Authority)

Trong mỗi tập tin CSDL phải có một và chỉ một record SOA (start of authority). Record SOA chỉ ra rằng máy chủ name server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.

- Cú pháp của record SOA:

```
[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email] (
                        serial number;
                        refresh number;
                        retry number;
                        experi number;
                        Time-to-live number);
```

- Ví dụ 5.1.2: Cách khai báo ZONE record SOA

```
serverlinux.com. IN SOA dnsserver.serverlinux.com. root.serverlinux.com. (
                        2005040401; Serial
                        10800; Refresh after 3 hours
                        3600; Retry after 1 hour
                        604800; Expire after 1 week
                        86400 ); Minimum TTL of 1 day
```

NS (Name server)

Record tiếp theo cần có trong zone là NS (name server) record. Mỗi name server cho zone sẽ có một NS record.

- Cú pháp:[tên-domain] IN NS [DNS-Server]
- Ví dụ 5.1.3: Phân giải NS

```
serverlinux.com. IN NS dnsserver.serverlinux.com.
serverlinux.com. IN NS serverlinux.com.
```

Khai báo trên chỉ ra hai name server quản lý dữ liệu cho miền serverlinux.com là dnsserver.serverlinux.com và serverlinux.com.

A (Address) và CNAME (Canonical Name)

Record A (Address) ánh xạ tên máy (hostname) thành địa chỉ IP. Record CNAME (canonical name) tạo tên bí danh alias trỏ vào một tên hostname khác. Tên hostname khác là tên host trong có chỉ định địa chỉ IP thông qua record A hoặc lại trỏ vào một tên alias (canonical) khác.

- Cú pháp khai báo record A:#[hostname] IN A [IP_Address]
- Cú pháp khai báo record CNAME:#[Canonical_name] IN CNAME [hostname | Canonical_name]
- Ví dụ 5.1.4:Ví dụ cấu hình với Record A và CNAME

```
localhost.serverlinux.com.    IN A 127.0.0.1
dnsserver.serverlinux.com.    IN A 172.29.14.2
serverlinux.com.              IN A 172.29.14.1
diehard.serverlinux.com.      IN A 172.29.14.4
// khai báo một tên hostname ánh xạ cho nhiều địa chỉ IP
serverlinux.com.  IN    A     172.29.14.1
serverlinux.com.  IN    A     192.253.253.1

// Khai báo alias name (canonical name)
www.serverlinux.com.    IN    CNAME       serverlinux.com.
proxy             IN    CNAME       www.serverlinux.com.
```

MX (Mail Exchange)

DNS dùng record MX trong việc chuyển mail trên mạng Internet. Khi nhận được mail, trình chuyển mail (mailer) sẽ dựa vào record MX để quyết định đường đi của mail. Record MX chỉ ra một Mail Exchanger cho một miền - Mail Exchanger là một máy chủ xử lý (chuyển mail đến mailbox cục bộ hay làm gateway chuyển sang một giao thức chuyển mail khác như UUCP) hoặc chuyển tiếp mail đến một Mail Exchanger khác (trung gian) gần với mình nhất để đến tới máy chủ đích cuối cùng dùng giao thức SMTP (Simple Mail Transfer Protocol).

Để tránh việc gửi mail bị lặp lại, record MX có thêm một giá trị bổ sung ngoài tên miền của Mail Exchanger là một số thứ tự tham chiếu. Đây là giá trị nguyên không dấu 16-bit (0-65535) chỉ ra thứ tự ưu tiên của các Mail Exchanger.

- Cú pháp: [domain_name] IN MX [priority] [mail_host]
- Ví dụ 5.1.5: serverlinux.com. IN MX 10 mailserver.serverlinux.com.

Chỉ ra máy chủ mailserver.serverlinux.com là mail server quản lý mail cho miền serverlinux.com với số thứ tự tham chiếu 10.

Chú ý: các giá trị này chỉ có ý nghĩa so sánh với nhau. Ví dụ khai báo hai record MX:

```
serverlinux.com. IN MX 1 listo.serverlinux.com.
serverlinux.com. IN MX 2 hep.serverlinux.com.
```

PTR (Pointer)

Record PTR (pointer) dùng để ánh xạ địa chỉ IP thành tên máy hostname.

- Cú pháp:[address] IN PTR [hostname]

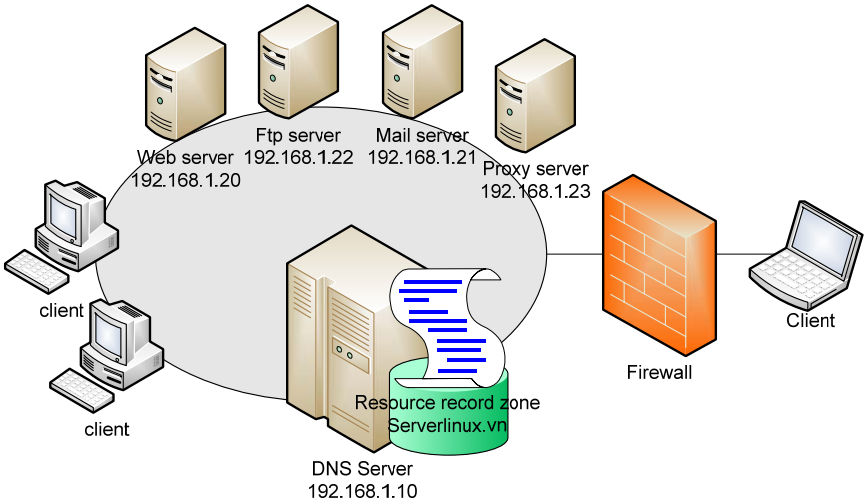
Trong đó [address] là địa chỉ ip của hostname nhưng phải được ghi đảo ngược và kết hợp với tên miền inaddr.arpa.

- Ví dụ 5.1.6: Các record PTR cho các host trong mạng 1.168.192:

```
1.1.168.192.in-addr.arpa. IN PTR serverlinux.com.
2.1.168.192.in-addr.arpa. IN PTR dnsserver.serverlinux.com.
3.1.168.192.in-addr.arpa. IN PTR mailserver.serverlinux.com.
4.1.168.192.in-addr.arpa. IN PTR dnshard.serverlinux.com.
```

5.1.4. CẤU HÌNH DNS MIỀN CỤC BỘ

Mô hình và yêu cầu bài tập



Yêu cầu: Miền serverlinux.vn được thuê từ tổ chức VNNIC, hãy cấu hình DNS server quản lý dữ liệu cho miền này

Hướng dẫn thực hiện

1. Cài đặt BIND
2. Khai báo zone trong /etc/named.rfc1912.zones
   - Zone thuận
   - Zone nghịch
3. Mô tả cơ sở dữ liệu
   - Zone thuận
   - Zone nghịch
4. Thay đổi cấu hình để cho phép hệ thống hoạt động trên địa chỉ IP cục bộ, cho mạng cục bộ hoặc bên ngoài truy vấn cơ sở dữ liệu.

```
Listen-on   port 53 {127.0.0.1; 192.168.1.17;}
Allow-query {localhost; 192.168.1.0/24; };
```

5. Khởi tạo và kiểm tra hoạt động
6. Khai báo dns client
7. Kiểm tra phân giải tên miền

Các bước thực hiện cấu hình

1. Kiểm tra phần mềm BIND
   - Dùng lệnh #rpm –qa bind* :để kiểm tra phần mềm bin đã cài đặt trên hệ thống hay chưa.
2. Cài đặt phần mềm BIND

```
[root@linux ~]#yum -y install bind
Hoặc download và cài đặt phần mềm ở dạng nhị phân bằng trình RPM
[root@linux ~]#rpm –ivh bind-9.7.3-2.el6_1.P3.3.i686.rpm
[root@linux ~]#rpm –ivh bind-libs-9.7.3-2.el6_1.P3.3.i686.rpm
[root@linux ~]#rpm –ivh bind-utils-9.7.3-2.el6_1.P3.3.i686.rpm
```

3. Thực hiện cấu hình địa chỉ IP cho máy DNS Server với địa chỉ: 192.168.1.17/24
4. Khai báo zone trong /etc/named.rfc1912.zones
   - Zone thuận: thêm vào các dòng khai báo bên dưới cùng tập tin

```
zone "serverlinux.vn" IN {    //Khai báo zone thuận
      type master;            //Khai báo kiểu master
      file "serverlinux.thuan";//Khai báo csdl thuận
      allow-update { none; }; //Không cho phép update
};
```

   - Zone nghịch

```
zone "1.168.192.in-addr.arpa" IN {  //Khai báo zone nghịch
      type master;      //Khai báo kiểu master
      file "serverlinux.nghich";//khai báo csdl nghich
      allow-update { none; };//Không cho phép update
};
```

5. Chỉnh sửa tập tin /etc/named.conf

```
options {
      listen-on port 53 { 127.0.0.1; 192.168.1.17; };//Thêm vào địa chỉ ip
máy dns server
      listen-on-v6 port 53 {::1; };
      directory   "/var/named";
      dump-file   "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
      allow-query{ localhost; 192.168.1.0/24; };//Khai báo dãy địa chỉ mạng
được phép truy cập dns server
      allow-query-cache { localhost; 192.168.1.0/24; };//Khai báo dãy địa
chỉ ip cho phép truy vấn dns server
};
logging {
channel default_debug {
```

```
file "data/named.run";
severity dynamic;
};
};
view localhost_resolver {
      match-clients     { localhost; };
      match-destinations { localhost; };
      recursion yes;
      include "/etc/named.rfc1912.zones";//liên kết đến file khai báo các
zone thuận và zone nghịch ở trên
};
```

6. Mô tả cơ sở dữ liệu trong thư mục /var/named

a) Zone thuận có tên serverlinux.thuan

```
$TTL  86400
@IN   SOA   dns1.serverlinux.vn.    root.serverlinux.vn.(
                  1997022700 ; Serial
                  28800; Refresh
                  14400; Retry
                  3600000; Expire
                  86400 ); Minimum
      IN    NS    dns1.serverlinux.vn.
      IN    MX    1     mail.serverlinux.vn.
dns1  IN    A     192.168.1.17
www   IN    CNAME dns1.serverlinux.vn.
mail  IN    CNAME dns1.serverlinux.vn.
ftp   IN    CNAME dns1.serverlinux.vn.
proxy IN    CNAME dns1.serverlinux.vn.
```

b) Zone nghịch có tên serverlinux.thuan: có thể copy từ zone thuận và đặt tên là serverlinux.nghich, sau đó chỉnh sửa vài chỗ như bên dưới.

```
$TTL  86400
@IN   SOA   dns1.serverlinux.vn.    root.serverlinux.vn.(
                  1997022700 ; Serial
                  28800; Refresh
                  14400; Retry
                  3600000; Expire
                  86400 ); Minimum
      IN    NS    dns1.serverlinux.vn.
17    IN    PTR   dns1.serverlinux.vn.
```

c) Phần quyền 2 CSDL vừa tạo: Nếu sử dụng trình soạn thảo VI để tạo 2 tập tin trên thì phải gán quyền truy cập cho 2 tập tin này. Thực hiện các lệnh sau:

```
#chmod 777 /var/named/serverlinux.thuan
```

```
#chmod 777 /var/named/serverlinux.nghich
```

7. Đặt nameserver và domain trong tập tin /etc/resolv.conf

```
nameserver  192.168.1.17
domain      serverlinux.vn
```

8. Khởi động dịch vụ DNS

a) Để khởi động dịch vụ DNS:

```
#/etc/init.d/named      restart
Hoặc lệnh: #service     named       restart
```

b) Kiểm tra xem dịch vụ DNS có hoạt động hay chưa bằng lệnh:

```
#pgrep            named
1489
```

c) Kiểm tra xem DNS đã phân giải hay chưa bằng lệnh:

```
[root@linux ~]# host www.serverlinux.vn
www.serverlinux.vn is an alias for dns1.serverlinux.vn.
dns1.serverlinux.vn has address 192.168.1.17
[root@linux ~]# host 192.168.1.17
192.168.1.17.in-addr.arpa domain name pointer dns1.serverlinux.vn.
```

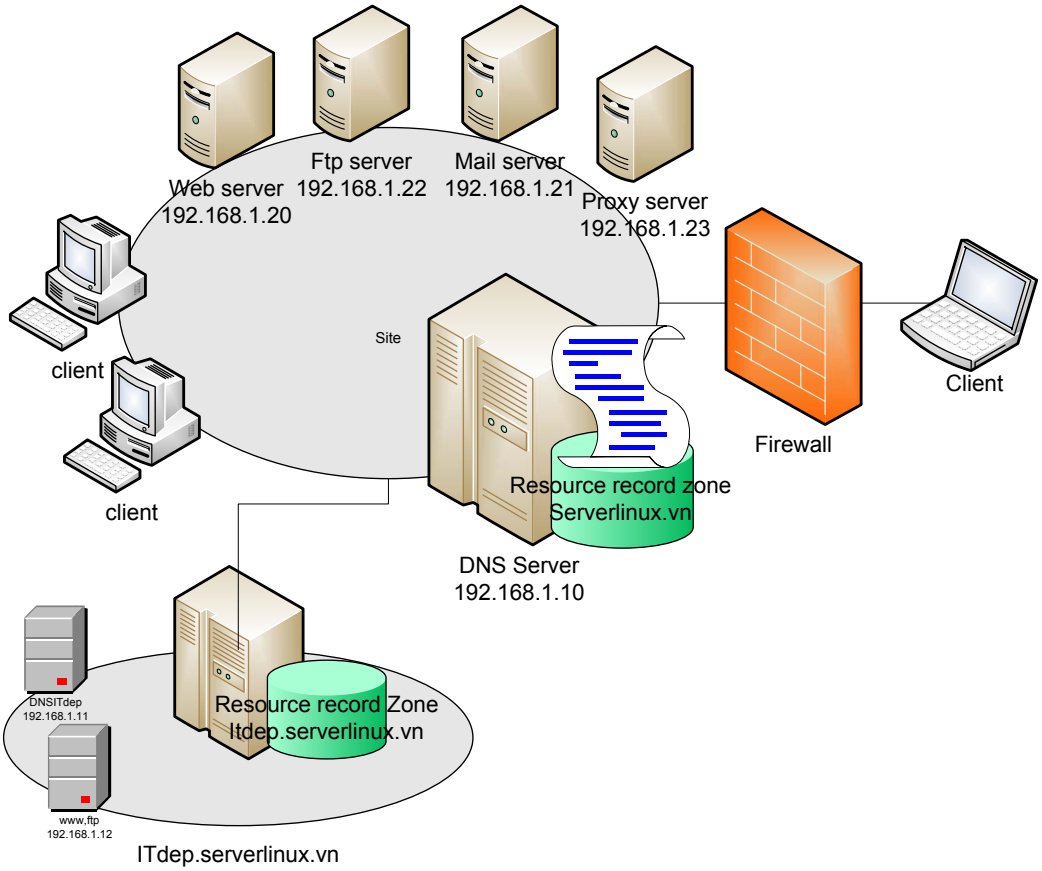
9. `[root@linux ~]#` Kiểm tra phân giải tên miền

Thực hiện lệnh `#nslookup` để kiểm tra phân giải tên miền. Sau khi gõ lệnh nslookup, command line sẽ là dấu ">", gõ lệnh

```
[root@linux ~]# nslookup
> set type=any
> dns1.serverlinux.vn
Server:         192.168.1.17
Address:        192.168.1.17#53

Name:   dns1.serverlinux.vn
Address: 192.168.1.17
>192.168.1.17
Server:         192.168.1.17
Address:        192.168.1.17#53

192.168.1.17.in-addr.arpa      name = dns1.serverlinux.vn.
```

5.1.5. CẤU HÌNH DNS MIỀN CON

Mô hình và yêu cầu cấu hình



Yêu cầu: Miền serverlinux.vn được thuê từ tổ chức VNNIC, hãy cấu hình DNS server quản lý dữ liệu cho miền này

Hướng dẫn

1) Mô tả cơ sỡ dữ liệu
    a. Zone thuận
    b. Zone nghịch
2) Khởi tạo và kiểm tra hoạt động
3) Kiểm tra phân giải tênmiền

Các bước thực hiện

1) Kiểm tra hoạt động của tên miền severlinux.vn

Thực hiện các lệnh sau đây để kiểm tra tên miền cục bộ severlinux.vn

```
[root@linux ~]# host dns1.serverlinux.vn
dns1.serverlinux.vn has address 192.168.1.17
[root@linux ~]#
```

2) Kiểm tra các gói phần bind* trên DNS server master

```
[root@DNS ~]# rpm -qa bind*
bind-libs-9.3.6-16.P1.el5
bind-utils-9.3.6-16.P1.el5
bind-9.3.6-16.P1.el5
```

3) Khai báo zone thuận và zone nghịch trên DNS server master. Khai báo zone trong /etc/named.rfc1912.zones

- Zone thuận: thêm vào các dòng khai báo bên dưới cùng tập tin

```
zone "serverlinux.vn" IN {
      type master;
      file "serverlinux.thuan";
      allow-update { none; };
};
```

- Zone nghịch

```
zone "1.168.192.in-addr.arpa" IN {
      type master;
      file "serverlinux.nghich";
      allow-update { none; };
};
```

4) [root@DNS etc]# vi /etc/named.caching-nameserver.conf

```
options {
      listen-on port 53 { 127.0.0.1; 192.168.1.17; };
      listen-on-v6 port 53 {::1; };
      directory   "/var/named";
      dump-file   "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
      allow-query{ localhost; 192.168.1.0/24; };
      allow-query-cache { localhost; 192.168.1.0/24; };
};
logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};
};
view localhost_resolver {
```

```
      match-clients     { localhost; };
      match-destinations { localhost; };
      recursion yes;
      include "/etc/named.rfc1912.zones";
};
```

5) Mô tả cơ sở dữ liệu trong thư mục /var/named

a. Zone thuận có tên serverlinux.thuan

```
$TTL  86400
@INSOAdns1.serverlinux.vn. root.serverlinux.vn.(
                        1997022700 ; Serial
                        28800; Refresh
                        14400; Retry
                        3600000; Expire
                        86400 ); Minimum
            IN    NS    dns1.serverlinux.vn.
            IN    MX    1     mail.serverlinux.vn.
dns1        IN    A     192.168.1.17
www         IN    CNAME dns1.serverlinux.vn.
mail        IN    CNAME dns1.serverlinux.vn.
ftp         IN    CNAME dns1.serverlinux.vn.
proxy       IN    CNAME dns1.serverlinux.vn.
itdep       IN    A     192.168.1.28
            IN    MX    1     mail.itdep.serverlinux.vn.
mail.itdep  IN    A           192.168.1.28
www.itdep   IN    CNAME       mail.itdep.serverlinux.vn.
ftp.itdep   IN    CNAME       mail.itdep.serverlinux.vn.
```

b. Zone nghịch có tên serverlinux.thuan: có thể copy từ zone thuận và đặt tên là serverlinux.nghich, sau đó chỉnh sửa vài chỗ như bên dưới.

```
$TTL  86400
@INSOAdns1.serverlinux.vn. root.serverlinux.vn.(
                        1997022700 ; Serial
                        28800; Refresh
                        14400; Retry
                        3600000; Expire
                        86400 ); Minimum
      IN    NS    dns1.serverlinux.vn.
17    IN    PTR   dns1.serverlinux.vn.
28    IN    PTR   itdep.serverlinux.vn.
      IN    PTR   mail.itdep.serverlinux.vn.
```

6) Khởi động dịch vụ DNS

a. Để khởi động dịch vụ DNS thực hiện lệnh sau:

```
#/etc/init.d/named      restart
Hoặc lệnh: #service           named       restart
```

b. Kiểm tra xem dịch vụ DNS có hoạt động hay chưa bằng lệnh: `#pgrep named`

c. Kiểm tra xem DNS đã phân giải hay chưa bằng lệnh:

```
[root@linux ~]# host dns1.serverlinux.vn
dns.serverlinux.vn has address 192.168.1.17
```

d. Kiểm tra phân giải tên miền

a) Thực hiện lệnh #nslookup để kiểm tra phân giải tên miền. Sau khi gõ lệnh nslookup, command line sẽ là dấu ">", gõ lệnh

```
[root@linux ~]# nslookup
> set type=any
> dns1.serverlinux.vn
Server:         192.168.1.17
Address:        192.168.1.17#53

Name:   dns1.serverlinux.vn
Address: 192.168.1.17
>192.168.1.17
Server:         192.168.1.17
Address:        192.168.1.17#53

192.168.1.17.in-addr.arpa      name = dns1.serverlinux.vn.
```

b) Kiểm tra tên miền itdep mx

```
#host -t    mx    itdep.serverlinux.vn
```

c) Kiểm tra tên miền itdep www

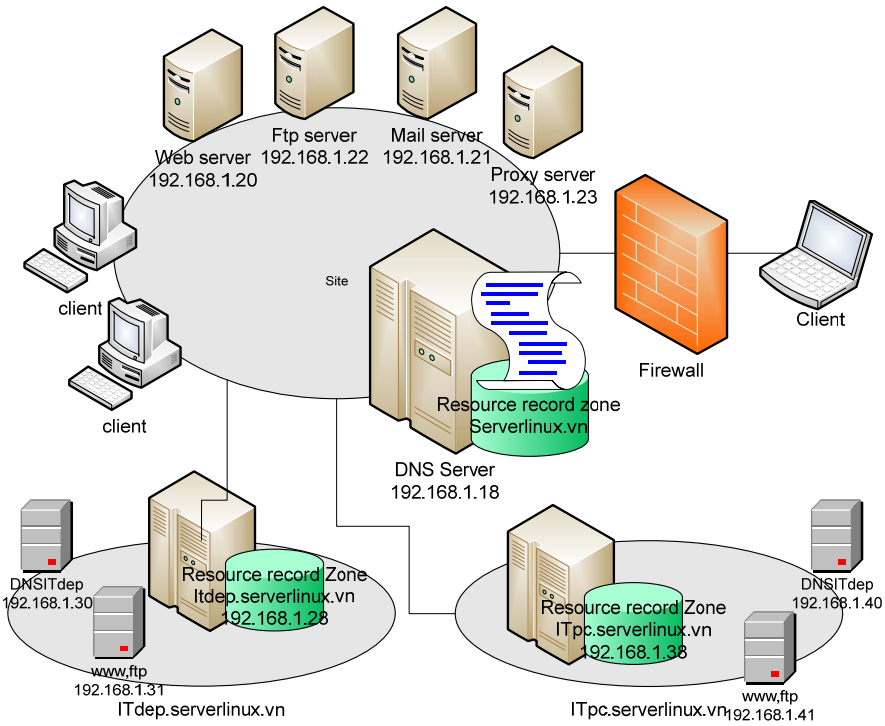
```
#host www.itdep.serverlinux.vn
```

d) Kiểm tra tên miền itdepftp

```
#host ftp.itdep.serverlinux.vn
```

5.1.6. CẤU HÌNH DNS LIÊN KẾT NHIỀU MIỀN CON

Mô hình và yêu cầu hệ thống



Yêu cầu: Miền serverlinux.vn được thuê từ tổ chức VNNIC, hãy cấu hình DNS server quản lý dữ liệu cho miền này.

Hướng dẫn cấu hình

1) Cấu hình ủy quyền trên dnssvr
- Zone thuận
    - Khai báo record NS và A trỏ về miền itdep.serverlinux.vn và miền pcm.serverlinux.vn
- Zone nghịch
    - Khai báo PTR tương ứng với record A
2) Khởi tạo và kiểm tra hoạt động
3) Cấu hình DNS cho miền itdep.serverlinux.vn
    a. Forwarders về máy chủ dnssvr
4) Cấu hình DNS cho miền pcm.serverlinux.vn
    a. Forwaders về máy chủ dnssvr

5) Kiểm tra phân giải tênmiền

Các bước thực hiện cấu hình

- Kiểm tra hoạt động của tên miền serverlinux.vn
- Thực hiện các lệnh sau đây để kiểm tra tên miền cục bộ serverlinux.vn

```
#host dns1.serverlinux.vn
→xuất ra địa chỉ và host của miền này
Tiếp tục gõ lệnh: #nslookup
>set type=any
>serverlinux.vn
→hiện ra thông tin về tên miền serverlinux.vn
```

- Cấu hình named-caching-nameserver.conf

```
[root@localhost named]# vi /etc/named-caching-nameserver.conf
options {
        listen-on port 53 { 127.0.0.1; 192.168.1.17; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 192.168.1.0/24; };
        allow-query-cache { localhost; 192.168.1.0/24; };
recursion yes;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
zone "." IN {
        type hint;
        file "named.ca";
};
include "/etc/named.rfc1912.zones";
```

- Cấu hình tập tin /etc/named.rfc.1912.zones

```
#Khai báo zone thuận
zone "serverlinux.vn" IN {
        type master;
        file "serverlinux.thuan";
        allow-update { none; };
};
#khai báo zone nghich
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "serverlinux.nghich";
        allow-update { none; };
};
```

- Mô tả cơ sở dữ liệu trong thư mục /var/named

a. Zone thuận có tên `serverlinux.thuan`

```
$TTL 1D
@       IN SOA  dns1.serverlinux.vn. root.serverlinux.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
      IN      NS      dns1.serverlinux.vn.
      IN      MX      1       mail.serverlinux.vn.
dns1        IN      A       192.168.1.18
mail        IN      CNAME   dns1.serverlinux.vn.

itdep       IN      A       192.168.1.28
      IN      MX      1       mail.itdep.serverlinux.vn.
mail.itdep  IN      A       192.168.1.28
www.itdep   IN      CNAME   mail.itdep.serverlinux.vn.
ftp.itdep   IN      CNAME   mail.itdep.serverlinux.vn.
```

b. Zone nghịch có tên serverlinux.nghich: có thể copy từ zone thuận và đặt tên là `serverlinux.nghich`, sau đó chỉnh sửa vài chỗ như bên dưới.

```
$TTL 1D
@       IN SOA  dns1.serverlinux.vn. root.serverlinux.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
```

```
        IN      NS      dns1.serverlinux.vn.
18      IN      PTR     dns1.serverlinux.vn.
28      IN      PTR     itdep.serverlinux.vn.
        IN      PTR     mail.itdep.serverlinux.vn.
```

- Khởi động dịch vụ DNS

a. Để khởi động dịch vụ DNS thực hiện lệnh sau:

```
#/etc/init.d/named      restart
Hoặc lệnh: #service           named       restart
```

b. Kiểm tra xem dịch vụ DNS có hoạt động hay chưa bằng lệnh:

```
#pgrep            named
1489
```

c. Kiểm tra xem DNS đã phân giải hay chưa bằng lệnh:

```
#host       dns1.serverlinux.vn
Hoặc #host  192.168.1.18
```

d. Khai báo zone thuận và zone nghịch cho tên miền itdep

```
zone "itdep.serverlinux.vn" IN {
                  type master;
                  file "itdep.thuan";
                  allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
                  type master;
                  file "itdep.nghich";
                  allow-update { none; };
};
```

e. Cấu hình /etc/named-caching-nameserver.conf

```
options {
        listen-on port 53 { 127.0.0.1; 192.168.1.28; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";

        allow-query { localhost; any; };
        recursion       yes;
        forwarders      { 192.168.1.18; };
        allow-query-cache { localhost; any; };

        dnssec-enable yes;
```

```
        dnssec-validation yes;
        dnssec-lookaside auto;
        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
zone "." IN {
        type hint;
        file "named.ca";
};
include "/etc/named.rfc1912.zones";
```

f. Khai báo nameserver trong /etc/resolv.conf

```
nameserver  192.168.1.17
domain      serverlinux.vn
```

g. Cấu hình cơ sở dữ liệu itdep.thuan và itdep.nghich

- Itdep.thuan

```
$TTL 1D
@   IN SOA  dnsit.itdep.serverlinux.vn. root.itdep.serverlinux.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      dnsit.itdep.serverlinux.vn.
        IN      MX      1       mail.itdep.serverlinux.vn.
dnsit   IN      A       192.168.1.28
mail    IN      A       192.168.1.28
```

- Itdep.nghich

```
$TTL 1D
@   IN SOA  dnsit.itdep.serverlinux.vn. root.itdep.serverlinux.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      dnsit.itdep.serverlinux.vn.
28      IN      PTR     dnsit.itdep.serverlinux.vn.
```

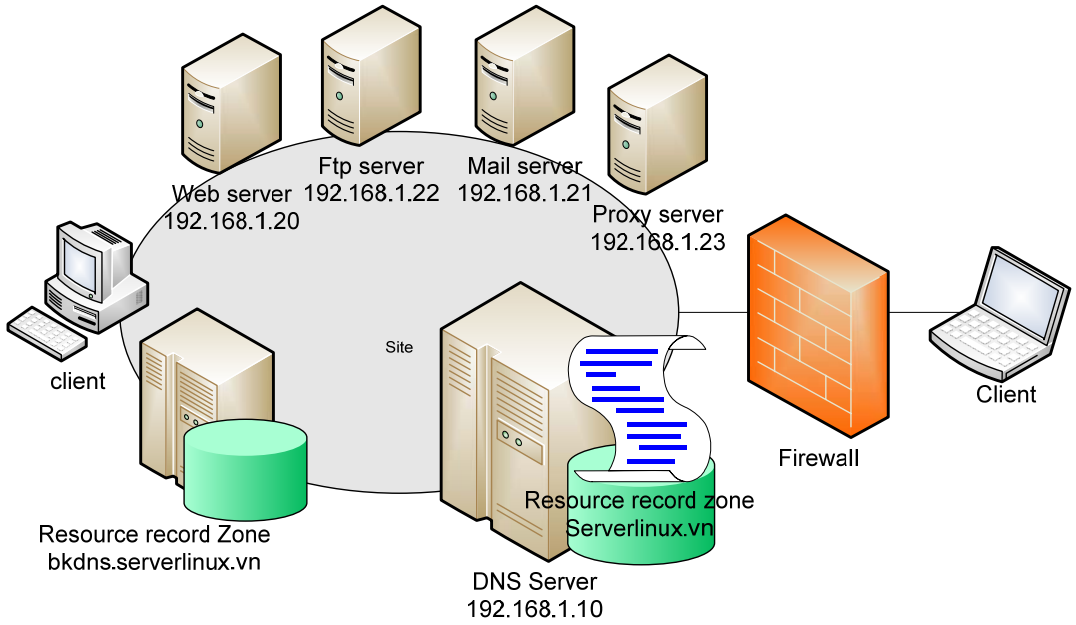
```
        IN      PTR     mail.itdep.serverlinux.vn.
```

a. Kiểm tra phân giải tên miền

```
[root@localhost named]# nslookup
> set type=any
> 192.168.1.28
Server:         192.168.1.18
Address:        192.168.1.18#53

28.1.168.192.in-addr.arpa       name = mail.itdep.serverlinux.vn.
28.1.168.192.in-addr.arpa       name = itdep.serverlinux.vn.

> itdep.serverlinux.vn
Server:         192.168.1.18
Address:        192.168.1.18#53

Name:   itdep.serverlinux.vn
Address: 192.168.1.28
itdep.serverlinux.vn    mail exchanger = 1 mail.itdep.serverlinux.vn.

> serverlinux.vn
Server:         192.168.1.18
Address:        192.168.1.18#53

serverlinux.vn
        origin = dns1.serverlinux.vn
        mail addr = root.serverlinux.vn
        serial = 0
        refresh = 86400
        retry = 3600
        expire = 604800
        minimum = 10800
serverlinux.vn  nameserver = dns1.serverlinux.vn.
serverlinux.vn  mail exchanger = 1 mail.serverlinux.vn.
>
```

5.1.7. CẤU HÌNH DNS SERVER DỰ PHÒNG

Mô hình và yêu cầu hệ thống



Hướng dẫn cấu hình

1) Khai báo zone backup trên serverlinux
   - Zone thuận
   - Zone nghịch
2) Cho phép cope CSDL từ serverlinux
   - Zone thuận
   - Zone nghịch
3) Khởi tạo và kiểm tra hoạt động
4) Khai báo dnsclient
5) Kiểm tra phân giải tên miền

Các bước thực hiện cấu hình

1) Phần 1: Cấu hình DNS server master

a) Kiểm tra kết nối đến DNS dự phòng

```
[root@DNS ~]# ping 192.168.1.17
PING 192.168.1.17 (192.168.1.17) 56(84) bytes of data.
```

```
64 bytes from 192.168.1.17: icmp_seq=1 ttl=64 time=1.46 ms
64 bytes from 192.168.1.17: icmp_seq=2 ttl=64 time=0.295 ms
--- 192.168.1.17 ping statistics ---
```

b) Kiểm tra các gói phần bind* trên DNS server master

```
[root@DNS ~]# rpm -qa bind*
bind-libs-9.3.6-16.P1.el5
bind-utils-9.3.6-16.P1.el5
bind-9.3.6-16.P1.el5
```

c) Khai báo zone thuận và zone nghịch trên DNS server master

```
[root@DNS etc]# vi named.caching-nameserver.conf
options {
listen-on port 53 { 127.0.0.1; 192.168.1.17; };
listen-on-v6 port 53 {::1; };
directory"/var/named";
dump-file"/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
// Those options should be used carefully because they disable port
// randomization
// query-sourceport 53;
// query-source-v6 port 53;
allow-query{ localhost; any; };
//allow-transfer{ localhost; 192.168.1.0/24; };
//allow-recursion { localhost; 192.168.1.0/24; };
allow-query-cache { localhost; any; };
};
controls {
inet127.0.0.1 allow {localhost; } keys { rndckey; };
};
logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};
};
# here is the section for internal informations
view "internal" {
match-clients { localhost; 192.168.1.0/24; };
zone "." IN {
type hint;
file "named.ca";
};
//# set zones for internal
```

```
zone "serverlinux.vn" IN {
type master;
file "serverlinux.thuan";
allow-update { 192.168.1.27; };
            allow-transfer { 192.168.1.27; };
};
//# set zones for internal
zone "1.168.192.in-addr.arpa" IN {
                  type master;
                  file "serverlinux.nghich";
                  allow-update { 192.168.1.27; };
                  allow-transfer { 192.168.1.27; };
};
zone "localdomain" IN {
            type master;
            file "localdomain.zone";
            allow-update { none; };
};
zone "localhost" IN {
      type master;
      file "localhost.zone";
      allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
                  type master;
                  file "named.local";
                  allow-update { none; };
};
zone "255.in-addr.arpa" IN {
                  type master;
                  file "named.broadcast";
                  allow-update { none; };
};
zone "0.in-addr.arpa" IN {
            type master;
      file "named.zero";
      allow-update { none; };
};
};
```

d) Tạo tập tin cơ sở dữ liệu trong /var/named trên DNS server master

- Tạo tập tin thuận serverlinux.thuan miền cục bộ

```
[root@linux ~]# vi serverlinux.thuan
$TTL86400
```

```
@ IN  SOA   dns1.serverlinux.vn.root.serverlinux.vn.(
                              2011022700 ; Serial
                              28800; Refresh
                              14400; Retry
                              3600000; Expire
                              86400 ); Minimum
IN    NS    dns1.serverlinux.vn.
IN    NS    bkdns1.serverlinux.vn.
IN    MX    10    dns1.serverlinux.vn.
Dns1  IN    A     192.168.1.17
Bkdns1      IN    A192.168.1.27
www   IN    CNAME dns1.serverlinux.vn.
mail  IN    CNAME dns1.serverlinux.vn.
ftp   IN    CNAME dns1.serverlinux.vn.
proxy IN    CNAME dns1.serverlinux.vn.
```

- Tạo tập tin thuận 1.168.192.db miền cục bộ

```
[root@linux ~]# vi 1.168.192.db
$TTL86400
@           IN    SOA dns1.serverlinux.vn.      root.serverlinux.vn.(
                              2011022700 ; Serial
                              28800; Refresh
                              14400; Retry
                              3600000; Expire
                              86400 ); Minimum
IN    NS    dns1.serverlinux.vn.
IN    NS    bkns1.serverlinux.vn.
17    IN    PTR   dns1.serverlinux.vn.
27    IN    PTR   bkdns1.serverlinux.vn.
```

e) Khởi động lại named

```
[root@DNS ~]# /etc/init.d/named restart
Stopping named:               [OK]
Starting named:               [OK]
[root@DNS ~]# pgrep named
3075
```

f) Kiểm tra hoạt động của DNS

```
[root@DNS ~]# host dns.serverlinux.vn
dns.serverlinux.vn has address 192.168.1.17
```

10. Phần 2: Cấu hình DNS dự phòng (máy slave)

- Kiểm tra kết nối đến DNS server master

```
[root@DNS ~]# ping 192.168.1.17
PING 192.168.1.17 (192.168.1.17) 56(84) bytes of data.
```

```
64 bytes from 192.168.1.17: icmp_seq=1 ttl=64 time=1.46 ms
64 bytes from 192.168.1.17: icmp_seq=2 ttl=64 time=0.295 ms
--- 192.168.1.17 ping statistics ---
```

- Kiểm tra các gói phần bind* trên DNS server master

```
[root@DNS ~]# rpm -qa bind*
bind-libs-9.3.6-16.P1.el5
bind-utils-9.3.6-16.P1.el5
bind-9.3.6-16.P1.el5
```

- Cấu hình tập tin /etc/named.caching-nameserver.conf

```
options {
listen-on port 53 { 127.0.0.1; 192.168.1.17; };
listen-on-v6 port 53 {::1; };
directory"/var/named";
dump-file"/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";

// Those options should be used carefully because they disable port
// randomization
// query-sourceport 53;
// query-source-v6 port 53;

allow-query{ localhost; any; };
allow-query-cache { localhost; any; };
};
logging {
            channel default_debug {
            file "data/named.run";
            severity dynamic;
};
};
view localhost_resolver {
            match-clients{ localhost; };
            match-destinations { localhost; };
            recursion yes;
            include "/etc/named.rfc1912.zones";
};
```

- Khai báo zone thuận và zone nghịch trên DNS server master

```
[root@dns etc]# vi named.rfc1912.zones
zone "." IN {
type hint;
file "named.ca";
```

```
};

zone "localdomain" IN {
            type master;
            file "localdomain.zone";
            allow-update { none; };
};
zone "localhost" IN {
            type master;
            file "localhost.zone";
            allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
            type master;
            file "named.local";
            allow-update { none; };
};

zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN
{
            type master;
            file "named.ip6.local";
            allow-update { none; };
};

zone "255.in-addr.arpa" IN {
            type master;
            file "named.broadcast";
            allow-update { none; };
};

zone "0.in-addr.arpa" IN {
            type master;
            file "named.zero";
            allow-update { none; };
};
zone "serverlinux.vn" IN {
            type slave;
            masters { 192.168.1.17; };
            file "slaves/bk.thuan";
            allow-update { none; };
};
```

```
zone "1.168.192.in-addr.arpa" IN {
            type slave;
            masters { 192.168.1.17; };
            file "slaves/bk.nghich";
            allow-update { none; };
};
```

- Không khai báo cơ sở dữ liệu trong /var/named trên DNS dự phòng
- Khởi động lại named

```
[root@DNS ~]# /etc/init.d/named restart
Stopping named:          [OK]
Starting named:          [OK]
[root@DNS ~]# pgrep named
3075
```

- Kiểm tra DNS dự phòng copy cơ sở dữ liệu từ DNS server master về thư mục /var/named/slave

```
[root@dns var]# ll /var/named/slaves/
total 16
-rw-r--r-- 1 named named 367 May4 18:00 bk.nghich
-rw-r--r-- 1 named named 435 May4 17:57 bk.thuan
```

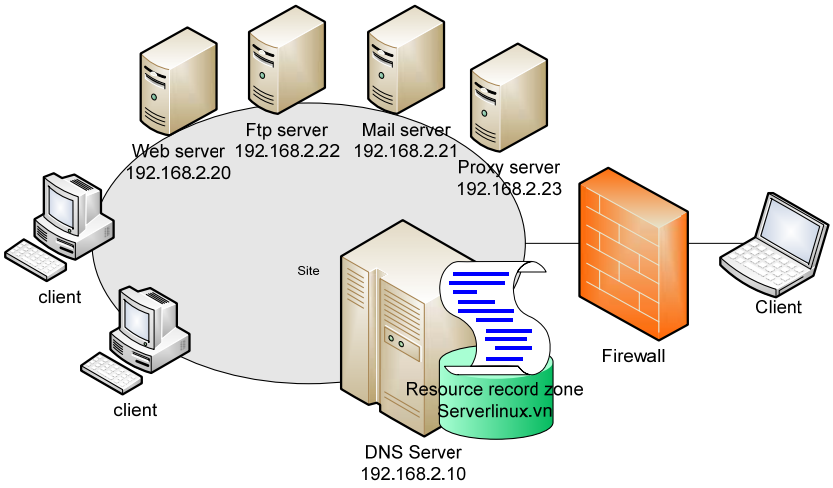
- Kiểm tra hoạt động của DNSdự phòng

```
[root@DNS ~]# host dns1.serverlinux.vn
dns.serverlinux.vn has address 192.168.1.17
```

5.2. CÂU HỎI ÔN TẬP VỀ DNS

5.2.1. THỰC HÀNH 1: THIẾT LẬP DNS QUẢN LÝ MIỀN CỤC BỘ

Trung tâm đào tạo tin học vừa thuê một tên miền "serverlinux.com" từ tổ chức quản lý tên miền VNNIC. Anh/Chị hãy tổ chức DNS server trên máy chủ Linux theo mô hình sau:

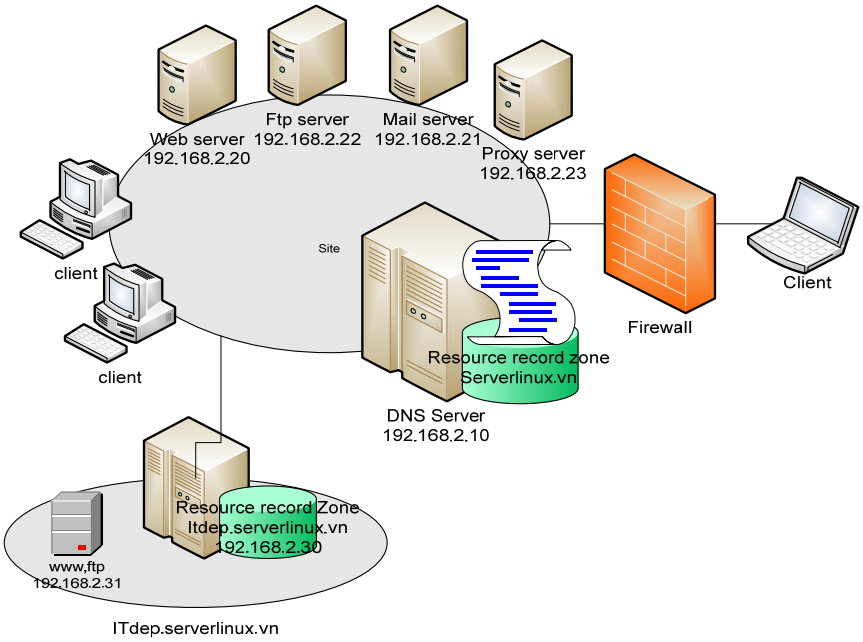


HƯỚNG DẪN

- Khai báo zone trong file /etc/named.rfc1912.zones
    - Zone thuận.
    - Zone nghịch.
- Thay đổi các thông số trong tập tin /etc/named.conf
- Mô tả cơ sở dữ liệu.
    - Zone thuận.
    - Zone nghịch.
- Khởi tạo và kiểm tra hoạt động.
- Khai báo dns client.
- Kiểm tra phân giải tên miền.

5.2.2. THỰC HÀNH 2: THIẾT LẬP DNS HOSTING CHO MIỀN CON

Hãy thiết lập DNS để hosting cho miền con itdep.serverlinux.com theo yêu cầu được mô tả cụ thể trong mô hình sau:

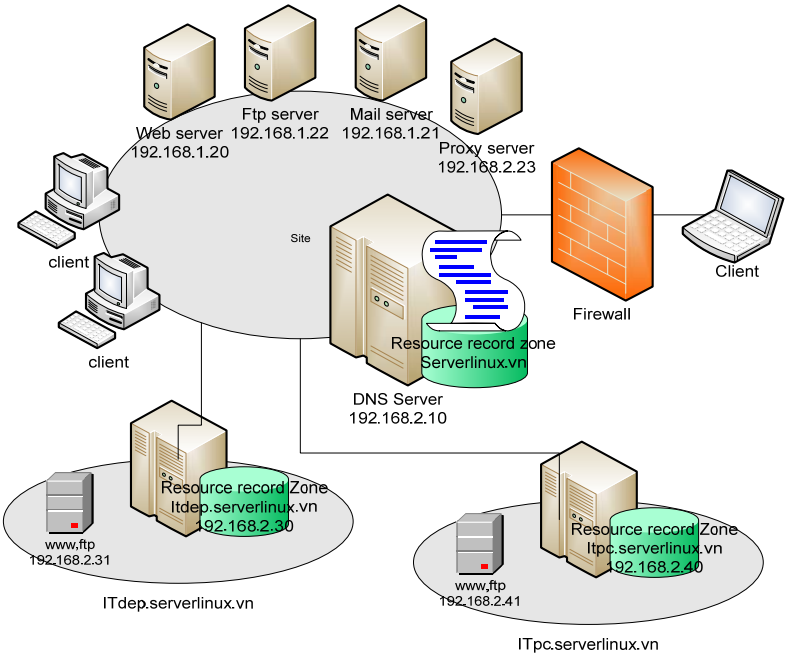


Hướng dẫn:

- Cấu hình DNS cho miền serverlinux.com
- Cấu hình DNS hosting cho miền itdep.serverlinux.com
    - Zone thuận.
    - Zone nghịch (nếu cần)
- Khởi tạo và kiểm tra hoạt động
- Kiểm tra phân giải tên miền

5.2.3. THỰC HÀNH 3: THIẾT LẬP DNS LIÊN KẾT NHIỀU VÙNG

Hãy thiết lập DNS để liên kết cho hai miền con itdep.serverlinux.com và pcm.serverlinux.com theo yêu cầu được mô tả cụ thể trong mô hình sau:

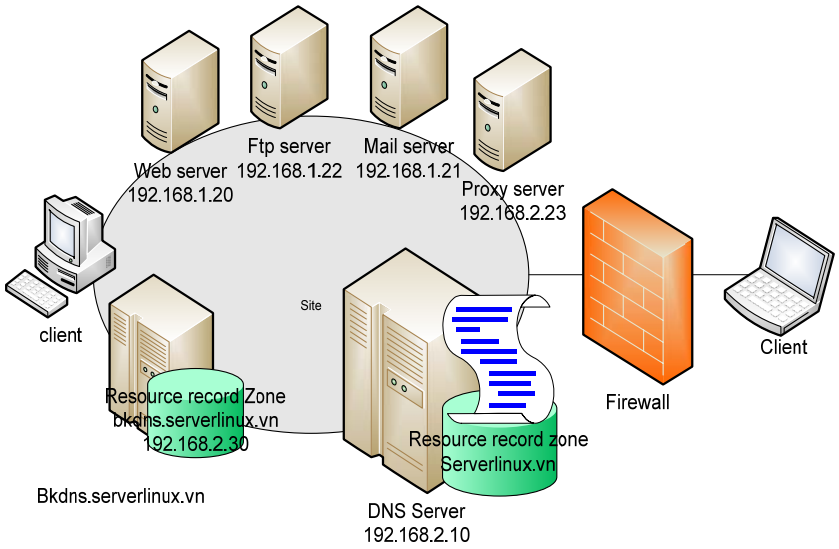


Hướng dẫn:

- Cấu hình DNS cho miền serverlinux.com
- Ủy quyền hai miền con itdep.serverlinux.com và pcm.serverlinux.com
    - Khai báo record NS và A trỏ về miền itdep.serverlinux.com và miền pcm.serverlinux.com
    - Khai báo và PTR tương ứng với record A.
- Khởi tạo và kiểm tra hoạt động
- Cấu hình DNS cho miền itdep.serverlinux.com
    - Forwarders về máy chủ dnssvr.
- Cấu hình DNS cho miền pcm.serverlinux.com
    - Forwarders về máy chủ dnssvr.
- Kiểm tra phân giải tên miền

5.2.4. THỰC HÀNH 4: THIẾT LẬP DNS DỰ PHÒNG

Hãy thiết lập DNS dự phòng (slave nameserver) để sao chép cơ sở dữ liệu cho miền serverlinux.com theo yêu cầu dựa trên mô hình sau:



Hướng dẫn:

- Cấu hình DNS server chính (master nameserver)
- Cấu hình DNS server dự phòng.
    - Zone thuận.
    - Zone nghịch.
- Cho phép copy CSDL từ dnssvr
    - Zone thuận.
    - Zone nghịch.
- Khởi tạo và kiểm tra hoạt động.
- Khai báo dns client.
- Kiểm tra phân giải tên miền.

5.3. DỊCH VỤ FTP

5.3.1. GIỚI THIỆU FTP

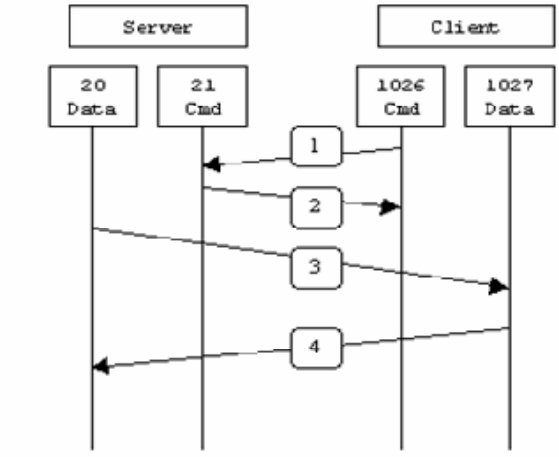
FTP được viết tắt từ chuỗi File Transfer Protocol. Giao thức này được xây dựng dựa trên chuẩn TCP, FTP cung cấp cơ chế truyền tin dưới dạng file thông qua mạng TCP/IP, FTP là một dịch vụ đặc biệt vì nó dùng đến hai cổng: Cổng 20 (còn gọi là data port) dùng để truyền dữ liệu và cổng 21 (còn gọi là command port) dùng để truyền lệnh.Một số chương trình ftp server sử dụng trên Linux:Vsftpd, Wu-ftpd, PureFTPd, ProFTPD. FTP có 2 loại:

Active FTP

Ở chế độ chủ động (active), máy khách FTP dùng một cổng ngẫu nhiên không dành riêng (cổng N > 1024) kết nối vào cổng 21 của FTP server. Sau đó, máy khách lắng nghe trên cổng N+1 và gửi lệnh PORT N+1 đến FTP server. Tiếp theo, từ cổng dữ liệu của mình, FTP server sẽ kết nối ngược lại vào cổng dữ liệu của client đã khai báo trước đó (tức là N+1). Ở khía cạnh firewall, để FTP Server hỗ trợ chế độ active thì các kênh truyền sau phải mở:

- Cổng 21 phải được mở cho bất cứ nguồn gửi nào (để client khởi tạo kết nối)
- FTP server's port 21 to ports > 1024 (server trả lời về cổng điều khiển của client)
- Cho kết nối từ cổng 20 của FTP server đến các cổng > 1024 (server khởi tạo kết nối vào cổng dữ liệu của client)
- Nhận kết nối hướng đến cổng 20 của FTP server từ các cổng > 1024 (client gửi xác nhận ACKs đến cổng data của server)

Sơ đồ kết nối:



- Bước 1: Client khởi tạo kết nối vào cổng 21 của server và gửi lệnh PORT 1027.

- Bước 2: Server gửi xác nhận ACK về cổng lệnh của client.
- Bước 3: Server khởi tạo kết nối từ cổng 20 của mình đến cổng dữ liệu mà client đã khai báo trước đó.
- Bước 4: Client gửi ACK phản hồi cho server.

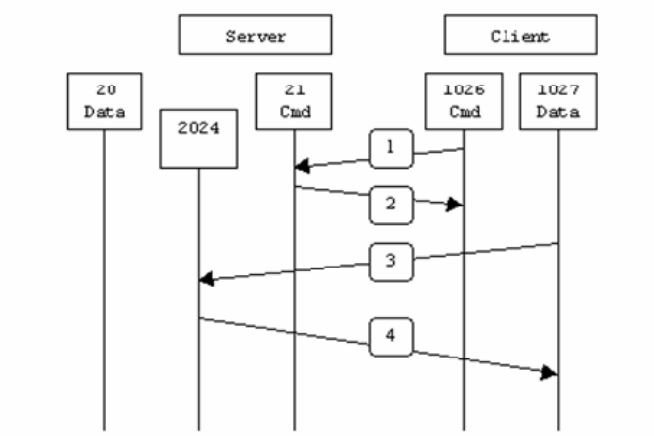
Khi FTP Server hoạt động ở chế độ chủ động, client không tạo kết nối thật sự vào cổng dữ liệu của FTP server, mà chỉ đơn giản là thông báo cho server biết rằng nó đang lắng nghe trên cổng nào và server phải kết nối ngược về client vào cổng đó.

Passive FTP

Phương thức này gọi là FTP thụ động (passive) hoặc PASV (là lệnh mà client gửi cho server để báo cho biết là nó đang ở chế độ passive). Ở chế độ thụ động, FTP client tạo kết nối đến server. Khi kết nối FTP được mở, client sẽ mở hai cổng không dành riêng N, N+1 (N > 1024). Cổng thứ nhất dùng để liên lạc với cổng 21 của server, nhưng thay vì gửi lệnh PORT và sau đó là server kết nối ngược về client, thì lệnh PASV được phát ra. Kết quả là server sẽ mở một cổng không dành riêng bất kỳ P (P > 1024) và gửi lệnh PORT P ngược về cho client. Sau đó client sẽ khởi tạo kết nối từ cổng N+1 vào cổng P trên server để truyền dữ liệu. Phía Firewall trên server FTP, để hỗ trợ FTP chế độ passive, các kênh truyền sau phải được mở:

- Cổng FTP 21 của server nhận kết nối từ bất kỳ nguồn nào (cho client khởi tạo kết nối).
- Cho phép trả lời từ cổng 21 FTP server đến cổng bất kỳ trên 1024 (Server trả lời cho cổng control của client).
- Nhận kết nối trên cổng FTP server > 1024 từ bất cứ nguồn nào (Client tạo kết nối để truyền dữ liệu đến cổng ngẫu nhiên mà server đã chỉ ra).
- Cho phép trả lời từ cổng FTP server > 1024 đến các cổng > 1024 (Server gửi xác nhận ACKs đến cổng dữ liệu của client).

Sơ đồ:

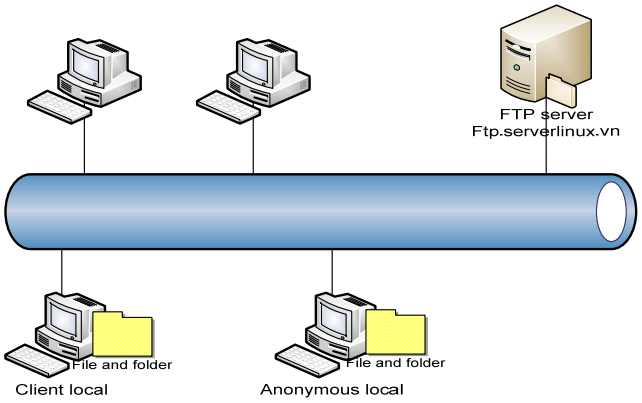


- Bước 1: Client kết nối vào cổng lệnh của server và phát lệnh PASV.
- Bước 2: Server trả lời bằng lệnh PORT 2024, cho client biết cổng 2024 đang mở để nhận kết nối dữ liệu.
- Bước 3: Client tạo kết nối truyền dữ liệu từ cổng dữ liệu của nó đến cổng dữ liệu 2024 của server.
- Bước 4: Là server trả lời bằng xác nhận ACK về cho cổng dữ liệu của client.

5.3.2. CẤU HÌNH FTP SERVER

Mô hình và yêu cầu hệ thống

Cấu hình cho phép người dùng anonymous và local user upload dữ liệu lên FTP Server theo mô hình sau đây:



Hướng dẫn cấu hình

a) Tạo người dùng cục bộ

b) Khai báo tên miền ftp.serverlinux.vn trong DNS server
c) Cài đặt vsftpd
d) Cấu hình tập tin /etc/vsftpd/vsftpd.conf
e) Khởi động dịch vụ FTP
f) Kiểm tra hoạt động
    1) Kiểm tra tiến trình vsftpd
    2) Login bằng người dùng anonymous trên windows
    3) Upload tài liệu
    4) Login bằng tài khoản hv1 trên windows
    5) Upload tài liệu
g) Ftp client từ Linux
h) ftp client từ Windows

Các bước thực hiện

a) Tạo người dùng cục bộ

```
[root@localhost ~]# useradd hv1     #tạo người dùng hv1
useradd: user hv1 exists

[root@localhost ~]# passwd hv1      #đặt mật khẩu tạo người dùng hv1
Changing password for user hv1.
New UNIX password:            #Nhập mật khẩu vào
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:     #xác thực lại mật khẩu
passwd: all authentication tokens updated successfully.
```

b) Cấu hình zone thuận serverlinux.vn

```
$TTL  86400
@           IN    SOA   dns1.serverlinux.vn.    root.serverlinux.vn.(
                        2011022700 ; Serial
                        28800; Refresh
                        14400; Retry
                        3600000; Expire
                        86400 ); Minimum
IN    NS    dns1.serverlinux.vn.
      IN    MX    1     dns1.serverlinux.vn.
dns1  IN    A     192.168.1.17
```

```
www   IN    CNAME dns1.serverlinux.vn.
mail  IN    CNAME dns1.serverlinux.vn.
ftp   IN    CNAME 192.168.1.28
proxy IN    CNAME dns1.serverlinux.vn.
```

c) Khởi động dns server

```
[root@localhost ~]# /etc/init.d/named restart
Stopping named:               [OK]
Starting named:               [OK]

[root@localhost ~]# hostftp.serverlinux.vn
[root@localhost ~]# host ftp.serverlinux.vn
ftp.serverlinux.vn is an alias for ns1.serverlinux.vn.
dns1.serverlinux.vn has address 192.168.1.17
```

d) Cài đặt vsftpd

```
[root@linux ~]#yum -y install vsftpd
```

e) Cấu hình tập tin /etc/vsftpd/vsftpd.conf

```
[root@linux ~]#vi /etc/vsftpd/vsftpd.conf
# line 12: no anonymous
anonymous_enable=NO     #Không cho phép người dùng anonymous login vào
# line 81,82: uncomment (permit ascii mode transfer)
ascii_upload_enable=YES
ascii_download_enable=YES
# line 96: uncomment ( enable chroot list )
chroot_list_enable=YES
chroot_local_user=YES
# line 99: uncomment ( enable chroot list file )
chroot_list_file=/etc/vsftpd/chroot_list
# line 105: uncomment
ls_recurse_enable=YES
# add at the bottom
# specify root directory ( if don't specify, users' home directory become
FTP home directory )
local_root=public_html
# use localtime
use_localtime=YES       #sử dụng thời gian hệ thống

[root@linux ~]# vi /etc/vsftpd/chroot_list
# add users you allow to move over their home directory
```

```
hv1
```

f) Tắt firewall: FTP server khi chạy mở port (20,21) nên ta phải mở 2 port này bằng cách tắt firewall

```
[root@linux ~]# /etc/init.d/iptables stop
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
```

g) Khởi động dịch vụ FTP

```
[root@linux ~]# /etc/rc.d/init.d/vsftpd start
Starting vsftpd for vsftpd:         [OK]
[root@linux ~]# chkconfig vsftpd on
```

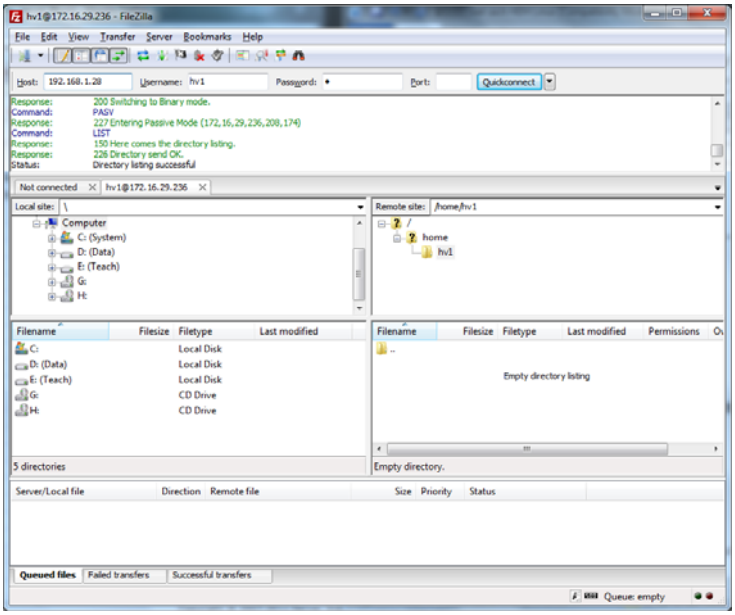
h) Ftp client từ Linux

```
[root@linux vsftpd]# ftp 192.168.1.28
Connected to 192.168.1.28.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.1.28:root): hv1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

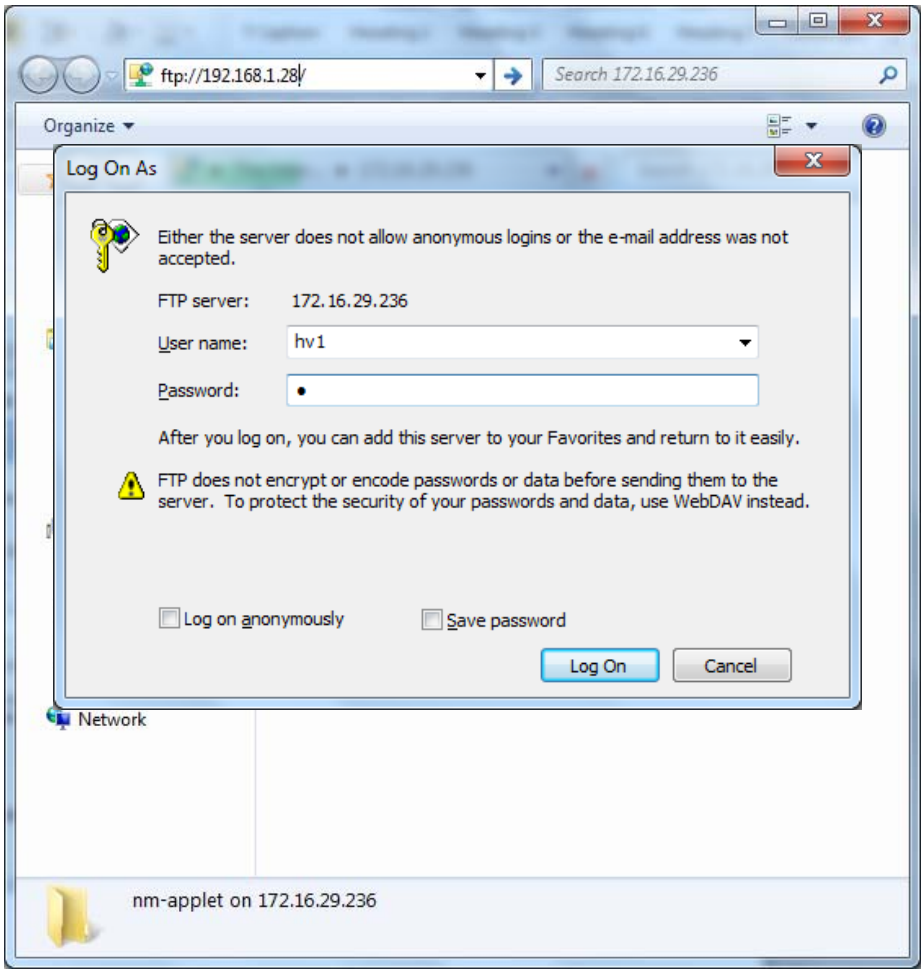
Kiểm tra

```
ftp> ls
227 Entering Passive Mode (192,168,1,28,41,97)
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

i) Ftp client FileZilla từ Windows



Hoặc gõ lệnh trong Run: ftp://192.168.1.28



5.3.3. GIỚI HẠN TRUY CẬP FTP

Yêu cầu bài tập

- Cấu hình chỉ cho phép người dùng cục bộ truy cập vào ftp server ngoại trừ người dùng hv2
- Cấm host 192.168.1.200 truy cập vào ftp server

Hướng dẫn cấu hình

a) Tạo người dùng cục bộ
b) Cấu hình ftp
    1) Giới hạn người dùng anonymous
    2) Giới hạn host truy cập ftp server
c) Khởi tạo ftp server
d) Kiểm tra hoạt động trên linux
    1) Kiểm tra tiến trình vsftps
    2) Kiểm tra tên miềnftp.serverlinux.vn
e) Kiểm tra hoạt động trên windows
    1) Login bằng người dùng anonymous
    2) Login bằng người dùng cục bộ
    3) Login từ host 192.168.1.200

Các bước thực hiện cấu hình

a) Tạo người dùng cục bộ

```
[root@localhost ~]# useradd hv1
useradd: user hv1 exists

[root@localhost ~]# passwd hv1
Changing password for user hv1.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
```

```
passwd: all authentication tokens updated successfully.

[root@localhost ~]# useradd hv2
useradd: user hv2 exists
[root@localhost ~]# passwd hv2
Changing password for user hv2.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

[root@localhost ~]# su - hv2
```

b) Cấu hình /etc/vsftpd/vdftpd.conf

- Cấu hình cấm người dùng anonymous truy cập ftp server

```
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=NO
anon_root=/var/ftp
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

- Cấm user cục bộ hv1 truy cập ftp serrver trong tập tin /etc/vsftpd/ftpusers

```
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
hv1
```

- Và trong tập tin /etc/vsftpd/user_list

```
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
Root
Bin
Daemon
Adm
Lp
Sync
Shutdown
Halt
Mail
News
Uucp
Operator
Games
Nobody
hv1
```

- Cấm host 192.168.1.200 truy cập ftp server trong tập tin /etc/hosts.deny

```
#
# hosts.deny      This file describes the names of the hosts which are
#           *not* allowed to use the local INET services, as decided
#           by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow.In particular
# you should know that NFS uses portmap!
vsftpd:192.168.1.200
```

c) Kiểm tra sự hoạt động của ftp

```
[root@localhost ~]# host
[root@localhost ~]# host ftp.serverlinux.vn
ftp.serverlinux.vn is an alias for dns1.serverlinux.vn.
dns1.serverlinux.vn has address 192.168.1.3
[root@localhost ~]# pgrep vsftpd
4821
```

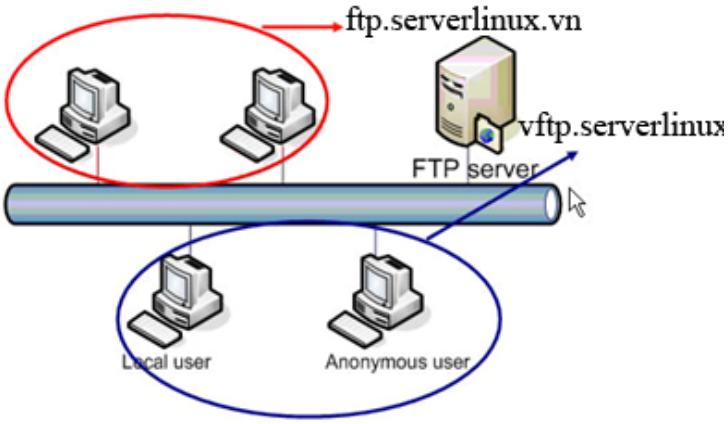
d) Cấu hình iptables để cho phép ftp được phép truy cập qua firewall

- Bằng tiện ích #setup

```
root@localhost ~]# /etc/init.d/iptables restart
Flushing firewall rules:                                   [OK]
Setting chains to policy ACCEPT: nat mangle filter         [OK]
Unloading iptables modules:                                [OK]
Applying iptables firewall rules:                          [OK]
Loading additional iptables modules: p_conntrack_netbios_n[OK]ntrack_ftp
```

5.3.4. CẤU HÌNH TẠO NHIỀU FTP SITE

Mô hình và yêu cầu hệ thống



- Site 1: ftp.serverlinux.vn
- Site 2: vftp.serverlinux.vn

Hướng dẫn cấu hình

a) Tạo IP alias cho vftp site
b) Cấu hình ftp site 1: ftp.serverlinux.vn
c) Cấu hình ftp site 2: vftp.serverlinux.vn
d) Kiểm tra hoạt động
   1) Kiểm tra tiến trình vsftpd
   2) Login bằng tài khoản anonymous và user hv1 hv2

Các bước thực hiện cấu hình

a) Tạo ip alias cho vftp site

b) Bằng cách vào thư mục /etc/sysconfig/network-scripts để copy file ifcfg-eth0 thanh ifcfg-eth0:0. Sau đó chỉnh sử tập tin ifcfg-eth0:0 với nội dung như sau:

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0:0
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:0c:29:d7:6b:ae
NETMASK=255.255.255.0
IPADDR=192.168.1.6
GATEWAY=192.168.1.254
TYPE=Ethernet
```

c) Khởi động lại network bằng lệnh

```
[root@localhost network-scripts]# /etc/init.d/network restart
Shutting down interface eth0:              [OK]
Shutting down interface eth1:              [OK]
Shutting down loopback interface:          [OK]
Bringing up loopback interface:            [OK]
Bringing up interface eth0:                [OK]
Bringing up interface eth1: Determining IP information for eth1... done.

root@localhost network-scripts]# ifconfig|more
eth0  Link encap:EthernetHWaddr 00:0C:29:D7:6B:AEinet
addr:192.168.1.3Bcast:192.168.1.255Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICASTMTU:1500Metric:1
            RX packets:5747 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3886 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:5363775 (5.1 MiB)TX bytes:385221 (376.1 KiB)
      Interrupt:67 Base address:0x2000
eth0:0      Link encap:EthernetHWaddr 00:0C:29:D7:6B:AE
            inet addr:192.168.1.6Bcast:192.168.1.255
      Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICASTMTU:1500Metric:1
            Interrupt:67 Base address:0x2000
eth1  Link encap:EthernetHWaddr 00:0C:29:D7:6B:B8
            inet addr:172.16.29.121Bcast:172.16.29.255
            Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICASTMTU:1500Metric:1
            RX packets:26455 errors:0 dropped:0 overruns:0 frame:0
            TX packets:6003 errors:0 dropped:0 overruns:0
carrier:0collisions:0 txqueuelen:1000
```

```
            RX bytes:13022728 (12.4 MiB)TX bytes:509634 (497.6 KiB)
            Interrupt:67 Base address:0x2080
lo          Link encap:Local Loopback
            inet addr:127.0.0.1Mask:255.0.0.0
            UP LOOPBACK RUNNINGMTU:16436Metric:1
            RX packets:4801 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4801 errors:0 dropped:0 overruns:0
carrier:0collisions:0 txqueuelen:0
            RX bytes:5782608 (5.5 MiB)TX bytes:5782608 (5.5 MiB)
```

d) Bước tiếp theo vào thư mục /etc/vsftpd, copy file vsftpd.conf ra môt tập tin mới có tên ftp_ao.conf bằng lệnh

```
#cd /etc/vsftpd
#cp vsftpd.confftp_ao.conf
```

e) Cấu hình site 1 ftp.serverlinux.vn

- Cấu hình tập tin /etc/vsftpd/vsftpd.conf như bên dưới:

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=NO
anon_root=/ftproot
#
# Uncomment this to allow local users to log in.
local_enable=YES
#thêm vào các dòng sau ở cuối file (nếu dòng nào có rồi thì không cần phải
thêm)
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
#local_root=public_html
use_localtime=YES
listen_address=192.168.1.3
```

- Cấu hinh dns về tên miền ftp.serverlinux.vn

```
$TTL  86400
@INSOA dns1.serverlinux.vn. root.serverlinux.vn. (
                  2011022700 ; Serial
                  28800; Refresh
                  14400; Retry
                  3600000; Expire
                  86400 ); Minimum
            IN    NSdns1.serverlinux.vn.
```

```
            IN    MX    1     dns1.serverlinux.vn.
dns1  IN    A     192.168.1.3
www   IN    CNAME dns1.serverlinux.vn.
mail  IN    CNAME dns1.serverlinux.vn.
ftp   IN    CNAME dns1.serverlinux.vn.
proxy IN    CNAME dns1.serverlinux.vn.
```

f) Cấu hình site vftp.serverlinux.vn

- Cấu hình tập tin /etc/vsftpd/ftp_ao.conf

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=NO
anon_root=/ftproot
#
# Uncomment this to allow local users to log in.
local_enable=YES
#thêm vào các dòng sau ở cuối file (nếu dòng nào có rồi thì không cần phải
thêm)
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
#local_root=public_html
use_localtime=YES
listen_address=192.168.1.6
```

- Cấu hình fns về tên miền vftp.serverlinux.vn

```
$TTL  86400
@INSOAdns1.serverlinux.vn. root.serverlinux.vn.(
                  2011022700 ; Serial
                  28800; Refresh
                  14400; Retry
                  3600000; Expire
                  86400 ); Minimum
            IN    NSdns1.serverlinux.vn.
            IN    MX          1     dns1.serverlinux.vn.
dns1  IN    A     192.168.1.3
www   IN    CNAME dns1.serverlinux.vn.
mail  IN    CNAME dns1.serverlinux.vn.
ftp   IN    CNAME dns1.serverlinux.vn.
proxy IN    CNAME dns1.serverlinux.vn.
vftp  IN    A     192.168.1.6
```

g) Kiểm tra sự hoạt động

- Khởi động named

```
root@localhost network-scripts]#/etc/init.d/named restart
Stopping named:                    [OK]
Starting named:                    [OK]
```

- Khởi động vsftpd

```
root@localhost network-scripts]# /etc/init.d/vsftpd restart
Shutting down vsftpd:              [OK]
Starting vsftpd for ftp_ao:        [OK]
Starting vsftpd for vsftpd:        [OK]
root@localhost network-scripts]# pgrep vsftpd
7904
7909
root@localhost network-scripts]# host frp.serverlinux.vn
Host frp.serverlinux.vn not found: 3(NXDOMAIN)
root@localhost network-scripts]# host ftp.serverlinux.vn
ftp.serverlinux.vn is an alias for dns1.serverlinux.vn.
dns1.serverlinux.vn has address 192.168.1.3
[root@localhostnetwork-scripts]# host vftp.serverlinux.vn
vftp.serverlinux.vn has address 192.168.1.6
```

5.4. DỊCH VỤ WEB

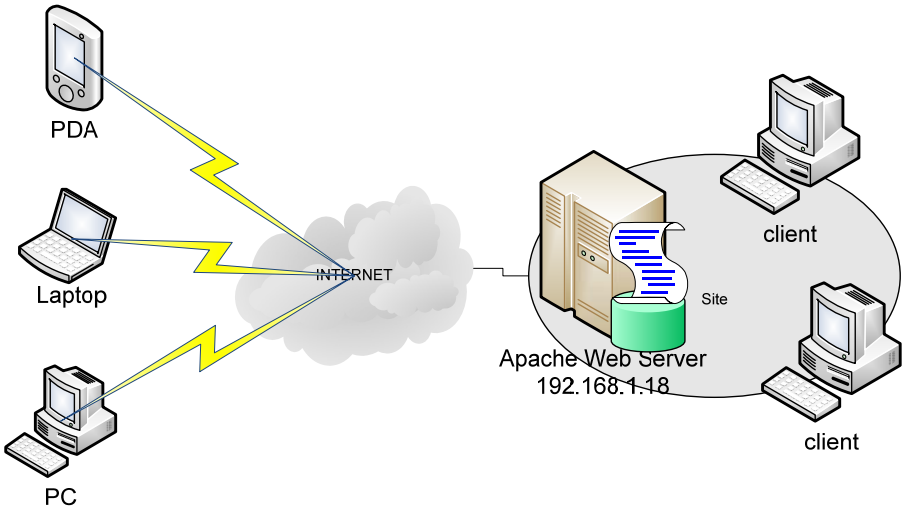
5.4.1. GIỚI THIỆU WEB SERVER

Apache là một phần mềm có nhiều tính năng mạnh và linh hoạt dùng để làm Web Server.

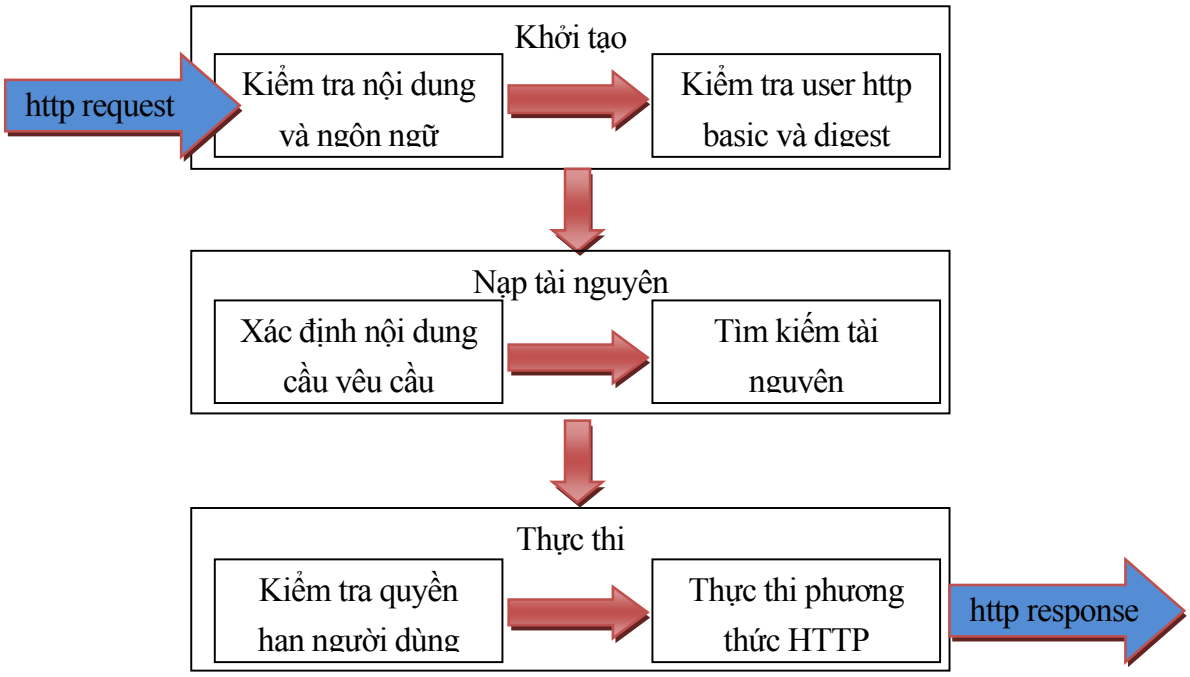
- Hỗ trợ đầy đủ những giao thức HTTP trước đây như HTTP/1.1
- Có thể cấu hình và mở rộng với những module của công ty thứ ba
- Cung cấp source code đầy đủ với Clicense không hạn chế.
- Chạy trên nhiều hệ điều hành như Windows NT/9x, Netware 5.x, OS/2 và trên hầu hết các hệ điều hành Unix

5.4.2. THỰC HÀNH 1: CẤU HÌNH APACHE WEB SERVER

MÔ HÌNH VÀ YÊU CẦU BÀI TẬP



MÔ HÌNH HOẠT ĐỘNG



HƯỚNG DẪN THỰC HIỆN

a. Chuẩn bị nội dung website
b. Đăng ký tên web site
c. Cấu hình Apache web server
d. Khai báo servername
    - Khai báo DocumentRoot
    - Khai báo DirectoryIndex
e. Reload web service
f. Kiểm tra

CÁC BƯỚC THỰC HIỆN

a) Tạo nội dung trang web

```
#cat  >     /var/www/html/index.htm
<html>
<body>
Day la trang web www.serverlinux.vn
</body>
</html>
```

b) Đăng tên web site trong tập tin zone thuận của DNS

```
[root@localhost named]# vi serverlinux.thuan
$TTL    86400
@   IN  SOA dns.serverlinux.vn. root.serverlinux.vn. (
                        2011042700 ; Serial
                        28800      ; Refresh
                        14400      ; Retry
                        3600000    ; Expire
                        86400 )    ; Minimum
       IN      NS      dns.serverlinux.vn.
       IN      MX      10      mail.serverlinux.vn.
dns    IN      A       192.168.1.17
www    IN      A       192.168.1.18
mail   IN      A       192.168.1.19
ftp    IN      CNAME   mail.serverlinux.vn.
proxy  IN      CNAME   mail.serverlinux.vn.
```

c) Kiểm tra host www.serverlinux.vn

```
[root@localhost named]# /etc/init.d/named restart
Stopping named:                        [  OK  ]
Starting named:                        [  OK  ]
[root@localhost named]#
[root@localhost named]# host www.serverlinux.vn
www.serverlinux.vn has address 192.168.1.18
```

d) Cấu hình /etc/httpd/conf/httpd.conf

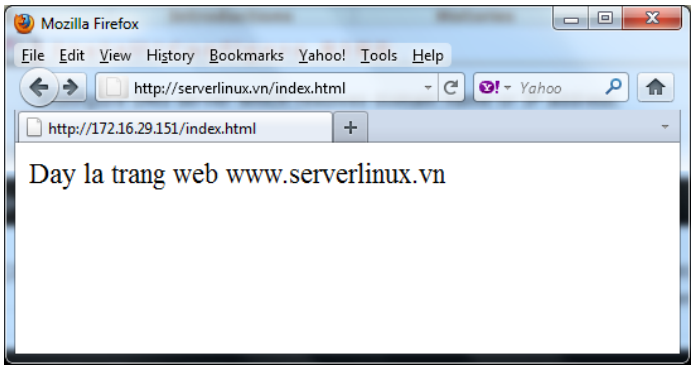
```
#Thay đổi dòng 265:
ServerName www.serverlinux.vn:80
# Cấu hình tên máy tính (hostname) của server. Nó được dùng trong việc tạo
ra những URL chuyển tiếp (redirection URL). Nếu không chỉ ra, server sẽ cố
gắng suy luận từ địa chỉ IP của nó. Tuy nhiên, điều này có thể không tin
cậy hoặc không trả ra tên máy tính đúng.
#Thay đổi dòng 262
ServerAdmin       root@serverlinux.vn
# ServerAdmin: Địa chỉ Email của người quản trị
#Thay đổi dòng 292
DocumentRoot      /var/www/html
# Cấu hình thư mục gốc lưu trữ nội dung của Website. Web Server sẽ lấy
những tập tin trong thư mục này phục vụ cho yêu cầu của client.
ServerRoot /etc/httpd
#Chỉ định vị trí cài đặt chương trình Apache.
Listen       80
```

```
#Qui định địa chỉ IP hoặc cổng mà Apache nhận kết nối từ client, mặc định
hệ thống sử dụng mọi địa chỉ ip trên card mạng và số hiệu cổng là 80.
BindAddress 192.168.1.18
TimeOut 300
# Qui định thời gian tồn tại (sống) của một kết nối (được tính bằng giây)
một khi client kết nối vào Web server.
#Thay đổi dòng 76
KeepAlive On
#Cho phép hoặc không cho phép client gửi được nhiều yêu cầu dựa trên một
kết nối với Web Server.
#Thay đổi dòng 83
MaxKeepAliveRequests 100
#Số Request tối đa trên một kết nối (nếu cho phép nhiều Request trên một
kết nối).
#Thay đổi dòng 89
KeepAliveTimeout 15
#Qui định thời gian để chờ cho một yêu cầu (request) kế tiếp từ một client
trên cùng một kết nối (được tính bằng giây).
# Qui định cơ chế liên kết địa chỉ IP với cổng ứng dụng cho Web server.
#Thay đổi dòng dòng  402:
DirectoryIndex index.html index.html.var index.htm index.php
```

e) Khởi động lại dịch vụ httpd

```
[root@WEBServer conf]# /etc/init.d/httpd        restart
Stopping httpd:                            [  OK  ]
Starting httpd:                            [  OK  ]
[root@WEBServer conf]# chkconfig    http  on
```

f) Truy cập vào web server với địa chỉ http://serverlinux.vn



5.4.3. THỰC HÀNH 2: CẤU HÌNH WEB ĐỘNG PHP – MYSQL

Trong phần này ta sẽ tìm hiểu cách cấu hình một website hỗ trợ Web động PHP sử dụng cơ sở dữ liệu MySQL. Trong phần này ta chỉ cài đặt PHP, MySQL và biết cách cấu hình Website hỗ trợ ngôn ngữ PHP.

Kiểm tra phần mềm httpd đã cài đặt hay chưa

```
[root@localhost ~]# rpm -qa httpd
httpd-2.2.15-5.el6.centos.i686
[root@localhost ~]# rpm -qa php
php-5.3.3-3.el6_1.3.i686
[root@localhost ~]# rpm -qa mysql
mysql-5.1.52-1.el6_0.1.i686
```

Cài đặt php

Cài đặt PHP bằng tùy chọn YUM: #yum –y install php*

```
[root@localhost ~]# yum -y install php*
Resolving Dependencies
--> Running transaction check
---> Package unixODBC.i686 0:2.2.14-11.el6 set to be updated
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
 Package       Arch      Version                 Repository        Size
================================================================================
Installing:
 php-bcmath    i686      5.3.3-3.el6_1.3       updates     32 k
 php-dba       i686      5.3.3-3.el6_1.3       updates     38 k
 php-devel     i686      5.3.3-3.el6_1.3       pdates    505 k
Transaction Summary
================================================================================
Install      27 Package(s)
Upgrade       0 Package(s)
Total download size: 6.3 M
Installed size: 21 M
Downloading Packages:
(1/27): aspell-0.60.6-12.el6.i686.rpm                    | 629 kB     00:00
……
(27/27): unixODBC-2.2.14-11.el6.i686.rpm                 | 382 kB     00:00
--------------------------------------------------------------------------------
Total                                          1.2 MB/s | 6.3 MB     00:05
```

```
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : 1:php-pear-1.9.0-2.el6.noarch          1/27
……….
  libtidy.i686 0:0.99.0-19.20070615.1.el6    recode.i686 0:3.6-28.1.el6
  unixODBC.i686 0:2.2.14-11.el6
Complete!
```

Cấu hình/etc/httpd/conf/httpd.conf

- DirectoryIndex index.htm index.php
- AddType application/x-httpd-php.php
- Khởi tạo lại dịch vụ httpd và kiểm tra

Tạo dữ liệu PHP và chép vào thư mục /var/www/html

a) Tạo trang index.htm

```
<html>
<body>
<form action="welcome.php" method="post">
      Name: <input type="text" name="name"/>
                  Age: <input type="text" name="age" />
                  <input type="submit" />
</form>
</body>
</html>
```

Trang này cung cấp hai input field và nút submit để người dùng điền thông tin tên, tuổi, sau đó submit để gởi đến file welcome.php để hiển thị kết quả. Tạo trang welcome.php

```
<html>
<body>
            Welcome <?php echo $_POST["name"]; ?>.<br />
            You are <?php echo $_POST["age"]; ?> years old.
</body>
</html>
```

b) Thêm hai tùy chọn trong cấu hình /etc/httpd/conf/httpd.conf

```
#Thay đổi dòng 402
DirectoryIndex index.html index.php
#Thay đổi dòng 765
AddType application/x-httpd-php.php
```

c) Khởi tạo lại dịch vụ httpd và kiểm tra

```
#service httpd restart
```

5.4.4. THỰC HÀNH 3: CẤU HÌNH WEB SERVERCHỨNG THỰC BASIC

Cơ sở lý thuyết

Đối với những thông tin cần bảo mật, khi có yêu cầu truy xuất thông tin này, Web Server phải chứng thực những yêu cầu này có hợp lệ hay không. Thông thường, thông tin chứng thực bao gồm username và password.

Nguyên tắc hoạt động:

- Nếu một tài nguyên được bảo vệ với sự chứng thực. Apache sẽ gửi một yêu cầu "401 Authentication" thông báo cho người dùng nhập vào username và password của mình. Nhận được yêu cầu này, client sẽ trả lời 401 đến server trong đó có chứa username và password. Server sẽ kiểm tra những thông số này khi nhận được. Nếu hợp lệ server sẽ trả về những thông tin yêu cầu, ngược lại nó sẽ trả về một thông báo lỗi.
- Username và password bạn cung cấp chỉ có tác dụng trong lần giao dịch của browser với server lúc đó.
- Nếu lần sau truy cập lại website này, bạn phải nhập lại username và password.
- Song song với trả lời 401, toàn bộ thông tin sẽ trả ngược lại cho client. Trong những trường hợp riêng biệt, server sẽ cấp lại cho client một thẻ chứng thực để bảo vệ website. Thẻ này được gọi là realm hay là một tên chứng thực. Browser sẽ lưu lại username và password mà bạn đã cung cấp cùng với realm. Như thế, nếu truy cập những tài nguyên khác mà có cùng realm, username và password thì user không cần nhập trở lại những thông tin chứng thực. Thông thường, việc lưu trữ này chỉ có tác dụng trong giao dịch hiện hành của browser. Nhưng cũng có một vài browser cho phép bạn lưu chúng một cách cố địnhđể bạn chẳng bao giờ nhập lại username và password.

Các bước cấu hình chứng thực:

- **Bước 1:** Tạo tập tin password, tập tin password cần phải tạo trên Server. Tiện ích htpasswd giúp tạo tập tin password một cách dễ dàng. Cách sử dụng tiện ích như sau: `#htpasswd -c <vị_trí_tập_tin_password><username>`
  - Ví dụ 5.4.1:

```
# htpasswd -c /etc/httpd/conf/passwords rbowen
New password: mypassword
Re-type new password: mypassword
```

Tùy chọn –c sẽ tạo một tập tin password mới. Nếu tập tin này đã tồn tại nó sẽ xóa nội dung cũ và ghi vào nội dung mớitại thư mục gốc của apache

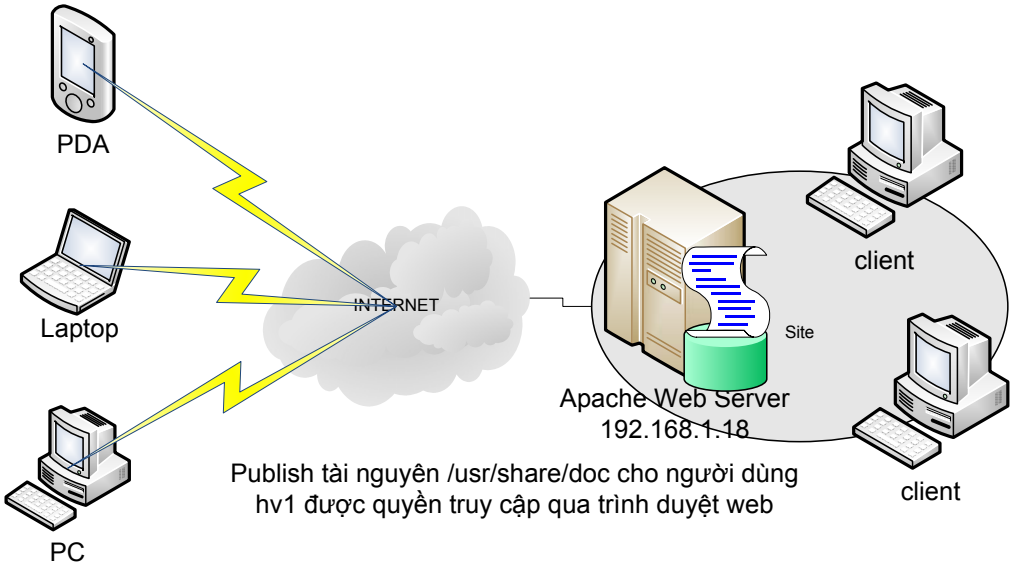
- **Bước 2**: Cấu hình sự chứng thực trên Apache:

```
<Directory /upload>
EnablePut On
AuthType Basic
AuthName Temporary
AuthUserFile /etc/httpd/conf/passwd
EnableDelete Off
umask 007
<Limit PUT>
require user rbowen sungo
</Limit>
</Directory>
```

- **Bước 3**: Tạo tập tin group, Apache hỗ trợ thêm tính năng nhóm người dùng. Người quản trị có thể tạo những nhóm người dùng được phép truy cập đến tài nguyên. Định dạng của tập tin group:<tên nhóm>: user1 user2 user3 … usern
  - Ví dụ 5.4.2:authors: rich daniel allan
  - Sau khi tạo tập tin nhóm, bạn cần cấu hình để apache để chỉ ra tập tin nhóm này bằng những directive sau:

```
<Directory /upload>
      AuthType Basic
      AuthName "Apache Admin Guide Authors"
      AuthUserFile /etc/httpd/conf/passwords
      AuthGroupFile /etc/httpd/conf/groups
      Require group authors
</Directory>
```

Mô hình và yêu cầu bài tập



Hướng dẫn cấu hình

- Cấu hình Apache web server
  - Khai báo Virtual Dir
  - Cấu hình chúng thực Basic
- Reload web service
- Kiểm hoạt hoạt động

Các bước cấu hình

Bước 1: Cấu hình /etc/httpd/conf/httpd.conf. Thêm vào một số code như bên dưới:

```
 Alias /tailieu"/user/share/doc"
<Directory /usr/share/doc>
AuthTypeBasic
AuthNameChung_thuc_Basic
AuthUserFile/etc/httpd/conf/password
Require user hocvien sinhvien
Options Indexes MultiViews
Order allow,deny
Allow from all
</Directory>
```

Giải thích:

- AuthType: khai báo loại authentication sẽ sử dụng. Trong trường hợp này là Basic
- AuthName: đặt tên cho sự chứng thực.

- AuthUserFile: Chỉ định vị trí của tập tin password.
- AuthGroupFile: Chỉ định vị trí của tập tin group.
- Require: những yêu cầu hợp lệ được cho phép truy cập tài nguyên.

Bước 2:Khởi động lại dịch vụ httpd

```
[root@webserver conf]# /etc/init.d/httpd restart
Stopping httpd:          [OK]
Starting httpd:          [OK]
```

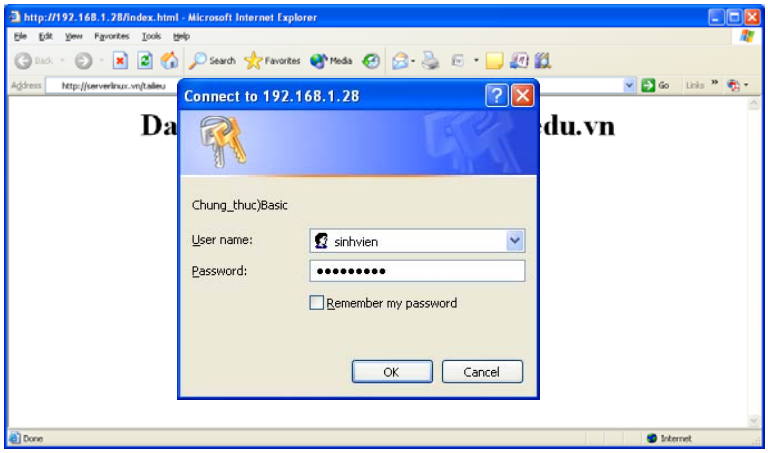
Bước 3: Tạo tài khoản sinh viên và tạo chứng thực

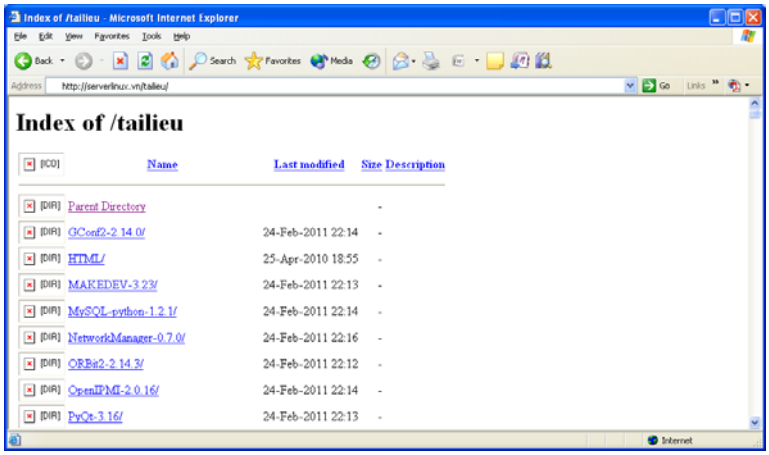
```
[root@webserver conf]# useradd sinhvien
[root@webserver conf]# passwd sinhvien
Changing password for user sinhvien.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@webserver conf]# htpasswd -c /etc/httpd/conf/password sinhvien
New password:
Re-type new password:
Adding password for user sinhvien
```

Bước 4: Khởi động lại dịch vụ mạng

```
[root@dns html]# /etc/init.d/httpd restart
Stopping httpd:                [OK]
Starting httpd:                [OK]
```

Bước 5: truy cập trang web serverlinux.vn





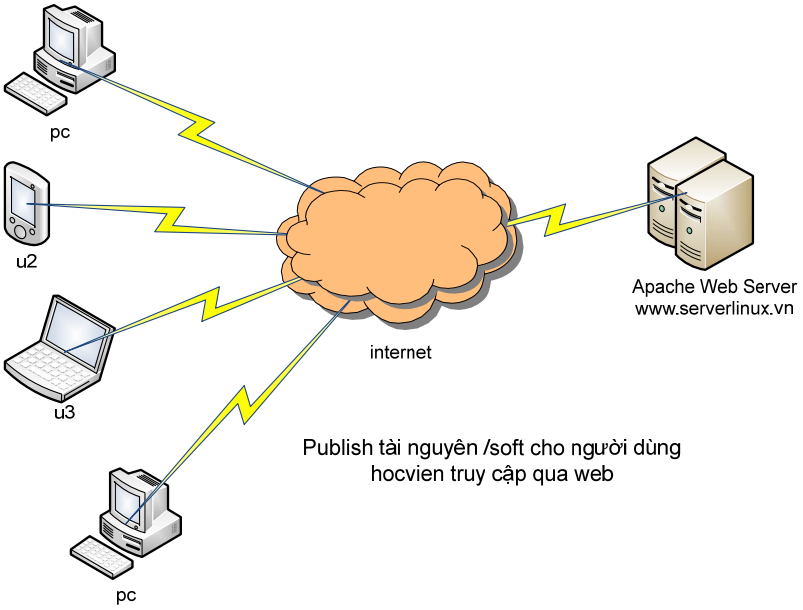
[root@webserver conf]# lynx http://serverlinux.vn/tailieu

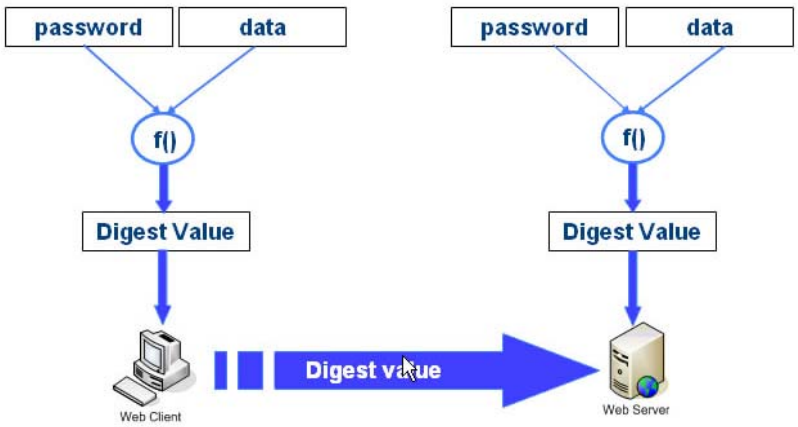
5.4.5. CẤU HÌNH CHỨNG THỰC DIGEST

Cơ sở lý thuyết

Digest authentication cung cấp một phương pháp bảo vệ nội dung web một cách luân phiên. Digest authentication được cung cấp bởi module mod_auth_digest, với phương pháp này tên user và mật khẩu sẽ không được gởi ở dạng plain text mà chúng được mã hóa (thông qua thuật toán MD5).

Mô hình và yêu cầu bài tập





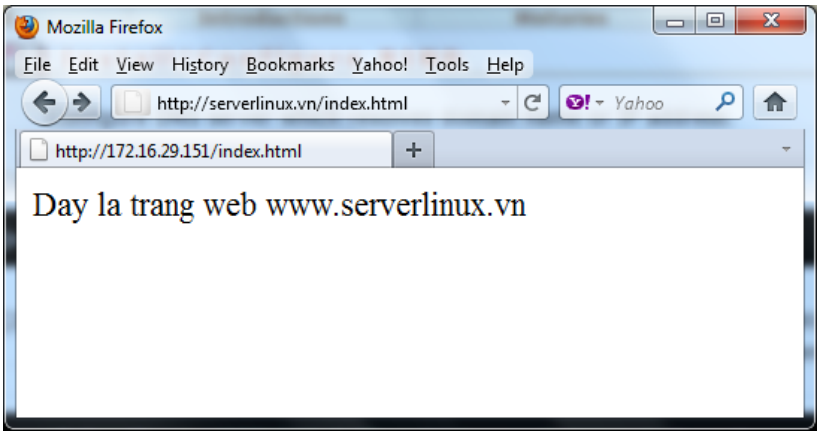
Hướng dẫn thực hiện

a) Cấu hình apache web server

   1) Khai báo virtual dir
   2) Cấu hình chứng thực Digest

b) Reload web service

c) Kiểm tra



Thực hiện cấu hình

a) Bước 1: Cấu hình /etc/httpd/conf/httpd.conf. Thêm vào một số code như bên dưới:

```
Alias /chiase  "/soft"
<Location /chiase>
        AuthType        Digest
        AuthName        private
        AuthDigestProvider      file
        AuthUserFile    /etc/httpd/conf/dpassword
        Require user linux hocvien
        Options Indexes MultiViews
        Order allow,deny
        Allow from all
</Location>
```

b) Bước 2:Khởi động lại dịch vụ httpd

```
[root@dns html]# /etc/init.d/httpd restart
Stopping httpd:          [OK]
Starting httpd:          [OK]
```

c) Bước 3: tạo tài khoản hocvien

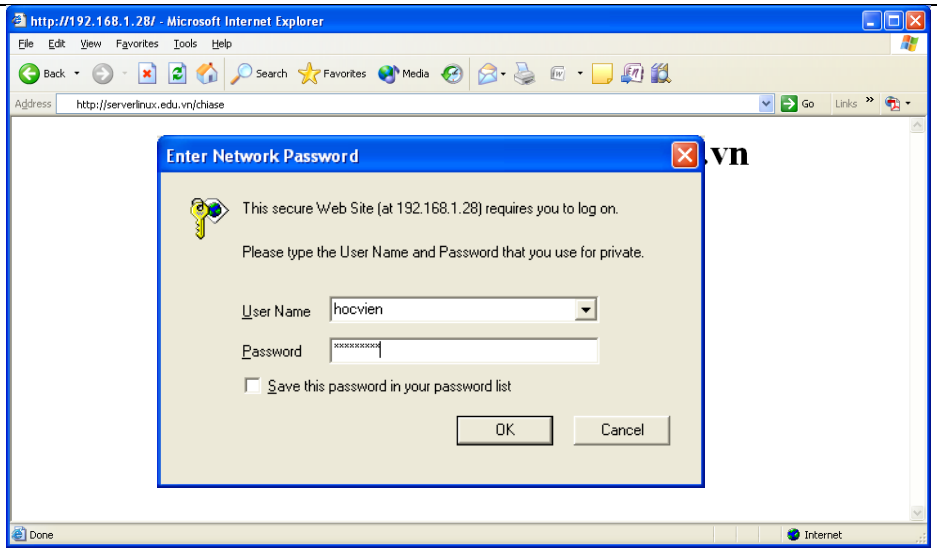
```
[root@dns html]# useradd hv1
[root@dns html]# passwd hv1
Changing password for user hv1.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

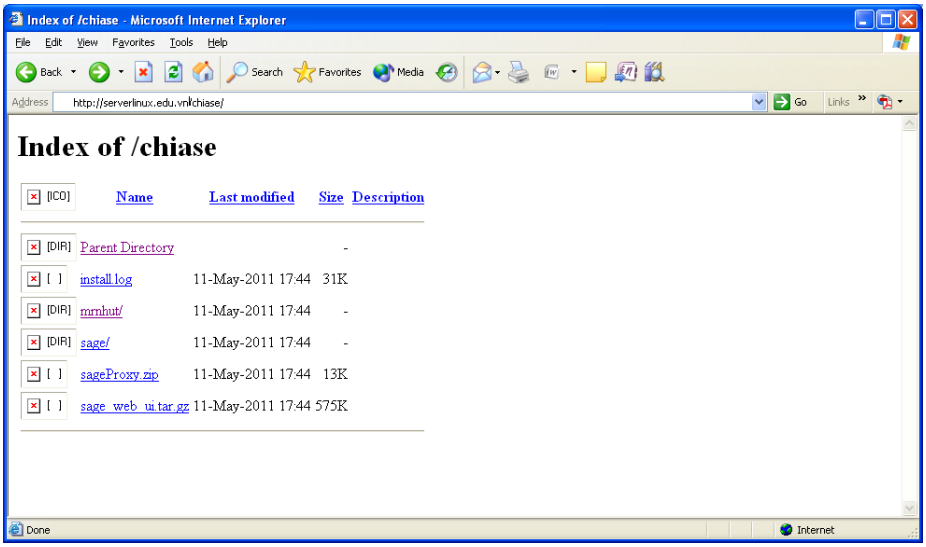
d) Bước 4: Tạo mật khẩu chứng thực truy cập hệ thống webserver cho user hocvien

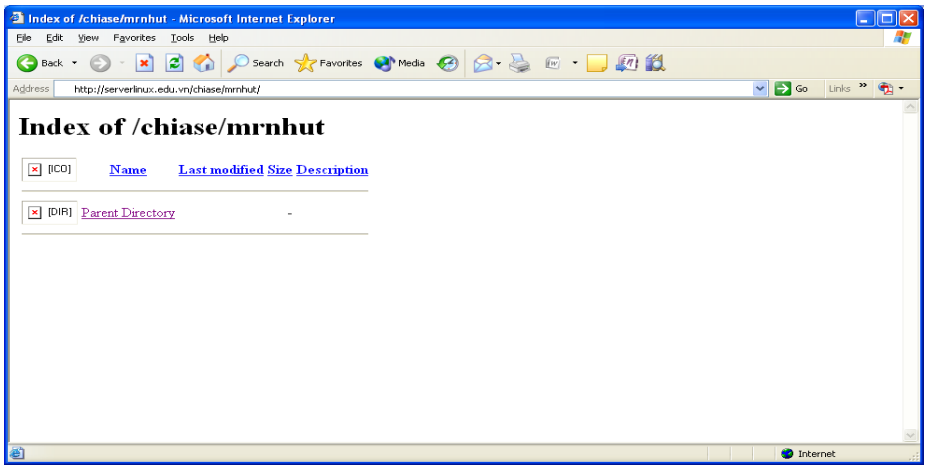
```
[root@dns conf]#htdigest -c /etc/httpd/conf/dpassword private hv1
Adding password for hv1 in realm private.
New password:
Re-type new password:
```

e) Bước 5: Khởi động lại dịch vụ mạng

```
[root@dns html]# /etc/init.d/httpd restart
Stopping httpd:          [OK]
Starting httpd:          [OK]
```

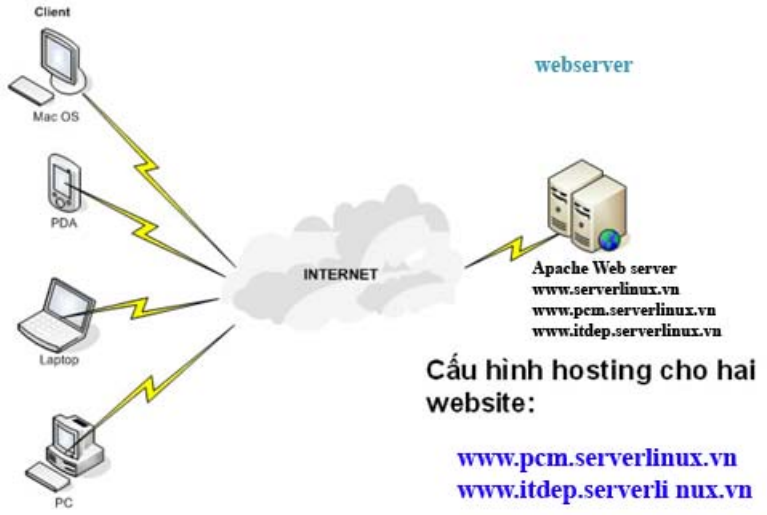



Index of /chiase - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://serverlinux.edu.vn/chiase/
Go Links
Index of /chiase
[ICO] Name Last modified Size Description
[DIR] Parent Directory -
[ ] install.log 11-May-2011 17:44 31K
[DIR] mrnhut/ 11-May-2011 17:44 -
[DIR] sage/ 11-May-2011 17:44 -
[ ] sageProxy.zip 11-May-2011 17:44 13K
[ ] sage_web_ui.tar.gz 11-May-2011 17:44 575K
Done
Internet


Index of /chiase/mrnhut - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://serverlinux.edu.vn/chiase/mrnhut/
Go Links
Index of /chiase/mrnhut
[ICO] Name Last modified Size Description
[DIR] Parent Directory -
Internet

5.4.6. CẤU HÌNH HOSTING WEBSITE

Mô hình và yêu cầu bài tập



Hướng dẫn thực hiện

a. Cấu hình Apache web server
   1) Khai báo NameVirtualHost
   2) Khai báo Virtualhost

b. Reload web service

c. Kiểm tra

Các bước thực hiện

a) Khai báo DNS Server

```
$TTL86400
@           IN    SOA   dns1.serverlinux.vn.root.     serverlinux.vn. (
                        2011022700 ; Serial
                        28800; Refresh
                        14400; Retry
                        3600000; Expire
                        86400 ); Minimum
            IN    NS    dns1.serverlinux.vn.
```

```
            IN    MX    10dns1.serverlinux.vn.
dns1  IN    A     192.168.1.17
www   IN    A     192.168.1.18
mail  IN    CNAME dns.serverlinux.vn.
ftp   IN    CNAME dns.serverlinux.vn.
proxy IN    CNAME dns.serverlinux.vn.
www.pcm     IN    A     192.168.1.18
www.itdep   IN    A     192.168.1.18
```

b) Khởi động DNS Server

```
[root@localhost ~]# /etc/init.d/named restart
Stopping named:                                    [  OK  ]
Starting named:                                    [  OK  ]
[root@localhost ~]# chkconfig named on
```

c) Kiểm tra hoạt động của host dns

```
[root@DNS conf]# host www.itdep.serverlinux.vn
www.itdep.serverlinux.vn is an alias for dns.serverlinux.vn.
dns.serverlinux.vn has address 192.168.1.17

[root@DNS conf]# host www.pcm.serverlinux.vn
www.pcm.serverlinux.vn is an alias for dns.serverlinux.vn.
dns.serverlinux.vn has address 192.168.1.17

[root@DNS conf]# host www.serverlinux.vn
www.serverlinux.vn is an alias for dns.serverlinux.vn.
dns.serverlinux.vn has address 192.168.1.17
```

d) Tạo thư mục VirtualHost

```
[root@DNS conf]#mkdir /webhosting
[root@DNS conf]#mkdir /webhosting/pcm/webhosting/itdep
[root@DNS conf]vi /webhosting/pcm/index.html
<html>
<body>
      Day la trang web www.pcm.serverlinux.vn
</body>
</html>
[root@DNS conf]vi /webhosting/ itdep/index.html
<html>
<body>
Day la trang web www.itdep.serverlinux.vn
```

```
</body>
</html>
```

e) Phần quyền cho các thư mục

- [root@DNS conf]chmod 777 /webhosting/pcm/index.html/webhosting/itdep/index.html

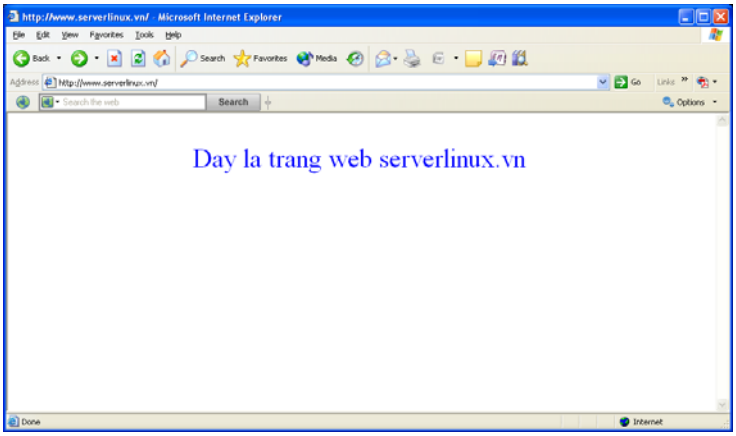
f) Cấu hình virtual host trong /etc/http/conf/httpd.conf

```
NameVirtualHost 192.168.1.17
#
……..
#<VirtualHost *:80>
#ServerAdmin webmaster@dummy-host.example.com
#DocumentRoot /www/docs/dummy-host.example.com
#ServerName dummy-host.example.com
#ErrorLog logs/dummy-host.example.com-error_log
#CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

<VirtualHost 192.168.1.17>
      DocumentRoot /var/www/html
      ServerName www.serverlinux.vn
</VirtualHost>

<VirtualHost 192.168.1.17>
      DocumentRoot /webhosting/pcm
      ServerName www.pcm.serverlinux.vn
</VirtualHost>

<VirtualHost 192.168.1.17>
      DocumentRoot /webhosting/itdep
      ServerName www.itdep.serverlinux.vn
</VirtualHost>
```

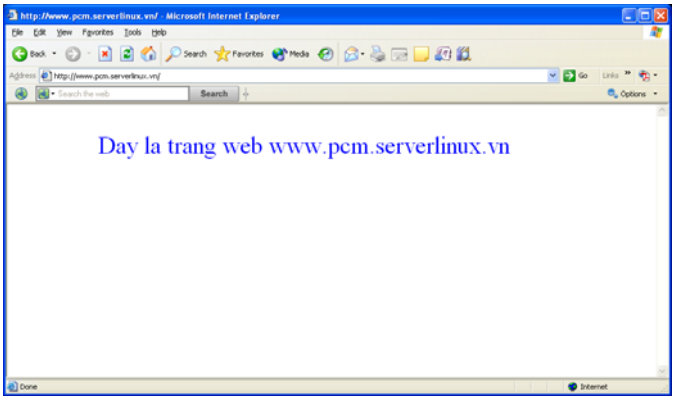
g) Khởi động httpd

```
[root@DNS conf]# /etc/init.d/httpd restart
Stopping httpd:          [OK]
Starting httpd:          [OK]
[root@DNS conf]# chkconfig httpd on
```

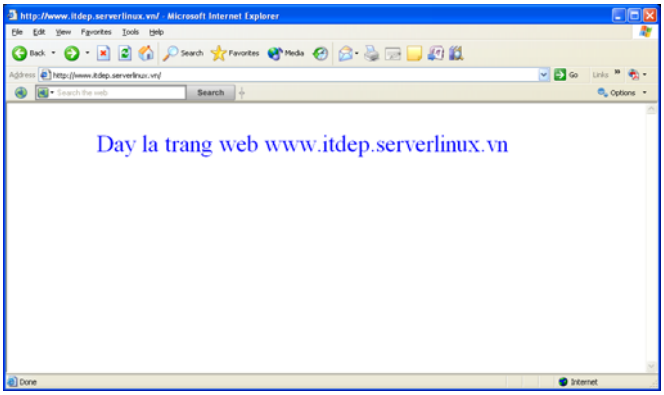
h) Truy cập vào web server http://serverlinux.vn



i) Truy cập vào web server http://pcm.serverlinux.vn

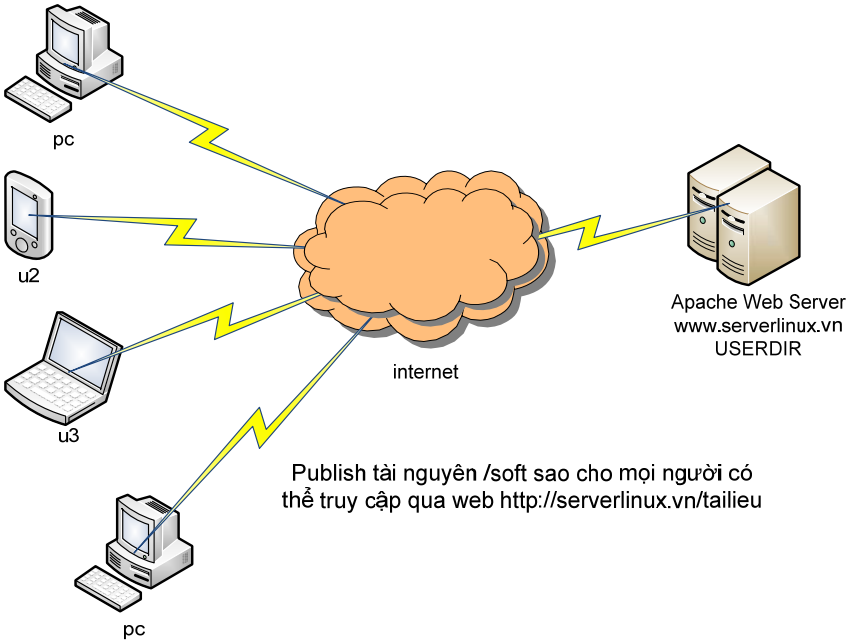


j) Truy cập vào web server http://itdep.serverlinux.vn



5.4.7. CẤU HÌNH PUBLISH TÀI NGUYÊN WEB

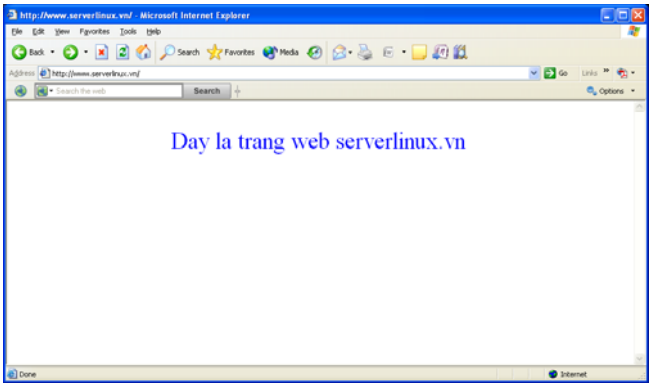
Mô hình và yêu cầu bài tập



Hướng dẫn thực hiện

a. Tạo virtual Directory
b. Khai báo Alias
c. Chỉ định quyền hạn
d. Reload web service
e. Kiểm tra hoạt động của http://serverlinux.vn/tailieu

a) Kiểm tra hoạt động của trang web http://serverlinux.vn/



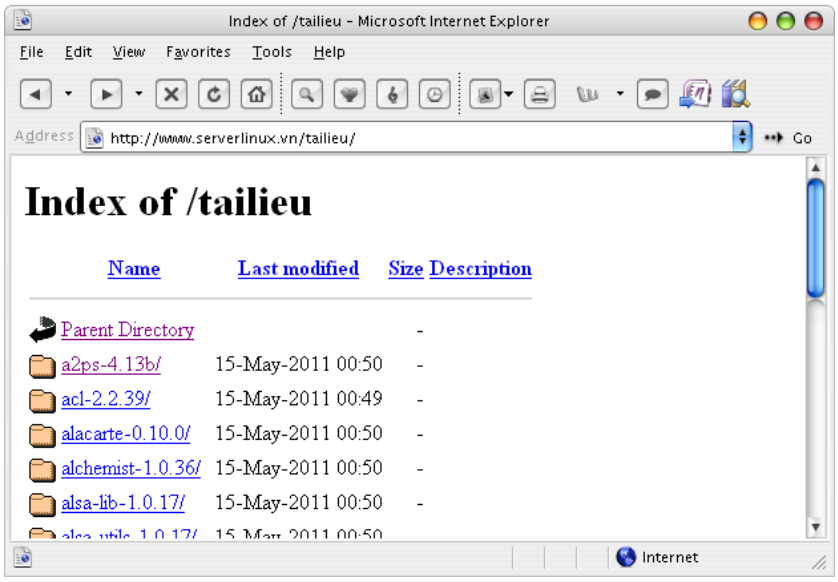
b) Cấu hình Alias trong tập tin cấu hình /etc/httpd/conf/httpd.conf

```
Alias /icons/ "/var/www/icons/"
<Directory "/var/www/icons">
      Options Indexes MultiViews
      AllowOverride None
      Order allow,deny
      Allow from all
</Directory>

Alias /tailieu/soft
<Directory /soft>
      Options Indexes MultiViews
Order allow,deny
      Allow from all
</Directory>
```

c) Khởi động lại web service

```
[root@localhost ~]# /etc/init.d/httpd restart
Stopping httpd:                            [OK]
Starting httpd:                            [OK]
```

d) Từ windows truy cập vào trang http://www.serverlinux.vn/tailieu



e) Giới hạn truy cập

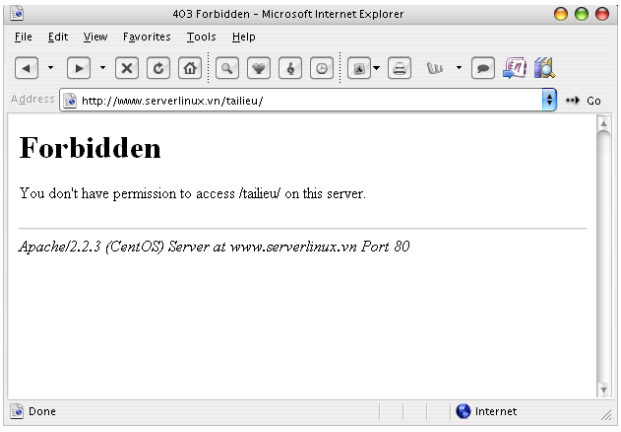
a. Để cấm truy cập vào thư mục tailieu, chúng ta tiến hành bỏ bớt dòngOptions Indexes MultiViews trong tập tin cấu hình httpd.conf như bên dưới:

```
Alias /icons/ "/var/www/icons/"
<Directory "/var/www/icons">
      Options Indexes MultiViews
      AllowOverride None
      Order allow,deny
      Allow from all
</Directory>
Alias /tailieu/soft
<Directory /soft>
#Options Indexes MultiViews
      Order allow,deny
      Allow from all
</Directory>
```

f) Khởi động lại web service

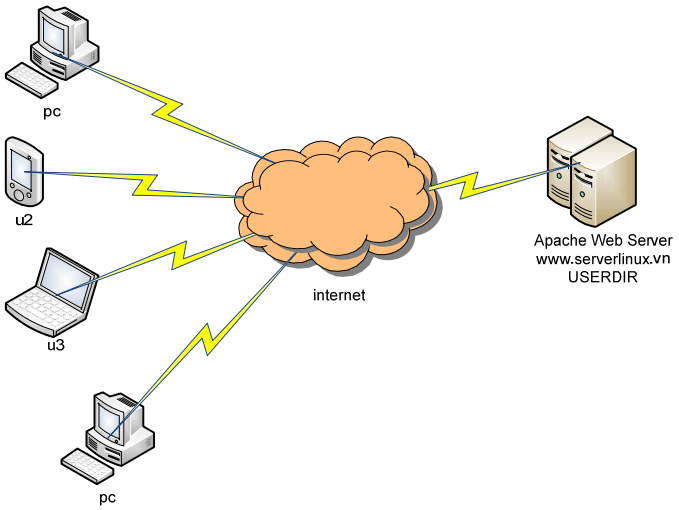
```
[root@localhost ~]# /etc/init.d/httpd restart
Stopping httpd:                [OK]
Starting httpd:                [OK]
```

g) Từ windows truy cập vào trang http://www.serverlinux.vn/tailieu



5.4.8. TẠO WEBSITE CHO NGƯỜI DÙNG

Mô hình và yêu cầu bài tập

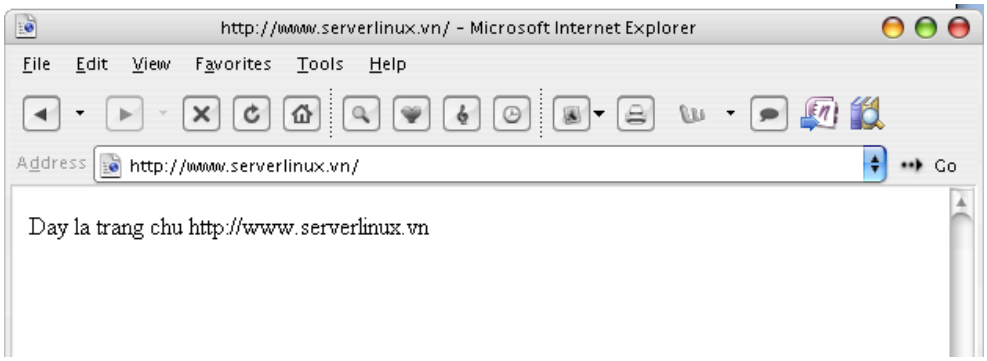


Hướng dẫn thực hiện

b. Tạo userdir
   1) Khai báo UserDir
   2) Cập quyền hạn truy cập
c. Reload web service
d. Kiểm tra hoạt động của trang web

Các bước thực hiện

a) Bước 1: Kiểm tra hoạt động của trang web http://www.serverlinux.vn



b) Bước 2: Cấu hình tập tin httpd.conf cho phép tạo trang web cá nhân cho user. Thêm vào các dòng như bên dưới:

```
Dòng 355 đổi thành: UserDir www
Thêm vào code từ dòng 384 đến dòng 295
<Directory /home/*/www>
AllowOverride FileInfo AuthConfig Limit
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
<Limit GET POST OPTIONS>
      Order allow,deny
      Allow from all
</Limit>
<LimitExcept GET POST OPTIONS>
      Order deny,allow
      Deny from all
</LimitExcept>
</Directory>
```

c) Bước 3: Tạo các user hv1 và hv2 bằng các câu lệnh như bên dưới:

```
[root@localhost ~]# useradd hv1
[root@localhost ~]# passwd hv1
Changing password for user hv1.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# useradd hv2
[root@localhost ~]# passwd hv2
Changing password for user hv2.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

d) Bước 4: Tạo trang web cá nhân trên user hv1

- Tạo thư mục www:

```
[hv1@Webserver ~]$ mkdir www
[hv1@Webserver ~]$ ls
bootstat.dat  explorer.scf  history.txt  JRE32.dll
explorer.exe  FaxSetup.log  index.html   www
```

- Tạo tập tin www/index.html

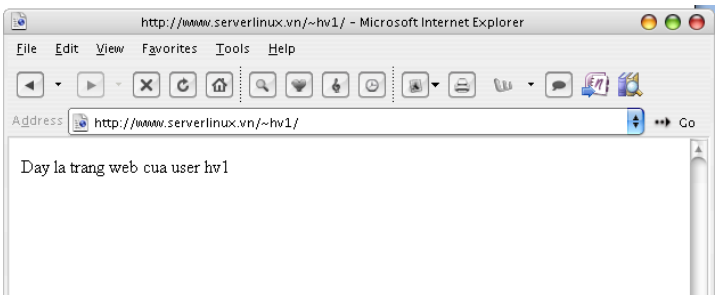
```
[hv1@Webserver ~]$vi index.html
```

```
<html>
<body>
Day la trang web cua user hv1
</body>
</html>
```

- Phân quyền truy cập

```
#chmod 711 /home/*
#chmod 755 /home/hv1/www.index.html
```

e) Bước 5: Truy cập vào trang web http://www.serverlinux.vn/~hv1



f) Bước 6: Làm tương tự cho user hv2

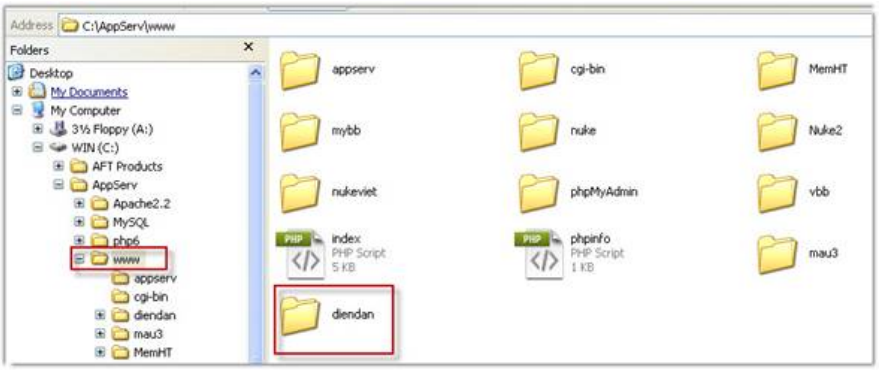
5.4.9. THỰC HÀNH 4: THIẾT LẬP FORUM SỬ DỤNG PHP VÀ MYSQL

Cài đặt MyBB

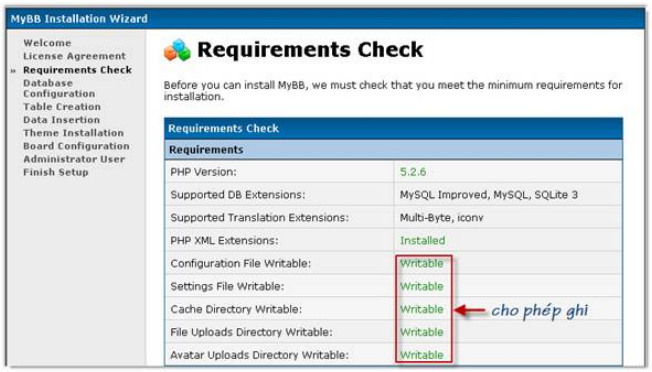
Gói mã nguồn mở được cung cấp hoàn toàn miễn phí tại trang chủ www.mybb.com,tính đến thời điểm viết chuyên đề này MyBB có phiên bản 1.6 với dung lượng nén 1,78MB. Để tải gói mã nguồn, bạn nhấn vào liên kết Download Now> rồi nhấn tiếp Download Now MyBB 1.6

Ngay sau khi tải về, bạn bấm chuột phải vào tập tin mybb_1600.zip chọn Extract Here. Khi đó, trong thư mục sẽ xuất hiện hai thư mục con Upload và Documentation, bạn hãy đổi tên thư mục

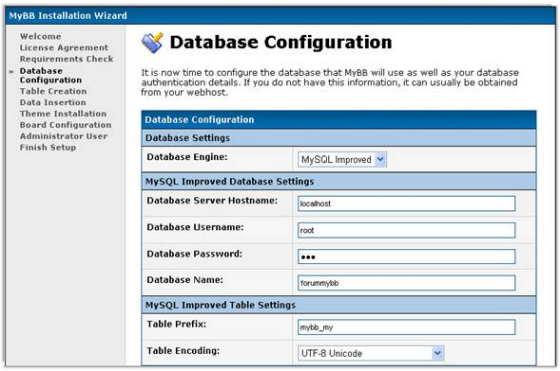
Uploadthành diendan (có thể thành các tên khác cũng được nhưng phải thống nhất cho cả quá trình cài đặt) và sao chép, dán nó vào thư mục www của Appserv.



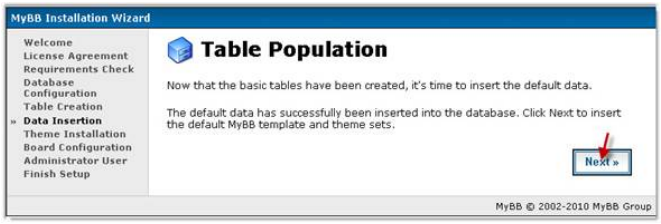
- Khởi động IE rồi nhập vào đường dẫn **localhost/diendan/install/index.php**, nhấn Enter. Quá trình cài đặt MyBB sẽ trải qua 11 bước, bạn nhấn nút Next ở bước đầu tiên, rồi xem qua một số quy định sử dụng mã nguồn ở bước hai, nhấn Next. Kế đến:
- Bước Requirements Check (bước 3): MyBB sẽ kiểm tra các yêu cầu các thông số như: tập tin config.php có thể ghi vào không (Configuration File Writable), thư mục Cache, File Uploads, Avatar Uploads có thể ghi không (Cache-File Uploads-Avatar Uploads Directory Writable), …nhấn Next.



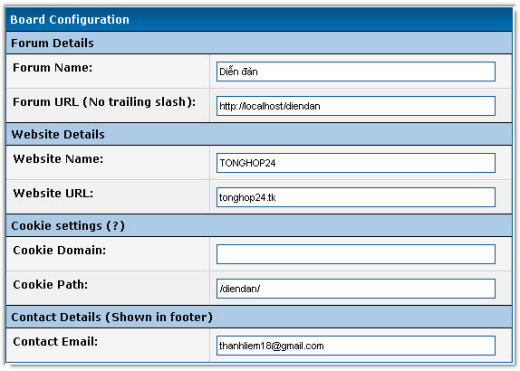
- Bước Database Configuration: Đây là bước quan trọng, cần phải điền đầy đủ và chính xác các thông tin. Gồm có: Database Engine (loại cơ sở dữ liệu nên dùng MySQL Improved), Database Server Hostname (mặc định là localhost), Database Username (nhập vào root), Database Password (mật khẩu), Database Name (tên cơ sở dữ liệu, như đã tạo là forummybb), Table Prefix (tiền tố đứng trước mỗi bảng trong cơ sở dữ liệu), Table Encoding (giữ mặc định). Khi xong nhấn Next để chuyển sang bước kế tiếp.



- Bước *Table Creation* sẽ kết nối và tạo bảng cơ sở dữ liệu, nhấn *Next*.
- Bước *Data Insertion* thông báo việc tạo bảng, đưa dữ liệu cơ bản vào cơ sở dữ liệu thành công, nhấn *Next* để tiếp tục.

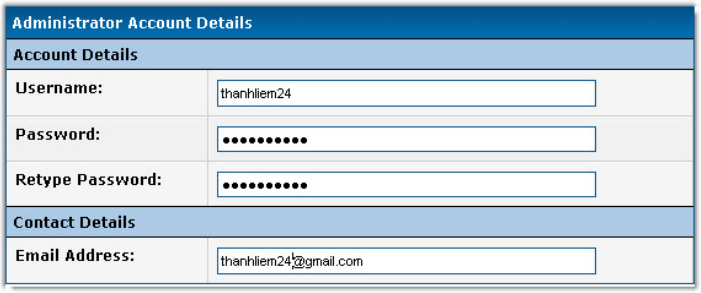


- Bước *Theme Installation* thông báo các chủ đề và mẫu giao diện mặc định đã được cài đặt, nhấn *Next*.
- Bước *Board Configuration*: Bạn đưa ra các thiết lập cơ bản về diễn đàn: *Forum name* (nhập vào tên diễn đàn), *Website name* (có thể để trống hoặc nhập tùy ý), *Website URL* (địa chỉ *website*), *Contact Email* (địa chỉ thư điện tử dùng để *MyBB* liên hệ khi đã cài đặt thành công, thư chỉ được gửi khi cài đặt trên hosting). Các thiết lập này có thể thay đổi sau khi đăng nhập vào *Admin Control Panel*.

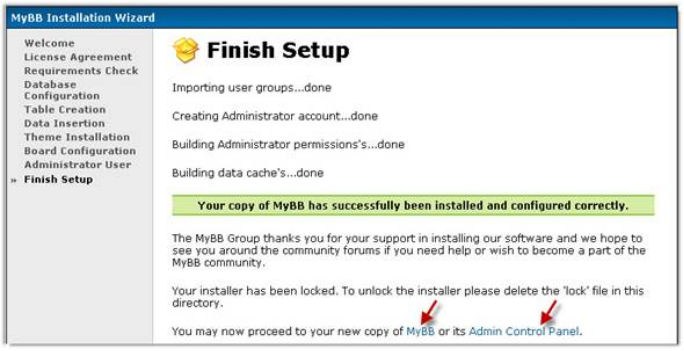


- Bước Administrator User: Bạn điền các thông tin về người quản trị diễn đàn Username (tên tài khoản), Password (mật khẩu quản trị), Retype Password (nhập lại mật khẩu), Email

Address (địa chỉ thư điện tử). Lưu ý, để bảo mật tài khoản quản trị tránh sử dụng các từ Administrator hoặc Admin.



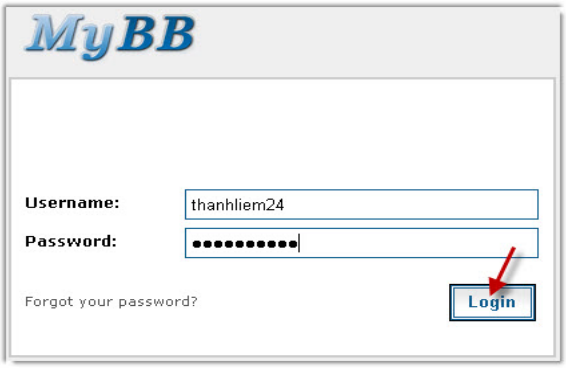
- Bước Finish Setup: Đây là bước cuối cùng của quá trình cài đặt, bạn sẽ thấy thông báo Your copy of MyBB has successfully been installed and configured correctly cho biết đã cài đặt thành công. Bây giờ, bạn có thể nhấn vào liên kết MyBB để truy cập ngay vào diễn đàn hoặc nhấn vào liên kết Admin Control Panel để vào trang quản trị diễn đàn.



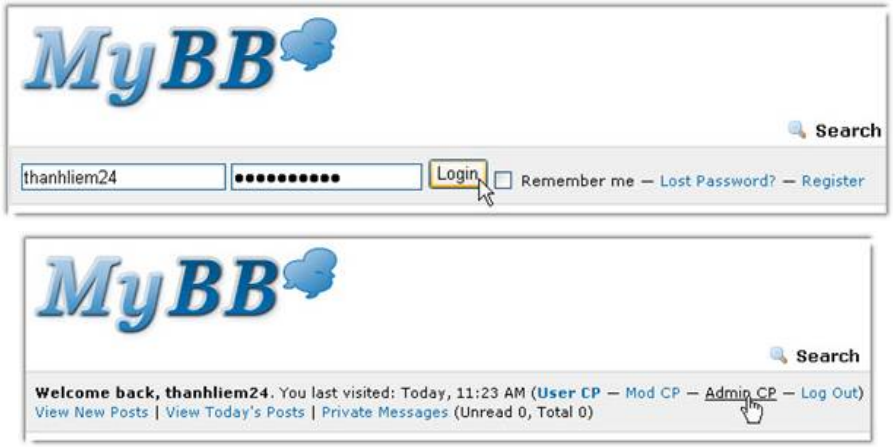
- Lưu ý, kể từ bước 3, việc cài đặt trên hosting sẽ có một số khác biệt trên localhost, sẽ được giới thiệu ở các phần tiếp theo.

Quản lý chuyên mục diễn đàn

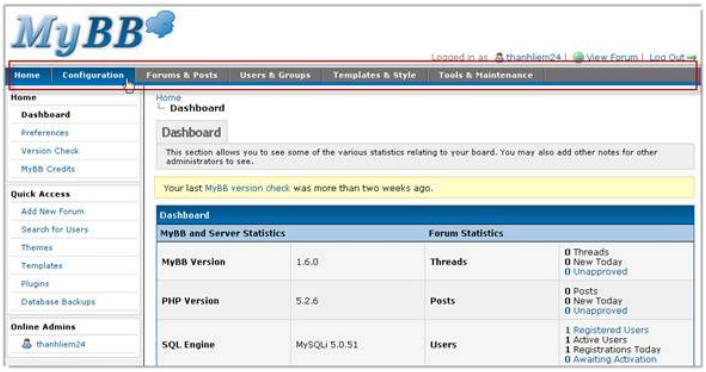
Khi cài đặt xong, bạn đã có một diễn đàn tại địa chỉ http://localhost/diendan và việc cần làm là phải thiết kế lại theo phong cách của mình. Để truy cập vào tài khoản quản trị, bạn truy cập vào http://localhost/diendan/admin/index.php rồi nhập vào Username (tên đăng nhập) và Password (mật khẩu).



- Ngoài ra còn có cách đăng nhập khác là bạn truy cập vào diễn đàn, nhấn liên kết *Login* bên dưới biểu tượng *MyBB*> nhập vào tài khoản quản trị > nhấn nút *Login.* Ở trang hiện ra, bạn nhấn vào liên kết *Admin CP*, rồi nhập lại tài khoản quản trị một lần nữa (gồm có tên đăng nhập và mật khẩu).



- Giao diện trang quản lý khá thân thiện và đơn giản gồm có các menu ngang *Home* (trang chủ của *Admin CP*), *Configuration* (các tính năng thay đổi thiết lập diễn đàn), *Forums & Posts* (quản lý chuyên mục và bài viết), *Users & Groups* (quản lý thành viên và nhóm người dùng), *Templates & Style* (quản lý giao diện), *Tools & Maintenance* (nhóm các công cụ khác).



Quản lý chuyên mục và bài viết

- Vấn đề được xem là quan trọng bậc nhất của diễn đàn có tính chất quyết định đến số lượng khách truy cập, đó chính là nội dung. Do đó, bạn cần xây dựng các chuyên mục và sắp xếp chúng sao cho phù hợp, tiện lợi nhất cho người xem, là rất cần thiết. Với tính năng *Forums & Posts*, bạn sẽ dễ dàng quản lý tất cả các chuyên mục, chuyên mục con và bài viết trên diễn đàn một cách hiệu quả nhất.
- Để thực hiện, bạn nhấn vào menu *Forums & Posts* rồi nhấn nút *Options* (phía sau chữ *My Caterogy*) > chọn *Edit Forum* để thay đổi.

- Ở trang mới hiện ra, bạn đổi lại tiêu đề của nhóm chuyên mục này tại ô *Title* (chẳng hạn đổi *My Category* thành *Về chúng tôi*), nhập vài lời chú thích ngắn tại khung *Description*, các thông tin còn lại giữ nguyên, rồi nhấn nút *Save Forum* ở cuối trang. Khi xong, bạn cũng thực hiện tương tự đối với chuyên mục *My Forum*.

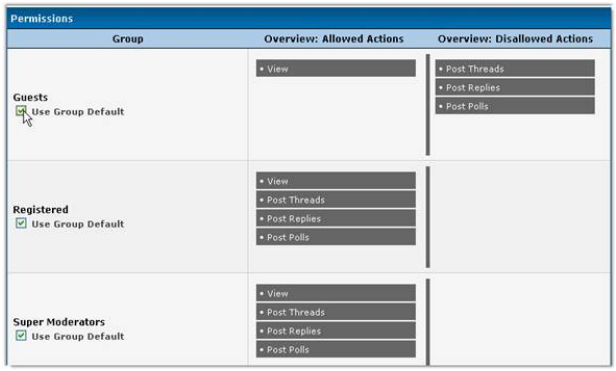
Tạo nhóm chuyên mục mới

- Ngoài nhóm chuyên mục Về chúng tôi, bạn có thể thêm nhiều nhóm chuyên mục khác, bằng cách nhấn vào thẻ Add New Forum (cạnh thẻ Forum Management). Trong khung Add New Forum, bạn chọn Category ở mục Create to, nhập tiêu đề tại ô Title, chú thích ngắn tại Description, Parent Forum (vì tạo nhóm chuyên mục nên giữ nguyên giá trị None), Display Order (thứ tự hiển thị, nhập số 2).

- Về các thiết lập phân quyền bên dưới cứ giữ nguyên, vì nhóm chuyên mục không cần thiết lắm. Khi xong, bạn nhấn *Save Forum*.

Tạo chuyên mục và chuyên mục con

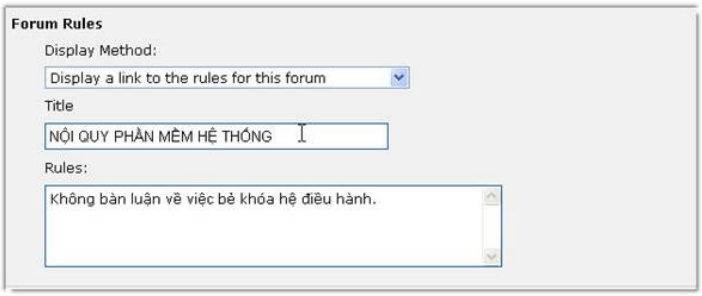
- Sau khi đã tạo nhóm chuyên mục, bạn cần tạo ra các chuyên mục thuộc mỗi nhóm. Bạn cũng nhấn *Add New Forum* để tạo chuyên mục nhưng chọn *Forum* ở mục *Create to* và chọn nhóm chuyên mục chứa nó tại trường *Parent Forum*.
- Kế đến, bạn cần phân quyền hoạt động của chuyên mục cho các nhóm đối tượng truy cập vào diễn đàn *Guest* (khách), *Registered* (thành viên), *Super Moderators* (điều hành viên chính), *Administrator* (quản trị viên), *Awaiting Activation* (thành viên đang chờ kích hoạt), *Moderators* (điều hành viên), *Banned* (đối tượng bị cấm), xong nhấn *Save Forum*.



- Ngoài ra, bạn nhấn vào liên kết *Show Additional Options* để thêm vào những thiết lập khác. Trong số đó có một thiết lập đáng quan tâm như *Forum Password* (mật khẩu truy cập vào

chuyên mục, các nhóm thành viên cũng phải có mật khẩu này mới vào được), *Forum is Active* (nếu không chọn thì người dùng sẽ không xem được chuyên mục), *Forum is Open* (nến không chọn thì người dùng không thể đăng bài), *Moderation Options* (thiết lập kiểm duyệt nội dung mới).

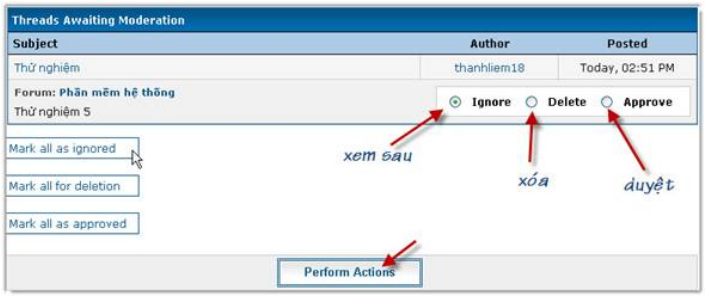
- Riêng đối với mục Forum Rules sẽ giúp bạn đưa ra nội quy sử dụng diễn đàn để các thành viên biết và thực hiện. Bạn chọn các hình thức hiển thị nội quy ở trường Display Method: Don't display rules for this forum (không hiển thi nội quy tại chuyên mục này), Display rules for this forum on the thread listing (hiển thị nội quy trong danh sách chủ đề), Display a link to the rules for this forum (hiển thị tiêu đề liên kết đến nội quy chuyên mục). Bạn nhập tiêu đề vào ô Title, nôi quy chuyên mục vào khung Rules.



Quản lý bài viết, tập tin đính kèm

- Khi thiết lập *Moderation Options* được kích hoạt thì các thành viên đăng bài đều phải chịu sự kiểm duyệt của quản trị viên hay điều hành viên chính. Danh sách các chủ đề mới được hiển thị tại mục *Moderation Queue*, cửa sổ bên phải gồm có ba thẻ quản lý *Threads* (chủ đề chờ duyệt), *Posts* (bài viết chờ duyệt) và *Attachments* (các tập tin đính kèm chờ duyệt).

- Trong khung Threads Awaiting Moderation, bạn sẽ được cung cấp các cột thông tin Subject (chủ đề), Author (tác giả), Posted (thời gian đăng bài). Ở mỗi chủ đề chờ duyệt sẽ có ba lựa chọn: Ingore (để lúc khác kiểm duyệt), Delete (xóa chủ đề), Approve (cho phép đăng chủ đề), xong nhấn Perform Actions để thực hiện tiến trình. Ngoài ra, nếu bạn một xử lý tất cả các chủ đề cùng lúc thì có thể nhấn Mark all as ingored (hoặc Mark all as delection hoặc Mark all as approved).



- Còn đối với các tập tin đính kèm, bạn chuyển sang thẻ *Attachments* rồi cũng thực hiện các thao tác tương tự. Lưu ý, việc cho phép đăng một chủ đề sẽ không liên quan đến tập tin đính kèm của chủ đề đó, tức là tập tin đính kèm vẫn còn nằm trong danh sách chờ duyệt.

Quản lý giao diện diễn đàn

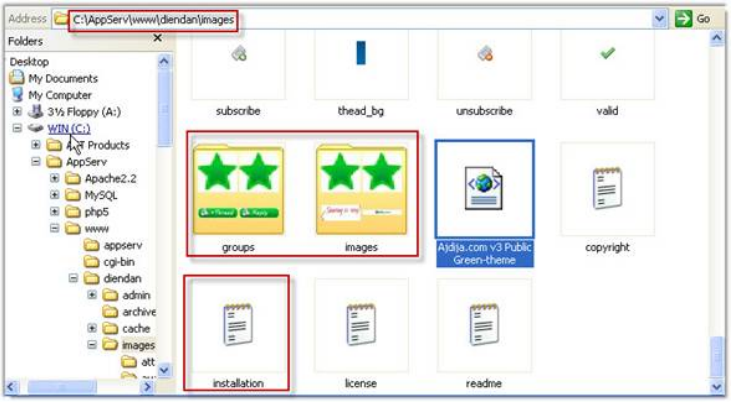
- Một yếu tố khác dẫn đến sự thành công của một diễn đàn là có giao diện đẹp, thân thiện và bắt mắt. *MyBB* cung cấp cho người dùng nhóm tính năng *Templates & Style* giúp dễ dàng quản lý và thay đổi giao diện. Đồng thời, tại đây còn cung cấp một thư viện nhiều mẫu giao diện đẹp, đang được nhiều thành viên của *MyBB* sử dụng.

Cài đặt giao diện mới

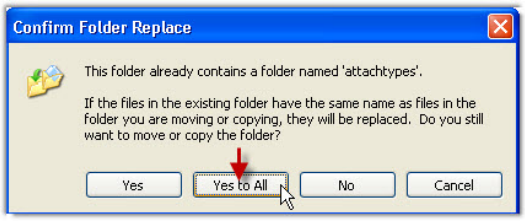
- Đầu tiên, bạn nhấn vào menu *Templates & Style* và nhấn chọn thẻ *Browses Theme* ở phía dưới.

- Trong danh sách các Themes hiện ra, bạn xem hình hiển thị mẫu và nhấn Download nếu thích giao diện đó. Ngoài những mẫu đó, bạn còn có thể tìm thấy các mẫu khác tại địa chỉ http://mods.mybb.com/themes. Tại đây, bạn nhấn vào tên mẫu (ví dụ Ajdija.com v3 Public Green) rồi nhấn vào liên kết Download, nhấn nút I agree để tải về tập tin nén dạng zip.

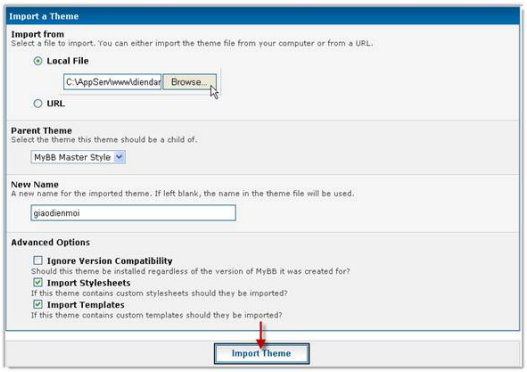
- Mỗi mẫu giao diện có cách cài đặt khác nhau tùy theo tác giả của mẫu đó. Thông thường, sau khi tải về bạn giải nén tập tin vào thư mục *diendan\images* của *Appserv*. Đối với mẫu này, bạn sẽ thấy hai thư mục *groups*, *images* và tập tin *Ajdija.com v3 Public Green-theme.xml* (cùng bốn tập tin dạng text khác dùng để cung cấp thông tin, hướng dẫn cài đặt mẫu).



- Bạn hãy mở tập tin installation.txt để xem qua hướng dẫn của tác giả. Theo hướng dẫn này, bạn cần sao chép các tập tin và thư mục con trong thư mục images sau khi giải nén vào thư mục image của diễn đàn. Nếu có tập tin trùng tên thì bạn nhấn Yesto all ở hộp thoại hiện ra để xác nhận việc ghi đè.

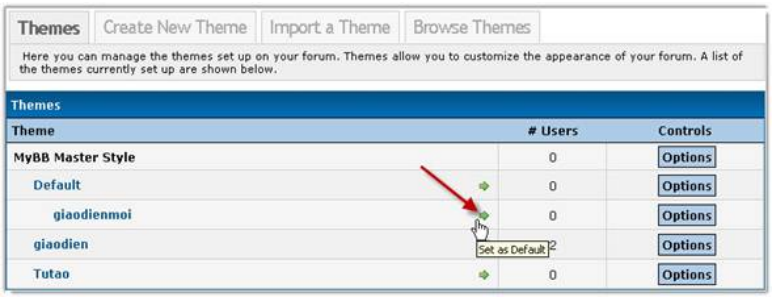


- Để cài đặt, bạn quay lại giao diện MyBB Admin Control Panel, nhấn chọn thẻ Import a Theme của mục Templates & Style. Trong khung Import a Theme, bạn nhấn nút Browse của mục Local File để duyệt đến tập tin Ajdija.com v3 Public Green-theme.xml, đặt tên cho giao diện mới ở mục New Name (có thể bỏ qua, MyBB sẽ sử dụng tên của mẫu giao diện đó), giữ nguyên các mục còn lại, nhấn nút Import Theme.



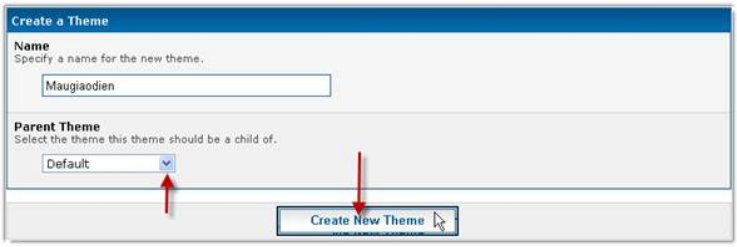
- Trang tiếp theo hiện ra yêu cầu bạn chỉnh sửa giao diện trước khi đưa vào sử dụng. Bạn có thể thay đổi các thuộc tính ở khung Edit Theme Properties, gồm Name (tên giao diện), Parent Theme (chọn nhóm giao diện phụ thuộc), Allowed User Groups (cho phép một nhóm thành viên nào đó sử dụng), Editor Style (giao diện cửa sổ soạn thảo bài viết), Board Logo (hình đại diện của diễn đàn, có thể đổi đường dẫn hoặc đổi tập tin), …, nhấn Save Themes Properties để thay đổi có hiệu lực.

- Nếu muốn sử dụng giao diện vừa cài đặt làm giao diện mặc định thì bạn nhấn vào biểu tượng mũi tên màu xanh phía sau tên giao diện đó. Lưu ý, khi đã chọn giao diện mặc định thì giao diện đó được sử dụng chung cho tất cả các nhóm thành viên, mặc dù trước đó có thiết lập chỉ cho phép hiển thị đối với một nhóm nào đó.



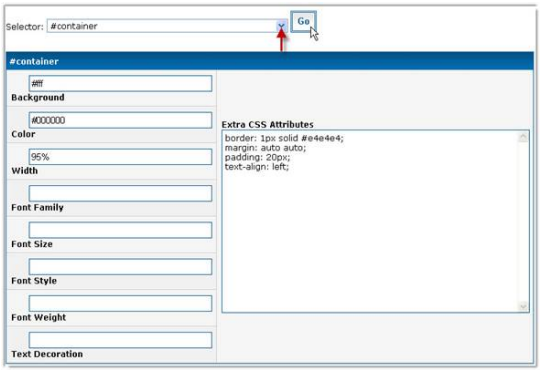
Tự tạo bộ cài đặt giao diện

- *MyBB* còn có một tính năng độc đáo là giúp người dùng tự thiết kế giao diện. Cạnh thẻ *Theme*, bạn nhấn chọn thẻ *Create New Theme* rồi nhập tên giao diện muốn tạo ở ô *Name*, chọn giao diện chứa nó ở trường *Parent Theme*, nhấn *Create New Theme*.



- Tại thẻ *Edit Stylesheets*, bạn cần chỉnh sửa những tập tin có định dạng *css* (*global.css*, *usercp.css*, *modcp.css*, *star_racings.css*, *showthread.css*). Minh họa với tập tin *global.css*, bạn nhấn nút *Options*> chọn *Edit Style*.

- Ở trang mới hiện ra, có hai hình thức chỉnh sửa *Simple Mode* (đơn giản)và *Advanced Mode* (nâng cao, chỉnh sửa trực tiếp trên các đoạn mã css). Đối với hình thức *Simple Mode*, bạn chọn mục ở trường *Selector* rồi thay đổi các giá trị ở trong khung bên dưới: *Background* (màu nền), *Color* (màu), *Width* (độ rộng), *Font Family* (nhóm font muốn dùng), *Font Size* (kích thước chữ), *Font Style* (kiểu chữ), …, xong nhấn *Save Changes* (hoặc *Save Changes & Close*).



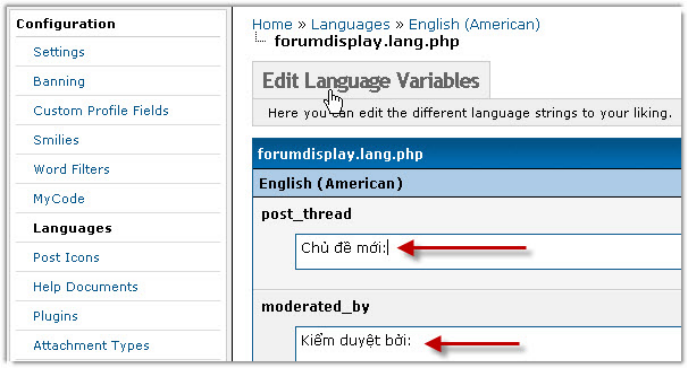
- Công việc cuối cùng là cần xuất bản tập tin ***xml***, bạn chuyển sang thẻ *Export Theme*, giữ nguyên các lựa chọn ở khung *Export Theme*> nhấn nút *Export Theme*> chọn nơi lưu trữ tập tin *Maugiaodien-theme.xml*.

Việt hóa giao diện

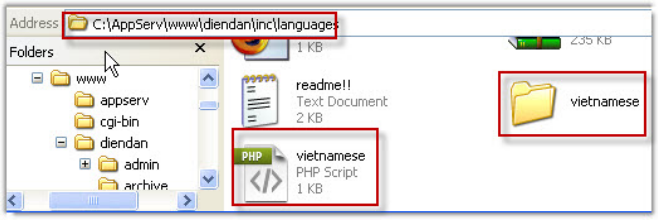
- Trong gói cài đặt của *MyBB* chỉ chứa duy nhất một ngôn ngữ là tiếng Anh (*English*). Bạn có thể tự mình chỉnh sửa giao diện tiếng Anh thành tiếng Việt. Để thực hiện, bạn vào menu *Configuration* rồi nhấn vào mục *Languages* ở khung bên phải. Trong khung *Installed Language Packs*, bạn nhấn nút *Options* > chọn *Edit with English (American)*.

- Trong trang mới hiện ra sẽ có hai loại giao diện để bạn chỉnh sửa ngôn ngữ, là giao diện bình thường của diễn đàn (*Front End*), giao diện bảng điều khiển của người quản trị (*Admin CP*). Đối với khung *Front End*, bạn nhấn vào liên kết *Edit* ở mỗi module, ví dụ module *forumdisplay.lang.php*.

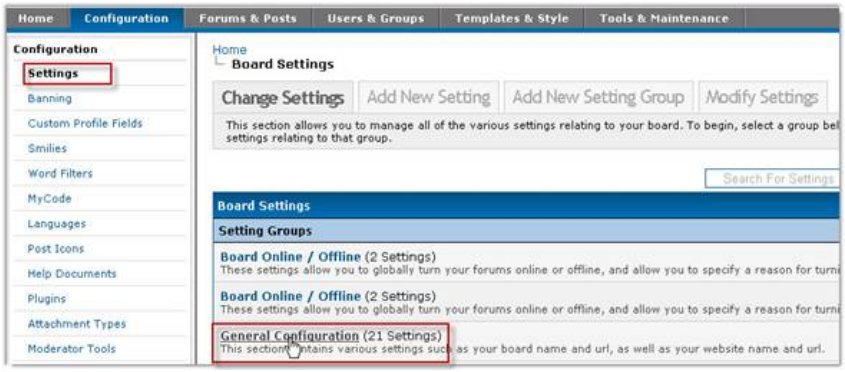
- Khi đó, bạn chỉ việc nhập vào các ô tương ứng những từ hoặc cụm từ tiếng Việt theo ý tưởng thiết kế diễn đàn của mình. Nếu chỉ đơn thuần là dịch thì có thể sử dụng công cụ *Google Translate* để dịch các cụm từ tiếng Anh sang tiếng Việt. Khi xong, bạn nhấn *Save Language File*. Cạnh thẻ *Language Files*, bạn nhấn chọn thẻ *Quick Phrases* để chỉnh sửa ngôn ngữ ở các trường đăng kí thành viên và một số trường thông báo khác.



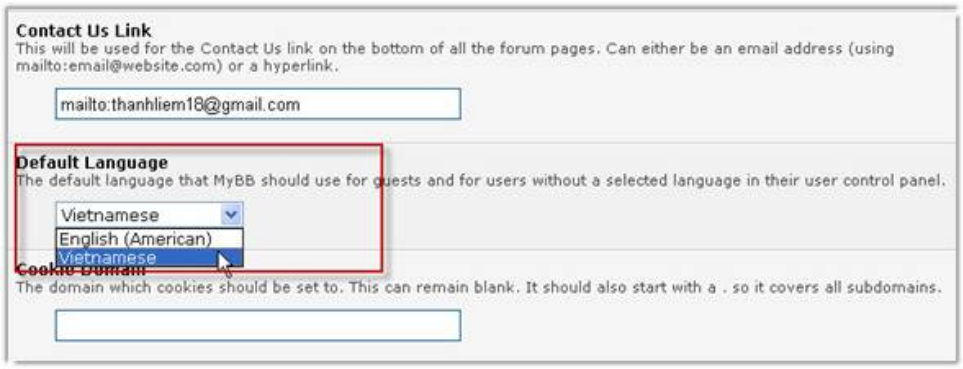
- Hiện tại trên Internet có rất nhiều gói ngôn ngữ tiếng Việt được người dùng tạo ra, bạn có thể tải gói ngôn ngữ có tỉ lệ Việt hóa trên 95% tại địa chỉ *http://tonghop24.com/home/*. Sau khi giải nén, bạn cần sao chép thư mục *vietnamese* và tập tin *vietnamese.php* trong thư mục *LangVietFull_2.1* vào thư mục *\inc\languages* của diễn đàn. Khi xong, bạn quay lại giao diện *Admin Control Panel* và kiểm tra trong khung *Installed Language Packs* sẽ xuất hiện mục *Vietnamese*.



- Để thiết lập tiếng Việt làm ngôn ngữ mặc định của diễn đàn, bạn nhấn *Settings* bên dưới chữ *Configuration* rồi tìm trong khung *Board Settings* mục *Genaral Configuration*.



- Trang tiếp theo hiện ra, bạn tìm đến mục *Default Language* trong khung bên phải, nhấn vào nút xổ xuống chọn *Vietnamese*, nhấn *Save Settings* ở cuối trang để hoàn tất. Ngoài ra, các tính năng khung này giúp chỉnh sửa những thông tin cơ bản về diễn đàn mà trong lúc cài đặt bạn khai báo sai hoặc thiếu sót.

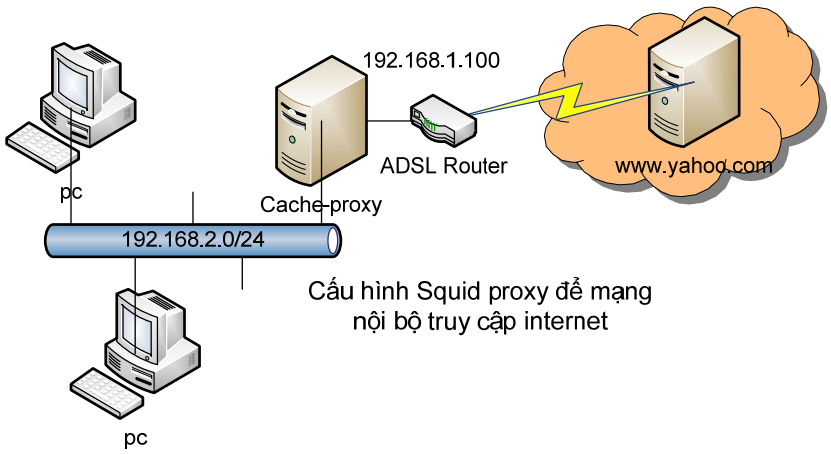


- Việc quản lý diễn đàn với các tính năng cơ bản như đã nêu sẽ giúp bạn có một diễn dàn chuyên nghiệp. Và sau loạt bài này, nếu có yêu cầu thêm thì tôi sẽ giới thiệu đến các bạn một số tính năng quản lý nâng cao, giúp diễn đàn hoạt động tốt hơn.

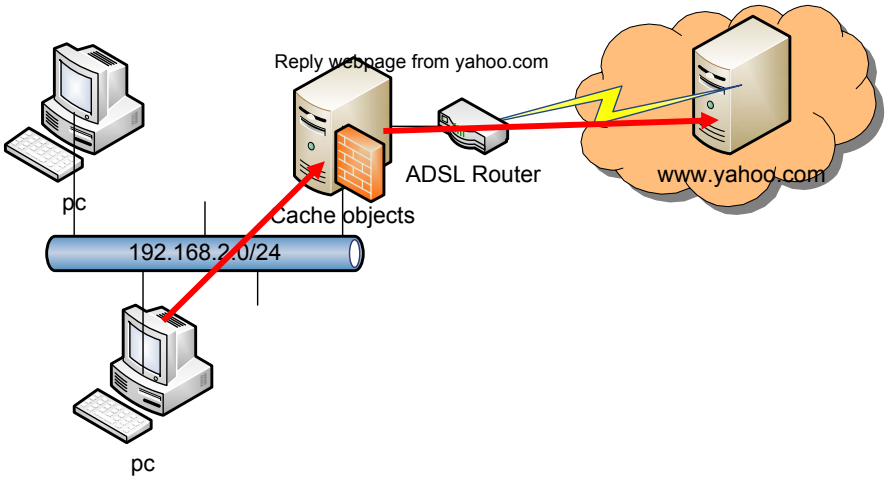
5.5. CẤU HÌNH INTERNET

5.5.1. CẤU HÌNH CHIA SẼ INTERNET

Mô hình và yêu cầu bài tập



Mô hình hoạt động



Hướng dẫn thực hiện

a) Kiểm tra cài đặt squid

```
[root@Webserver etc]# rpm -qa|grep squid
```

b) Cài đặt squid bằng yum hoặc rpm

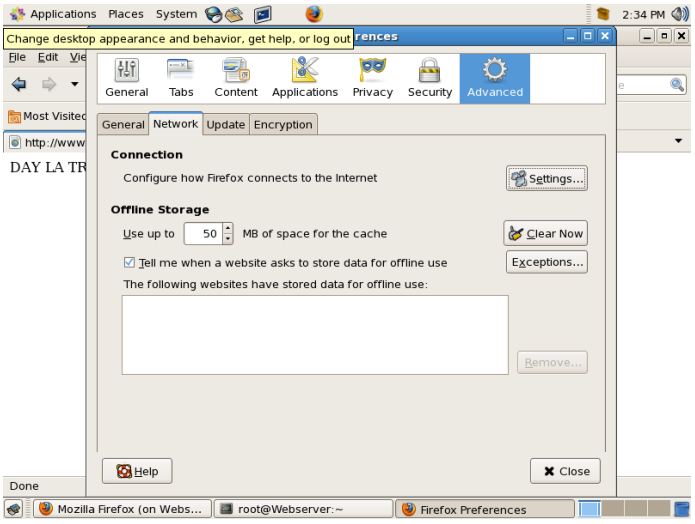
```
[root@linux ~]# yum -y install squid
Hoặc cài đặt file nhi phân bằng RPM
[root@linux ~]# rpm     -ivh  squid-3.1.10-1.el6_1.1.i686.rpm
```

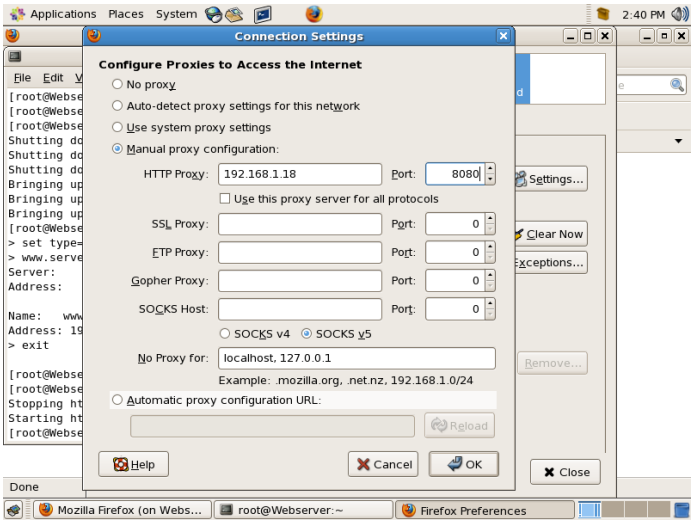
c) Cấu hình squid

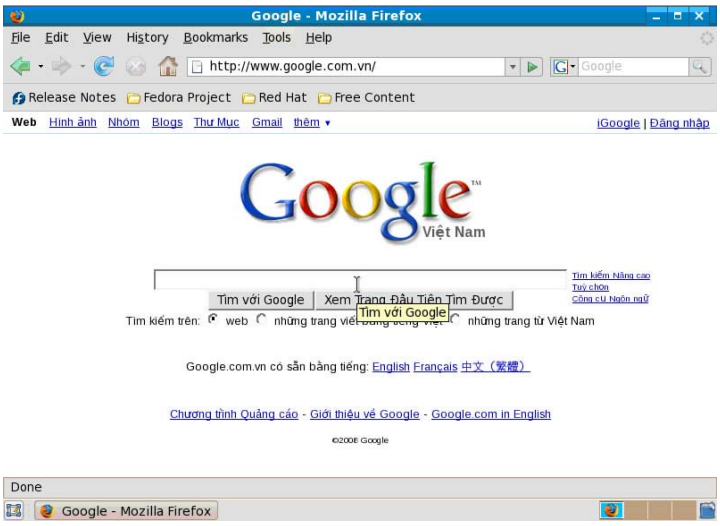
```
[root@prox ~]#vi /etc/squid/squid.conf
acl CONNECT method CONNECT
# Thêm dòng 31: add ( define new ACL )
acl lan src 10.0.0.0/24
http_access allow localhost

# Thêm dòng 59: add ( allow defined ACL above )
http_access allow lan

# Chỉnh sửa dòng 64: change
http_port   8080

# Thêm vào dưới cùng các dòng sau:
request_header_access Referer deny all
request_header_access X-Forwarded-For deny all
request_header_access Via deny all
request_header_access Cache-Control deny all

# Thêm vào (specify hostname)
visible_hostname prox.serverlinux

# Thêm vào (hide IP address)
forwarded_for off

[root@prox ~]#/etc/rc.d/init.d/squid start
Starting squid:                      [ OK ]
[root@prox ~]#chkconfig squid       on
```

d) Kiểm tra hoạt động của squid

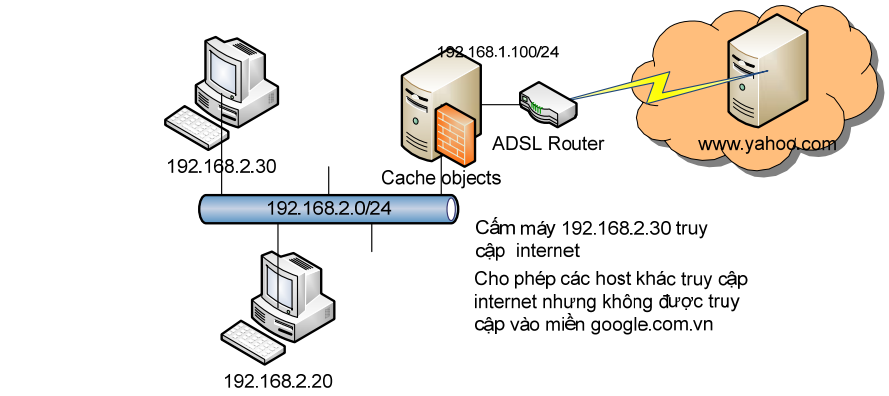
```
[root@Webserver etc]# squid -z
2011/10/24 12:04:09| Creating Swap Directories
[root@Webserver etc]# /etc/init.d/squid restart
Stopping squid:               [FAILED]
Starting squid: .             [  OK  ]
```

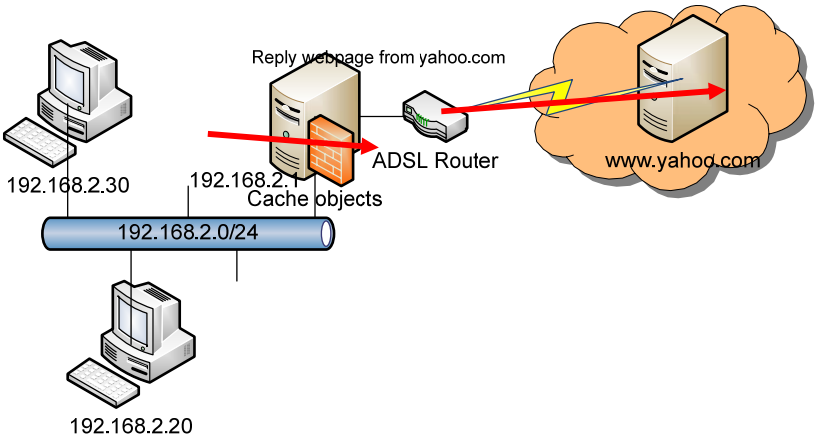

Applications Places System
2:34 PM
Change desktop appearance and behavior, get help, or log out
General Tabs Content Applications Privacy Security Advanced
General Network Update Encryption
Connection
Configure how Firefox connects to the Internet
Settings...
Offline Storage
Use up to 50 MB of space for the cache
Clear Now
Tell me when a website asks to store data for offline use
Exceptions...
The following websites have stored data for offline use:
Remove...
Help
Close
Done
Mozilla Firefox (on Webs...
root@Webserver:~
Firefox Preferences


Applications Places System
2:40 PM
Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 192.168.1.18
Port: 8080
Use this proxy server for all protocols
SSL Proxy:
FTP Proxy:
Gopher Proxy:
SOCKS Host:
SOCKS v4 SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
Help
Cancel
OK
Done
Mozilla Firefox (on Webs...
root@Webserver:~
Firefox Preferences


Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com.vn/
Release Notes
Fedora Project
Red Hat
Free Content
Web Hình ảnh Nhóm Blogs Thư Mục Gmail thêm
iGoogle | Đăng nhập
Google
Việt Nam
Tìm với Google
Xem Trang Đầu Tiên Tìm Được
Tìm kiếm Nâng cao
Tuỳ chỉnh
Công cụ Ngôn ngữ
Tìm kiếm trên: web những trang từ Việt Nam
Google.com.vn có sẵn bằng tiếng: English Français 中文（繁體）
Chương trình Quảng cáo - Giới thiệu về Google - Google.com in English
©2008 Google
Done
Google - Mozilla Firefox

5.5.2. GIỚI HẠN KẾT NỐI INTERNET





→

Hướng dẫn thực hiện

a. Cài đặt squid
b. Cấu hình squid
    1) Khai báo ACL src
    2) Khai báo ACL dstdomain
c. Apply ACL
d. Kiểm tra hoạt động

Các bước thực hiện

a) Cài đặt squid

```
[root@localhost ~]# yum -y install squid
Hoặc tải phần mềm squid dạng nhị phân và cài đặt bằng RPM
[root@localhost ~]# rpm –ivh squid-3.1.10-1.el6_1.1.i686.rpm
```

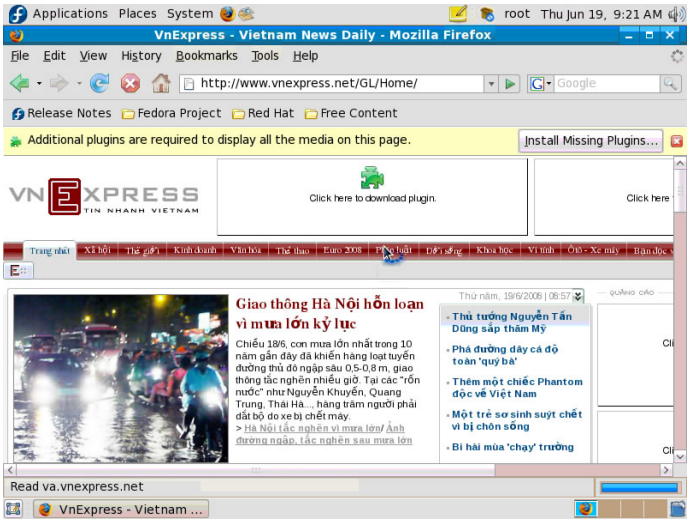
b) Cấu hình squid

```
[root@prox ~]#vi /etc/squid/squid.conf
acl CONNECT method CONNECT
# Thêm dòng 31: add ( define new ACL )
acl lan src 10.0.0.0/24
http_access allow localhost

# Thêm dòng 59: add ( allow defined ACL above )
http_access allow lan

# Chỉnh sửa dòng 64: change
http_port   8080

# Thêm vào dưới cùng các dòng sau:
request_header_access Referer deny all
request_header_access X-Forwarded-For deny all
request_header_access Via deny all
request_header_access Cache-Control deny all

# Thêm vào (specify hostname)
visible_hostname prox.serverlinux

# Thêm vào (hide IP address)
forwarded_for off
```

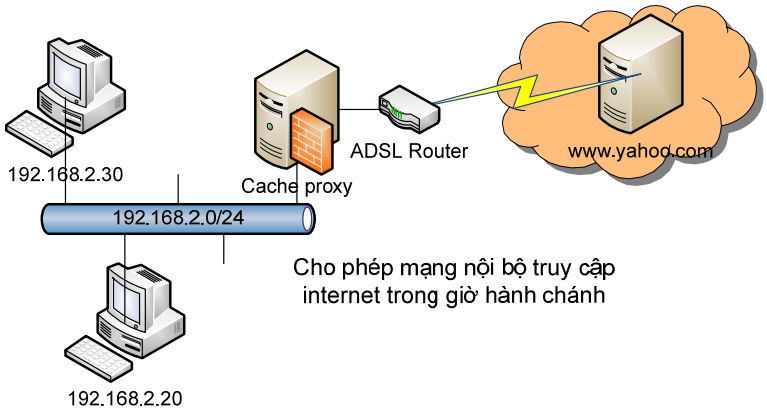
c) Khởi động squid

```
[root@prox ~]#/etc/rc.d/init.d/squid start
Starting squid:                      [ OK ]
[root@prox ~]#chkconfig squid       on
```

d) Truy cập web server



5.5.3. KIỂM SOÁT THỜI GIAN TRUY CẬP INTERNET



Hướng dẫn thực hiện

a. Cấu hình squid

1) Khai báo ACL time

2) Apply ACL time

b. Cấu hình squid cấm truy cập

```
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged)
machines
```

```
acl thoigian time MTWHF 7:30-17:30
http_access deny !thoigian
acl out_networks src 172.16.1.0/24
http_access deny out_networks
```

a) Khởi động squid

```
[root@prox ~]#/etc/rc.d/init.d/squid start
Starting squid:                        [ OK ]
[root@prox ~]#chkconfig squid          on
```

b) Cấu hình squid cho phép truy cập

```
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged)
machines
acl thoigian time MTWHF 7:30-17:30
http_access deny !thoigian
acl out_networks src 172.16.1.0/24
http_access allow out_networks
```

c) Khởi động squid

```
[root@prox ~]#/etc/rc.d/init.d/squid start
Starting squid:                        [ OK ]
[root@prox ~]#chkconfig squid          on
```

d) Truy cập web server

5.6. DỊCH VỤ MAIL

5.6.1. GIỚI THIỆU SMTP

SMTP là giao thức tin cậy chịu trách nhiệm phân phát mail. Nó chuyển mail từ hệ thống mạng này sang hệ thống mạng khác, chuyển mail trong hệ thống mạng nội bộ. Giao thức SMTP được định nghĩa trong RFC 821, SMTP là một dịch vụ tin cậy, hướng kết nối, sử dụng số hiệu cổng 25.

Để sử dụng các lệnh SMTP ta dùng lệnh telnet theo port 25 trên hệ thống ở xa sau đó gởi mail thông qua cơ chế dòng lệnh. Kỹ thuật này thỉnh thoảng cũng được sử dụng để kiểm tra hệ thống SMTP server, nhưng điều chính yếu ở đây là chúng ta sử dụng SMTP để minh hoạ làm cách nào mail được gởi qua các hệ thống khác nhau.

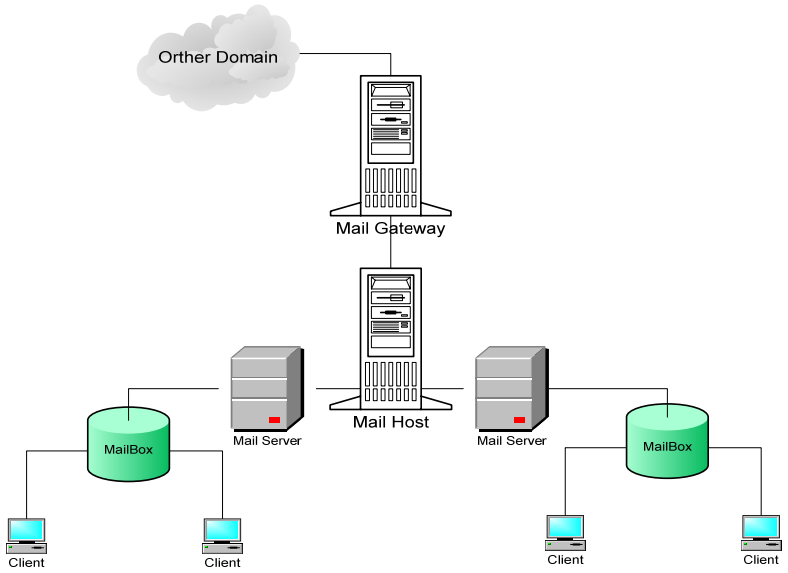
SMTP là hệ thống phân phát mail trực tiếp từ Mail server gởi đến Mail server nhận, điều này rất hiếm khi sử dụng. Hầu hết hệ thống mail sử dụng giao thức store and forward như UUCP và X.400. Hai giao thức này di chuyển mail đi qua mỗi pop, lưu trữ thông điệp tại mỗi hop và sau đó chuyển tới hệ thống tiếp theo, thông điệp đươc chuyển tiếp cho tới khi nó tới hệ thống phân phát cuối cùng.

5.6.2. POP

Có hai phiên bản của POP được sử dụng rộng rãi là POP2, POP3. POP2 được định nghĩa trong RFC 937, POP3 được định nghĩa trong RFC 1725. POP2 sử dụng cổng 109 và POP3 sử dụng cổng 110. Các câu lệnh trong hai giao thức này không giống nhau nhưng chúng cùng thực hiện chức năng cơ bản là kiểm tra tên đăng nhập, mật khẩu người dùng và chuyển mail của người dùng từ server tới hệ thống đọc mail cục bộ của user. Trong khi đó tập lệnh của POP3 hoàn toàn khác với tập lệnh của POP2.

5.6.3. HỆ THỐNG MAIL

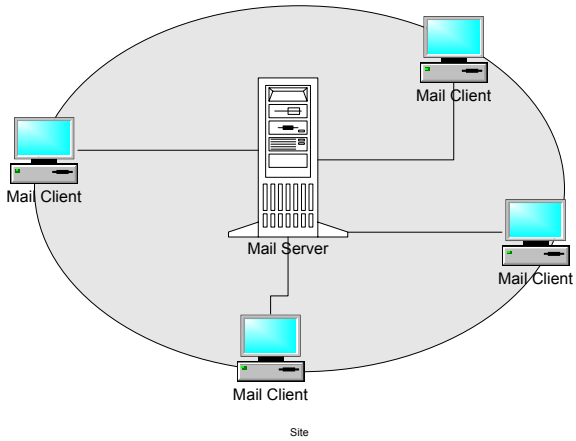
Một hệ thống mail yêu cầu phải có ít nhất hai thành phần, nó có thể định vị trên hai hệ thống khác nhau hoặc trên cùng một hệ thống, mail server và mail client. Ngoài ra, nó còn có những thành phần khác như Mail Host, Mail Gateway. Sơ đồ tổ chức hệ thống Mail:



Hình 4.2: Sơ đồ tổ chức Mail

Hệ thống mail cục bộ

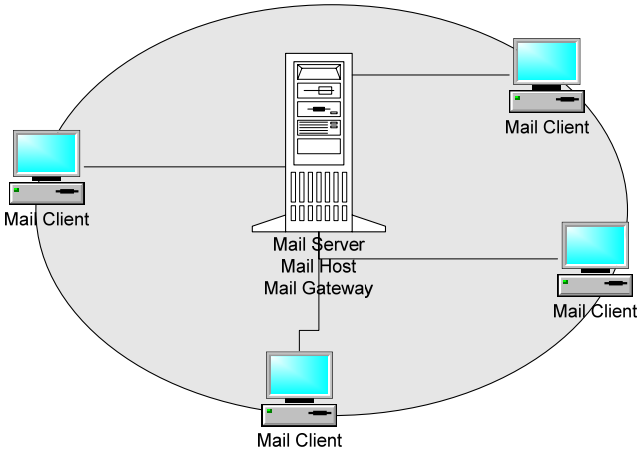
Cấu hình hệ thống mail đơn giản gồm một hoặc nhiều trạm làm việc kết nối vào một Mail Server. Tất cả mail đều chuyển cục bộ.



Hình 4.4: Sơ đồ Mail cục bộ

Hệ thống mail cục bộ có kết nối từ xa

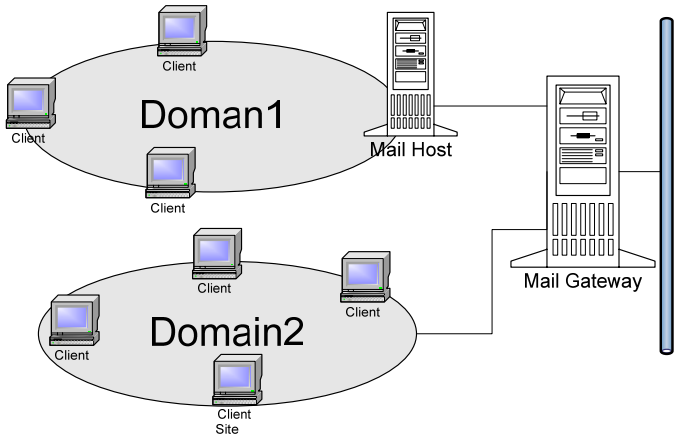
Hệ thống mail trong một mạng nhỏ gồm một mail server, một mail host và một mail gateway kết nối với hệ thống bên ngoài. Không cần DNS server.



Hình 4.5: hệ thống mail kết nối từ xa

Hệ thống hai domain và một gateway

Cấu hình dưới đây gồm hai domain và một mail gateway. Trong hệ thống này mail server, mail host, và mail gateway cung cấp trên domain hoạt động như một hệ thống độc lập.



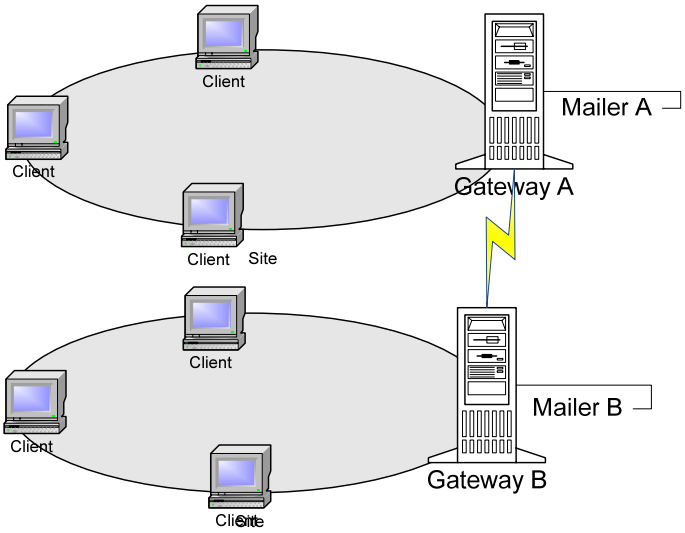
Hình 4.6: Hệ thống mail sử dụng mail gateway

Mô hình Mail Gateway

Một mail gateway là máy kết nối giữa các mạng dùng các giao thức truyền thông khác nhau hoặc kết nối các mạng khác nhau dùng chung giao thức. Ví dụ một mail gateway có thể kết nối một mạng TCP/IP với một mạng chạy bộ giao thức Systems Network Architecture (SNA).

Một mail gateway đơn giản nhất dùng để kết nối hai mạng dùng chung giao thức hoặc mailer. Khi đó mail gateway chuyển mail giữa domain nội bộ và các domain bên ngoài. Mail

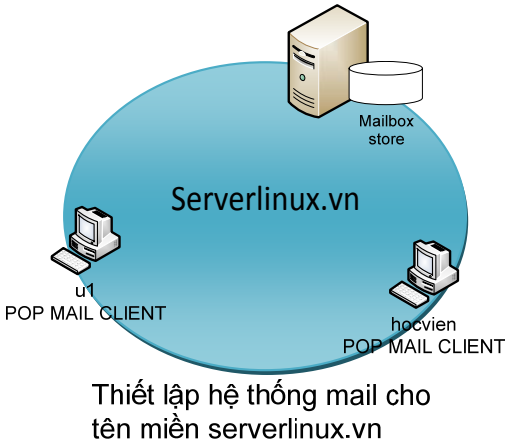
gateway cũng kết nối hai mạng dùng mailer khác nhau như hình vẽ dưới. Gateway giữa hai giao thức truyền khác nhau:



Hình 4.3: Sơ đồ mail gateway

5.6.4. THIẾT LẬP HỆ THỐNG MAIL CỤC BỘ

Mô hình và yêu cầu cấu hình



Hướng dẫn thực hiện

a. Kiểm tra DNS
b. Cấu hình tên host (/etc/host)
c. Cấu hình sendmail

1) Khai báo tên miền cục bộ
2) Chỉ định port listen
3) Khởi tạo dịch vụ

d. Cấu hình dovecot(pop3)
e. Cấu hình mail client Send/receive email

CÁC BƯỚC THỰC HIỆN

a) Kiểm tra cài đặt sendmail

```
[root@localhost named]# rpm -qa sendmail
sendmail-8.14.4-8.el6.i686

[root@localhost named]# host dns1.serverlinux.vn
dns1.serverlinux.vn has address 192.168.1.17

[root@localhost named]# host 192.168.1.17
17.1.168.192.in-addr.arpa domain name pointer dns1.serverlinux.vn.

[root@localhost named]# host mail.serverlinux.vn
mail.serverlinux.vn is an alias for dns1.serverlinux.vn.
dns1.serverlinux.vn has address 192.168.1.17
```

b) Cấu hình host name

```
[root@linux ~]# vi /etc/hosts
127.0.0.1       localhost.localdomain   serverlinux.vn
::1     localhost6.localdomain6 localhost6
192.168.1.17    Linux   serverlinx.vn
```

c) Cấu hình /etc/mail/sendmail.cf

```
81 # my LDAP cluster
82 # need to set this before any LDAP lookups are done (including classes)
83 #D{sendmailMTACluster}$m
84
85 Cwlocalhost serverlinux.vn
86 # file containing names of hosts for which we receive email
87 Fw/etc/mail/local-host-names
88
89 # my official domain name
```

```
90 # ... define this only if sendmail cannot automatically determine your
domain
91 #Dj$w.Foo.COM
……
259 # SMTP daemon options
260
261 #O DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA
262 O DaemonPortOptions=Name=MTA
263 # SMTP client options
264 #O ClientPortOptions=Family=inet, Address=0.0.0.0
```

d) Cấu hình cho phép truy cập /etc/mail/access

```
[root@localhost mail]# vi access
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# If you want to use AuthInfo with "M:PLAIN LOGIN", make sure to have the
# cyrus-sasl-plain package installed.
#
# By default we allow relaying from localhost...
Connect:localhost.localdomain           RELAY
Connect:localhost                       RELAY
Connect:127.0.0.1                       RELAY
Connect:serverlinux.vn                  RELAY
Connect:192.168.1.18                    RELAY
```

e) Khởi động sendmail

```
[root@localhost mail]# makemap hash access < access
[root@localhost mail]# /etc/init.d/sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [FAILED]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

f) Kiểm tra hoạt động của sendmail port 25

```
[root@localhost mail]# netstat -an|grep 25
tcp        0      0 127.0.0.1:25                0.0.0.0:*
LISTEN
```

```
udp        0      0 192.168.1.255:137           0.0.0.0:*
udp        0      0 172.16.29.255:137           0.0.0.0:*
udp   112592      0 172.16.29.255:137           0.0.0.0:*
udp        0      0 192.168.1.255:138           0.0.0.0:*
udp        0      0 172.16.29.255:138           0.0.0.0:*
udp    59104      0 172.16.29.255:138           0.0.0.0:*
unix  2    [ ACC ]   STREAM  LISTENING   13525  /var/lib/mysql/mysql.sock
unix  2    [ ACC ]   STREAM  LISTENING   17538  /tmp/.ICE-unix/2513
……..
unix  3    [ ]       STREAM  CONNECTED   15925
unix  3    [ ]       STREAM  CONNECTED   12530
unix  3    [ ]       STREAM  CONNECTED   12529
```

g) kiểm tra tài khoản trong /etc/passwd

```
[root@localhost named]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
……..
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
named:x:25:25:Named:/var/named:/sbin/nologin
hv1:x:503:503::/home/hv1:/bin/bash
squid:x:23:23::/var/spool/squid:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
```

Từ root gửi mail đến user hv1

```
[root@localhost mail]# mail -v hv1@serverlinux.vn
Subject: test
test
.
EOT
hv1@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 localhost.localdomain ESMTP Sendmail 8.14.4/8.14.4; Thu, 22 Dec 2011
13:59:10 -0500
>>> EHLO localhost.localdomain
250-localhost.localdomain Hello Linux [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
```

```
250-AUTH GSSAPI DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
>>> MAIL From:<root@localhost.localdomain> SIZE=214
AUTH=root@localhost.localdomain
553 5.5.4 <root@localhost.localdomain>... Real domain name required for
sender address
root... Using cached ESMTP connection to [127.0.0.1] via relay...
>>> RSET
250 2.0.0 Reset state
>>> MAIL From:<> SIZE=1238
250 2.1.0 <>... Sender ok
>>> RCPT To:<root@localhost.localdomain>
>>> DATA
250 2.1.5 <root@localhost.localdomain>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 pBMIxA8F003194 Message accepted for delivery
root... Sent (pBMIxA8F003194 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 localhost.localdomain closing connection
```

h) Đăng nhập vào user hv1 và kiểm tra mail

```
[root@dns1 mail]# su - hv1
[hv1@dns1 ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/hv1": 1 message 1 new
>N  1 root@dns1.serverlinu  Mon Nov  7 03:16  16/632   "test"
& 1   [ENTER]
root@dns1.serverlinu  Mon Nov  7 03:16  16/632   "test"
& 1
Message 1:
From root@dns1.serverlinux.vn  Mon Nov  7 03:16:21 2011
Date: Mon, 7 Nov 2011 03:16:21 +0700
From: root <root@dns1.serverlinux.vn>
To: hv1@serverlinux.vn
Subject: test

test hv1
&quit [ENTER]
```

i) Từ user hv1 gửi mail cho user hv2

```
[hv1@dns1 ~]$ mail -v hv2@serverlinux.vn
Subject: chao
chao^@^@hv2
.
Cc:
hv2@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 dns1.serverlinux.vn ESMTP Sendmail 8.13.8/8.13.8; Mon, 7 Nov 2011
03:21:52 +0700
>>> EHLO dns1.serverlinux.vn
250-dns1.serverlinux.vn Hello localhost.localdomain [127.0.0.1], pleased to
meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
>>> MAIL From:<hv1@dns1.serverlinux.vn> SIZE=43
AUTH=hv1@dns1.serverlinux.vn
250 2.1.0 <hv1@dns1.serverlinux.vn>... Sender ok
>>> RCPT To:<hv2@serverlinux.vn>
>>> DATA
250 2.1.5 <hv2@serverlinux.vn>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 pA6KLqI2007640 Message accepted for delivery
hv2@serverlinux.vn... Sent (pA6KLqI2007640 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
```

j) Đăng nhập vào user hv2 và kiểm tra mail

```
 [hv1@dns1 ~]$ su - hv2
Password:
[hv2@dns1 ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/hv2": 1 message 1 new
>N  1 hv1@dns1.serverlinux  Mon Nov  7 03:21  16/617   "chao"
& 1
Message 1:
```

```
From hv1@dns1.serverlinux.vn  Mon Nov  7 03:21:52 2011
Date: Mon, 7 Nov 2011 03:21:52 +0700
From: hv1@dns1.serverlinux.vn
To: hv2@serverlinux.vn
Subject: chao
chao
& quit
Saved 1 message in mbox
```

k) Từ user hv2 gửi mail cho root

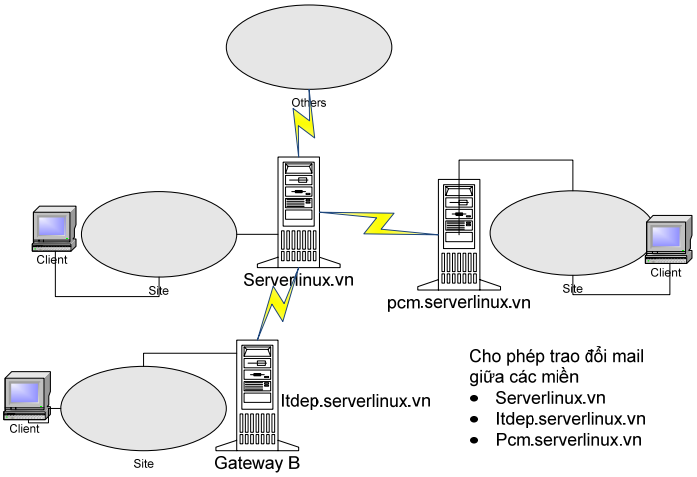
```
[hv2@dns1 ~]$ mail -v root@serverlinux.vn
Subject: chao root
chao root
.
Cc:
root@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 dns1.serverlinux.vn ESMTP Sendmail 8.13.8/8.13.8; Mon, 7 Nov 2011
03:26:32 +0700
>>> EHLO dns1.serverlinux.vn
250-dns1.serverlinux.vn Hello localhost.localdomain [127.0.0.1], pleased to
meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
>>> MAIL From:<hv2@dns1.serverlinux.vn> SIZE=54
AUTH=hv2@dns1.serverlinux.vn
250 2.1.0 <hv2@dns1.serverlinux.vn>... Sender ok
>>> RCPT To:<root@serverlinux.vn>
>>> DATA
250 2.1.5 <root@serverlinux.vn>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 pA6KQWNo007678 Message accepted for delivery
root@serverlinux.vn... Sent (pA6KQWNo007678 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 dns1.serverlinux.vn closing connection
```

```
[hv2@dns1 ~]$
```

l) Đăng nhập trở lại root và kiểm tra mail

```
[root@dns1 mail]# mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/root": 6 messages 6 new
>N  1 logwatch@localhost.l  Wed Oct 19 07:21  45/1748  "Logwatch for
localhost.localdoma"
 N  2 logwatch@localhost.l  Thu Oct 20 01:14 163/5543  "Logwatch for
localhost (Linux)"
 N  3 logwatch@localhost.l  Thu Oct 20 04:02 163/5543  "Logwatch for
localhost (Linux)"
 N  4 logwatch@DNSServer    Fri Oct 21 03:06 248/10059 "Logwatch for
dnsserver (Linux)"
 N  5 logwatch@DNSServer    Fri Oct 21 04:02 248/10059 "Logwatch for
dnsserver (Linux)"
 N  6 hv2@dns1.serverlinux  Mon Nov  7 03:26  16/630   "chao root"
& 6
Message 6: <Nhập vào mail cần xem>
From hv2@dns1.serverlinux.vn  Mon Nov  7 03:26:32 2011
Date: Mon, 7 Nov 2011 03:26:32 +0700
From: hv2@dns1.serverlinux.vn
To: root@serverlinux.vn
Subject: chao root

chao root

& quit
Saved 1 message in mbox
Held 5 messages in /var/spool/mail/root
```

5.6.5. THIẾT LẬP HỆ THỐNG MAIL TRAO ĐỔI CHO NHIỀU MIỀN



Hướng dẫn thực hiện

a. Kiểm tra dns nhiều miền con
b. Cấu hình relay mail cho 2 miền con từ miền serverlinux.vn
c. Cấu hình mail gateway cho itdep.serverlinux.vn
d. Cấu hình mail gateway cho pcm.serverlinux.vn
e. Khởi tạo dịch vụ
f. Kiểm tra hoạt động

Hướng dẫn thực hiện

a) Kiểm tra cấu hình DNS

```
[root@dns1 named]# nslookup
> set type=any
> serverlinux.vn
Server:         192.168.1.17
Address:        192.168.1.17#53

serverlinux.vn
        origin = dns1.serverlinux.vn
        mail addr = root.serverlinux.vn
        serial = 2011022700
        refresh = 28800
        retry = 14400
        expire = 3600000
```

```
        minimum = 86400
serverlinux.vn  nameserver = dns1.serverlinux.vn.
serverlinux.vn  mail exchanger = 1 dns1.serverlinux.vn.
> itdep.serverlinux.vn
Server:         192.168.1.17
Address:        192.168.1.17#53

Name:   itdep.serverlinux.vn
Address: 192.168.1.28
itdep.serverlinux.vn    mail exchanger = 1 mail.itdep.serverlinux.vn.
> 192.168.1.17
Server:         192.168.1.17
Address:        192.168.1.17#53

17.1.168.192.in-addr.arpa       name = dns1.serverlinux.vn.
> 192.168.1.28
Server:         192.168.1.17
Address:        192.168.1.17#53

28.1.168.192.in-addr.arpa       name = itdep.serverlinux.vn.
28.1.168.192.in-addr.arpa       name = mail.itdep.serverlinux.vn.
```

b) Cấu hình Access Relay Mail

```
[root@dns1 mail]# vi access
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
# by default we allow relaying from localhost...
Connect:localhost.localdomain           RELAY
Connect:localhost                       RELAY
Connect:127.0.0.1                       RELAY
Connect:serverlinux.vn                  RELAY
Connect:192.168.1.17                    RELAY
Connect:itdep.serverlinux.vn            RELAY
Connect:192.168.1.28                    RELAY
```

c) Biên dịch truy cập access

```
[root@dns1 mail]# makemap hash access < access
```

d) Khởi động lại dịch vụ sendmail

```
[root@dns1 mail]# /etc/init.d/sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

e) Chỉnh sửa tập tin sendmail.cf trong DNS itdep.serverlinux.vn

```
#Thay đổi dòng 89
89 Cwlocalhost itdep.serverlinux.vn
90 # file containing names of hosts for which we receive email
91 Fw/etc/mail/local-host-names
92
93 # my official domain name
94 # ... define this only if sendmail cannot automatically determine your
domain
95 #Dj$w.Foo.COM
96
97 # host/domain names ending with a token in class P are canonical
98 CP.
99
100 # "Smart" relay host (may be null)
#Thay đổi dòng 101
101 DSmail.serverlinux.vn
```

f) Khởi động lại dịch vụ sendmail trong itdep.serverlinux.vn

```
[root@dns1 mail]# /etc/init.d/sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

g) Tạo tài khoản hv trên itdep.serverlinux.vn và gửi mail giữa root và hv

```
[root@localhost mail]#useradd hv
[root@localhost mail]#passwd  hv
[root@localhost mail]# mail -v hv@itdep.serverlinux.vn
Subject: test1
test1
.
Cc:
```

```
WARNING: local host name (localhost) is not qualified; see cf/README: WHO
AM I?
hv@itdep.serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 localhost ESMTP Sendmail 8.13.8/8.13.8; Fri, 23 Dec 2011 07:35:58 +0700
>>> EHLO localhost
250-localhost Hello localhost.localdomain [127.0.0.1], pleased to meet you
…….
>>> .
250 2.0.0 pBN0Zw1U005360 Message accepted for delivery
hv@itdep.serverlinux.vn... Sent (pBN0Zw1U005360 Message accepted for
delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 localhost closing connection
```

h) Đăng nhập vào user hv và kiểm tra mail

```
[root@localhost mail]#su - hv
[root@localhost mail]# su - hv
[hv@localhost ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/hv": 1 message 1 new
>N  1 root@localhost        Fri Dec 23 07:35  16/578   "test1"
& 1
Message 1:
From root@localhost  Fri Dec 23 07:35:58 2011
Date: Fri, 23 Dec 2011 07:35:58 +0700
From: root <root@localhost>
To: hv@itdep.serverlinux.vn
Subject: test1
test1
& quit
Saved 1 message in mbox
[hv@localhost ~]$
```

i) Từ user sv@itdep.serverlinux.vngửi mail cho sv@serverlinux.vn

sv@itdep.serverlinux.vn gửi mail

```
[root@localhost mail]# su - sv
 [sv@dns2 ~]$ mail -v sv@serverlinux.vn
Subject: chao sv serverlinux.vn
xin chao sv serverlinux.vn
.
```

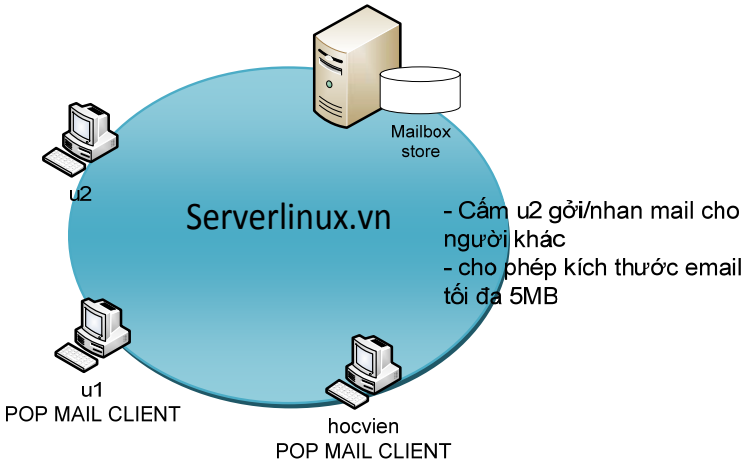
```
EOT
sv@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 dns2.itdep.serverlinux.vn ESMTP Sendmail 8.14.4/8.14.4; Fri, 23 Dec
2011 09:24:46 -0500
>>> EHLO dns2.itdep.serverlinux.vn
……..
>>> QUIT
221 2.0.0 dns2.itdep.serverlinux.vn closing connection
[sv@dns2 ~]$
```

sv@serverlinux.vn nhận mail từ sv@itdep.serverlinux.vn

```
[root@localhost mail]# su - sv
[sv@localhost ~]$ mail
Heirloom Mail version 12.4 7/29/08.  Type ? for help.
"/var/spool/mail/sv": 3 messages 2 new
    1 root                  Fri Dec 23 09:07  21/793   "test"
>N  2 Mail Delivery Subsys  Fri Dec 23 09:18  66/2411  "Returned mail: see
t"
 N  3 day la tai khoan dun  Fri Dec 23 09:24  23/1073  "chao sv
serverlinux."
& 3
Message  3:
From sv@dns2.itdep.serverlinux.vn  Fri Dec 23 09:24:53 2011
Return-Path: <sv@dns2.itdep.serverlinux.vn>
From: day la tai khoan dung de test <sv@dns2.itdep.serverlinux.vn>
Date: Fri, 23 Dec 2011 09:24:45 -0500
To: sv@serverlinux.vn
Subject: chao sv serverlinux.vn
User-Agent: Heirloom mailx 12.4 7/29/08
Content-Type: text/plain; charset=us-ascii
Status: R

xin chao sv serverlinux.vn

& quit
Held 3 messages in /var/spool/mail/sv
```

5.6.6. THIẾT LẬP KIỂM SOÁT MAIL CỦA NGƯỜI DÙNG

MÔ HÌNH VÀ YÊU CẦU CẤU HÌNH



HƯỚNG DẪN CẤU HÌNH

- Cấm email
- Chỉ định kích thước

CÁC BƯỚC THỰC HIỆN

a) Kiểm tra cài đặt sendmail

```
[root@localhost named]# rpm -qa sendmail
sendmail-8.14.4-8.el6.i686

[root@localhost named]# host dns1.serverlinux.vn
dns1.serverlinux.vn has address 192.168.1.17

[root@localhost named]# host 192.168.1.17
17.1.168.192.in-addr.arpa domain name pointer dns1.serverlinux.vn.

[root@localhost named]# host mail.serverlinux.vn
mail.serverlinux.vn is an alias for dns1.serverlinux.vn.
dns1.serverlinux.vn has address 192.168.1.17
```

b) Cấu hình host name

```
[root@linux ~]# vi /etc/hosts
```

```
127.0.0.1       localhost.localdomain   serverlinux.vn
::1     localhost6.localdomain6 localhost6
192.168.1.17    Linux   serverlinx.vn
```

c) Cấu hình /etc/mail/sendmail.cf

```
81 # my LDAP cluster
82 # need to set this before any LDAP lookups are done (including classes)
83 #D{sendmailMTACluster}$m
84
85 Cwlocalhost serverlinux.vn
86 # file containing names of hosts for which we receive email
87 Fw/etc/mail/local-host-names
88
89 # my official domain name
90 # ... define this only if sendmail cannot automatically determine your
domain
91 #Dj$w.Foo.COM
……
259 # SMTP daemon options
260
261 #O DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA
262 O DaemonPortOptions=Name=MTA
263 # SMTP client options
264 #O ClientPortOptions=Family=inet, Address=0.0.0.0
```

d) Cấu hình cấm truy cập /etc/mail/access

```
[root@localhost mail]# vi access
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# If you want to use AuthInfo with "M:PLAIN LOGIN", make sure to have the
# cyrus-sasl-plain package installed.
#
# By default we allow relaying from localhost...
Connect:localhost.localdomain           RELAY
Connect:localhost                       RELAY
Connect:127.0.0.1                       RELAY
Connect:serverlinux.vn                  RELAY
Connect:192.168.1.18                    RELAY
u2@serverlinux.vn                         REJECT
```

e) Khởi động sendmail

```
[root@localhost mail]# makemap hash access < access
[root@localhost mail]# /etc/init.d/sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

f) Kiểm tra hoạt động của sendmail port 25

```
[root@localhost mail]# netstat -an|grep 25
tcp        0      0 127.0.0.1:25                0.0.0.0:*
LISTEN
udp        0      0 192.168.1.255:137           0.0.0.0:*
udp        0      0 172.16.29.255:137           0.0.0.0:*
udp   112592      0 172.16.29.255:137           0.0.0.0:*
udp        0      0 192.168.1.255:138           0.0.0.0:*
udp        0      0 172.16.29.255:138           0.0.0.0:*
udp    59104      0 172.16.29.255:138           0.0.0.0:*
unix  2    [ ACC ]   STREAM  LISTENING   13525  /var/lib/mysql/mysql.sock
unix  2    [ ACC ]   STREAM  LISTENING   17538  /tmp/.ICE-unix/2513
……….
unix  3    [ ]       STREAM  CONNECTED   15925
unix  3    [ ]       STREAM  CONNECTED   12530
unix  3    [ ]       STREAM  CONNECTED   12529
```

g) kiểm tra tài khoản trong /etc/passwd

```
[root@localhost named]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
……….
named:x:25:25:Named:/var/named:/sbin/nologin
hv1:x:503:503::/home/hv1:/bin/bash
squid:x:23:23::/var/spool/squid:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
```

Từ root gửi mail đến user hv1

```
[root@localhost mail]# mail -v hv1@serverlinux.vn
Subject: test
test
.
```

```
EOT
hv1@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 localhost.localdomain ESMTP Sendmail 8.14.4/8.14.4; Thu, 22 Dec 2011
13:59:10 -0500
……..
root... Sent (pBMIxA8F003194 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 localhost.localdomain closing connection
```

h) Đăng nhập vào user hv1 và kiểm tra mail

```
[root@dns1 mail]# su - hv1
[hv1@dns1 ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/hv1": 1 message 1 new
>N  1 root@dns1.serverlinu  Mon Nov  7 03:16  16/632   "test"
& 1   [ENTER]
root@dns1.serverlinu  Mon Nov  7 03:16  16/632   "test"
& 1
Message 1:
From root@dns1.serverlinux.vn  Mon Nov  7 03:16:21 2011
Date: Mon, 7 Nov 2011 03:16:21 +0700
From: root <root@dns1.serverlinux.vn>
To: hv1@serverlinux.vn
Subject: test

test hv1
&quit [ENTER]
```

i) Từ user hv1 gửi mail cho user hv2

```
[hv1@dns1 ~]$ mail -v hv2@serverlinux.vn
Subject: chao
chao^@^@hv2
.
Cc:
hv2@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 dns1.serverlinux.vn ESMTP Sendmail 8.13.8/8.13.8; Mon, 7 Nov 2011
03:21:52 +0700
…….
250 2.1.5 <hv2@serverlinux.vn>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
```

```
250 2.0.0 pA6KLqI2007640 Message accepted for delivery
hv2@serverlinux.vn... Sent (pA6KLqI2007640 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
```

j) Đăng nhập vào user hv2 và kiểm tra mail

```
 [hv1@dns1 ~]$ su - hv2
Password:
[hv2@dns1 ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/hv2": 1 message 1 new
>N  1 hv1@dns1.serverlinux  Mon Nov  7 03:21  16/617   "chao"
& 1
Message 1:
From hv1@dns1.serverlinux.vn  Mon Nov  7 03:21:52 2011
Date: Mon, 7 Nov 2011 03:21:52 +0700
From: hv1@dns1.serverlinux.vn
To: hv2@serverlinux.vn
Subject: chao
chao
& quit
Saved 1 message in mbox
```

k) Từ user hv2 gửi mail cho root

```
[hv2@dns1 ~]$ mail -v root@serverlinux.vn
Subject: chao root
chao root
.
Cc:
root@serverlinux.vn... Connecting to [127.0.0.1] via relay...
220 dns1.serverlinux.vn ESMTP Sendmail 8.13.8/8.13.8; Mon, 7 Nov 2011
03:26:32 +0700
…….
root@serverlinux.vn... Sent (pA6KQWNo007678 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 dns1.serverlinux.vn closing connection
[hv2@dns1 ~]$
```

l) Đăng nhập trở lại root và kiểm tra mail

```
[root@dns1 mail]# mail
```

```
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/root": 6 messages 6 new
>N  1 logwatch@localhost.l  Wed Oct 19 07:21  45/1748  "Logwatch for
localhost.localdoma"
……
N  6 hv2@dns1.serverlinux  Mon Nov  7 03:26  16/630   "chao root"
& 6
Message 6: <Nhập vào mail cần xem>
From hv2@dns1.serverlinux.vn  Mon Nov  7 03:26:32 2011
Date: Mon, 7 Nov 2011 03:26:32 +0700
From: hv2@dns1.serverlinux.vn
To: root@serverlinux.vn
Subject: chao root

chao root

& quit
Saved 1 message in mbox
Held 5 messages in /var/spool/mail/root
```

m)Giới hạn dụng lượng gửi mail

```
#Thay đổi dòng 183
180
181 # maximum message size
182 #O MaxMessageSize=0
183 O MaxMessageSize=5000000
184
185 # substitution for space (blank) characters
186 O BlankSub=.
187
188 # avoid connecting to "expensive" mailers on initial submission?
189 O HoldExpensive=False
```

5.7. DỊCH VỤ NIS

5.7.1. CẤU HÌNH NIS SERVER

Cài đặt NIS

Kiểm tra gói ypserv*.rpm đã cài đặt rồi hay chưa. Nếu chưa thì tiến hành cài đặt bằng tiện ích YUM hoặc tải file nhị phân ypserv-2.19-3.i386.rpm

```
[root@localhost ~]# yum -y install ypserv rpcbind
Resolving Dependencies
--> Running transaction check
---> Package ypserv.i686 0:2.19-18.el6 set to be updated
--> Finished Dependency Resolution
Dependencies Resolved
================================================================
 Package       Arch      Version        Repository      Size
================================================================
Installing:
 ypserv           i686      2.19-18.el6       base    127 k
Transaction Summary
================================================================
Install       1 Package(s)
Upgrade       0 Package(s)
Total download size: 127 k
Installed size: 291 k
Downloading Packages:
ypserv-2.19-18.el6.i686.rpm         | 127 kB     00:06
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : ypserv-2.19-18.el6.i686     1/1
Installed:
  ypserv.i686 0:2.19-18.el6
Complete!
```

Khởi tạo NIS server

- Xem NIS domain hiện tại của server, cấu hình NIS domain cho server

- Hoặc thêm dòng sau vào file /etc/sysconfig/network:

- Chỉnh sửa file /var/yp/Makefile để bắt đầu khởi tạo những thông tin mà NIS sẽ phục vụ cho domain:

- Khởi tạo NIS server:

Cầu hình dịch vụ NIS để chia sẽ tài khoản người dùng trong hệ thống mạng cục bộ. Các bước cấu hình như sau:

```
[root@linux ~]#ypdomainname serverlinux.vn      # set NIS domain name

[root@linux ~]#vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=dlp.serverlinux.vn
# thêm dòng sau
NISDOMAIN=serverlinux.vn

[root@linux ~]#vi /var/yp/Makefile
# MERGE_PASSWD=true|false
# line 42: change
MERGE_PASSWD=false
# MERGE_GROUP=true|false
# line 46: change
MERGE_GROUP=false
# line 117: add
all: passwd shadow group hosts rpc services netid protocols

[root@linux ~]#vi /var/yp/securenets
255.255.255.0   10.0.0.0

[root@linux ~]#vi /etc/hosts
# thêm own IP address
10.0.0.30   dlp dlp.serverlinux

[root@linux ~]#/etc/rc.d/init.d/rpcbind start
Starting portmap:                   [ OK ]

[root@linux ~]#/etc/rc.d/init.d/ypserv    start
Starting YP server services:        [ OK ]

[root@linux ~]#/etc/rc.d/init.d/yppasswdd start
Starting YP passwd service:         [ OK ]

[root@linux ~]#chkconfig rpcbind    on

[root@linux ~]#chkconfig ypserv on

[root@linux ~]#chkconfig yppasswdd on
[root@linux ~]#/usr/lib64/yp/ypinit -m
# update NIS database
```

Tại thời điểm này, chúng ta phảixây dựng mộtdanh sách cácmáysẽchạycácmáy chủNIS. DLPlàtrong danh sáchcác máy chủmáychủNIS. Xinvuilòngtiếp tục để thêmtêncho các máy chủkhác trên mỗi dòng. Khiđang thực hiện vớidanh sách, gõ<control D>.

```
next host to add: dlp
next host to add:       # push Ctrl + D key
The current list of NIS servers looks like this:
dlp
Is this correct? [y/n: y] y
# answer yes
We need a few minutes to build the databases...
Building /var/yp/serverlinux/ypservers...
Running /var/yp/Makefile...
gmake[1]: Entering directory `/var/yp/serverlinux'
Updating passwd.byname...
Updating passwd.byuid...
Updating shadow.byname...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gmake[1]: Leaving directory `/var/yp/serverlinux'
dlp has been set up as a NIS master server.
Now you can run ypinit -s dlp on all slave server.
# It's neccessary to update NIS database with following way if new user is
added again
[root@linux ~]#cd /var/yp
[root@dlp yp]#make
```

5.7.2. **CẤU HÌNH NIS CLIENT**

- Chỉnh sửa file /etc/yp.conf

```
domain      serverlinux.vn          broadcast
```

- Start tiến trình ypbin:

- Sử dụng lệnh ypwhich để kiểm tra NIS server nào đang phục vụ những request NIS:

- Lệnh ypcat để liệt kê thông tin một bảng map trên NIS server:

- Cấu hình file /etc/nsswitch.conf để hệ thống cần tìm kiếm thông tin:

- Dùng một máy khác login bằng user chỉ có trên NIS server (không tồn tại ở máy cục bộ) để kiểm tra hoạt động sử dụng NIS chứng thực:

- Khi thay đổi thông tin trên bảng map của NIS server, như thêm user test vào file /etc/passwd

- Update lại thông tin trên NIS server như sau:

- Tại NIS client, xem lại bản map:

- Xóa thông tin của user test trên local:#userdel test

- Thử switch qua user test, kết quả vẫn switch được bình thường, vì lúc này thông tin đã được tìm kiếm trên NIS

```
[root@linux ~]#yum -y install ypbind rpcbind
[root@linux ~]#vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=www.serverlinux.vn
# add at the last line
NISDOMAIN=serverlinux.vn
[root@linux ~]#vi /etc/sysconfig/authconfig
USENIS=yes              # line 19: change
[root@linux ~]#vi /etc/yp.conf
# add at the last line ( [domain] server [NIS server] )
domain serverlinux server dlp.serverlinux
[root@linux ~]#vi /etc/nsswitch.conf
passwd:     files       nis   # line 33: add
shadow:     files       nis   # add
group:            files       nis   # add
hosts:            files dns nis     # add
```

```
# add optionally if you need ( create home directory automatically if it's
none )
[root@linux ~]#vi /etc/pam.d/system-auth
# add at the last line
session     optional      pam_mkhomedir.so skel=/etc/skel umask=077
[root@linux ~]#chkconfig rpcbind on
[root@linux ~]#chkconfig ypbind on
[root@linux ~]#shutdown -r now
www.serverlinux login:debian  # user on NIS
Password:         # password
Creating directory '/home/debian'.
[debian@www ~]$# logined
[debian@www ~]$ypwhich
dlp
[debian@www ~]$ypcat passwd
cent:x:500:500::/home/fermi:/bin/bash
ubuntu:x:502:502::/home/ubuntu:/bin/bash
fedora:x:501:501::/home/cent:/bin/bash
debian:x:503:503::/home/debian:/bin/bash
[debian@www ~]$ypcat hosts
10.0.0.30 dlp dlp.serverlinux
10.0.0.30 dlp dlp.serverlinux
127.0.0.1 localhost localhost.localdomain localhost4
localhost4.localdomain4
127.0.0.1 localhost localhost.localdomain localhost4
localhost4.localdomain4
127.0.0.1 localhost localhost.localdomain localhost4
localhost4.localdomain4
127.0.0.1 localhost localhost.localdomain localhost4
localhost4.localdomain4
[debian@www ~]$yppasswd       # try to chnage NIS password
Changing NIS account information for debian on dlp.
Please enter old password:          # current one
Changing NIS password for debian on dlp.
Please enter new password:          # new one
Please retype new password:
The NIS password has been changed on dlp.
[debian@www ~]$               #just changed
```

5.8. DỊCH VỤ LDAP

5.8.1. CẤU HÌNH LDAP SERVER

Cài đặt OpenLDAP

- Kiểm tra gói openldap đã được cài đặt hay chưa. Nếu chưa cài đặt thì có thể sử dụng trình tiện ích YUM hoặc trình cài đặt RPM để cài đặt phần mềm.

```
[root@dir ~]#yum -y install openldap-servers openldap-clients
[root@dir ~]#vi /etc/sysconfig/ldap
# line 16: uncomment and change
SLAPD_LDAPI=yes
[root@dir ~]#vi /etc/openldap/slapd.conf
# create new
pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args
[root@dir ~]#rm -rf /etc/openldap/slapd.d/*
[root@dir ~]#slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
[root@dir ~]#vi /etc/openldap/slapd.d/cn=config/olcDatabase\={0}config.ldif
# line 4: change
olcAccess: {0}to * by
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by
* break
[root@dir ~]#vi
/etc/openldap/slapd.d/cn=config/olcDatabase\={1}monitor.ldif
# create new
dn: olcDatabase={1}monitor
objectClass: olcDatabaseConfig
olcDatabase: {1}monitor
olcAccess: {1}to * by
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by
* break
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcMonitoring: FALSE
structuralObjectClass: olcDatabaseConfig
creatorsName: cn=config
modifiersName: cn=config
[root@dir ~]#chown -R ldap. /etc/openldap/slapd.d
```

```
[root@dir ~]#chmod -R 700 /etc/openldap/slapd.d
[root@dir ~]#/etc/rc.d/init.d/slapd start
Starting slapd:          [ OK ]
[root@dir ~]#chkconfig slapd on
```

Cấu hình openldap

```
[root@dir ~]#ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/core.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=core,cn=schema,cn=config"
[root@dir ~]#ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/cosine.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"
[root@dir ~]#ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/nis.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"
[root@dir ~]#ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/inetorgperson.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"
[root@dir ~]#slappasswd       # generate password
New password:           # input any one
Re-enter new password:
{SSHA}xxxxxxxxxxxxxxxxxxxxxxx
[root@dir ~]#vi backend.ldif
# create new
# replace the section "dc=***,dc=***" to your own suffix
# replace the section "olcRootPW: ***" to your own password generated by
slappasswd above
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
```

```
olcModulepath: /usr/lib64/openldap
olcModuleload: back_hdb
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcSuffix: dc=server,dc=world
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=server,dc=world
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcMonitoring: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=server,dc=world" write
by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=server,dc=world" write by * read
[root@dir ~]#ldapadd -Y EXTERNAL -H ldapi:/// -f backend.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=module,cn=config"
adding new entry "olcDatabase=hdb,cn=config"
[root@dir ~]#vi frontend.ldif
# create new
# replace the section "dc=***,dc=***" to your own suffix
# replace the section "userPassword: ***" to your own password generated by
slappasswd above
dn: dc=server,dc=world
objectClass: top
objectClass: dcObject
objectclass: organization
o: Server World
dc: Server
dn: cn=admin,dc=server,dc=world
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
```

```
userPassword: {SSHA}xxxxxxxxxxxxxxxxxxxxxxx
dn: ou=people,dc=server,dc=world
objectClass: organizationalUnit
ou: people
dn: ou=groups,dc=server,dc=world
objectClass: organizationalUnit
ou: groups
[root@dir ~]#ldapadd -x -D cn=admin,dc=server,dc=world -W -f frontend.ldif
Enter LDAP Password:          # password you set
adding new entry "dc=server,dc=world"
adding new entry "cn=admin,dc=server,dc=world"
adding new entry "ou=people,dc=server,dc=world"
adding new entry "ou=groups,dc=server,dc=world"
```

Thêm danh sách người dùng hệ thống cục bộ vào danh mục LDAP

```
[root@dir ~]#vi ldapuser.sh
# extract local users who have 500-999 digit UID
# replace "SUFFIX=***" to your own suffix
# this is an example
#!/bin/bash
SUFFIX='dc=server,dc=world'
LDIF='ldapuser.ldif'
echo -n > $LDIF
for line in `grep "x:[5-9][0-9][0-9]:" /etc/passwd | sed -e "s/ /%/g"`
do
   UID1=`echo $line | cut -d: -f1`
   NAME=`echo $line | cut -d: -f5 | cut -d, -f1`
   if [ ! "$NAME" ]
   then
      NAME=$UID1
   else
      NAME=`echo $NAME | sed -e "s/%/ /g"`
   fi
   SN=`echo $NAME | awk '{print $2}'`
   if [ ! "$SN" ]
   then
      SN=$NAME
   fi
   GIVEN=`echo $NAME | awk '{print $1}'`
   UID2=`echo $line | cut -d: -f3`
   GID=`echo $line | cut -d: -f4`
   PASS=`grep $UID1: /etc/shadow | cut -d: -f2`
```

```
   SHELL=`echo $line | cut -d: -f7`
   HOME=`echo $line | cut -d: -f6`
   EXPIRE=`passwd -S $UID1 | awk '{print $7}'`
   FLAG=`grep $UID1: /etc/shadow | cut -d: -f9`
   if [ ! "$FLAG" ]
   then
      FLAG="0"
   fi
   WARN=`passwd -S $UID1 | awk '{print $6}'`
   MIN=`passwd -S $UID1 | awk '{print $4}'`
   MAX=`passwd -S $UID1 | awk '{print $5}'`
   LAST=`grep $UID1: /etc/shadow | cut -d: -f3`
   echo "dn: uid=$UID1,ou=people,$SUFFIX" >> $LDIF
   echo "objectClass: inetOrgPerson" >> $LDIF
   echo "objectClass: posixAccount" >> $LDIF
   echo "objectClass: shadowAccount" >> $LDIF
   echo "uid: $UID1" >> $LDIF
   echo "sn: $SN" >> $LDIF
   echo "givenName: $GIVEN" >> $LDIF
   echo "cn: $NAME" >> $LDIF
   echo "displayName: $NAME" >> $LDIF
   echo "uidNumber: $UID2" >> $LDIF
   echo "gidNumber: $GID" >> $LDIF
   echo "userPassword: {crypt}$PASS" >> $LDIF
   echo "gecos: $NAME" >> $LDIF
   echo "loginShell: $SHELL" >> $LDIF
   echo "homeDirectory: $HOME" >> $LDIF
   echo "shadowExpire: $EXPIRE" >> $LDIF
   echo "shadowFlag: $FLAG" >> $LDIF
   echo "shadowWarning: $WARN" >> $LDIF
   echo "shadowMin: $MIN" >> $LDIF
   echo "shadowMax: $MAX" >> $LDIF
   echo "shadowLastChange: $LAST" >> $LDIF
   echo >> $LDIF
done
[root@dir ~]#sh ldapuser.sh
[root@dir ~]#ldapadd -x -D cn=admin,dc=server,dc=world -W -f ldapuser.ldif
Enter LDAP Password:    # LDAP admin password
adding new entry "uid=cent,ou=people,dc=server,dc=world"
adding new entry "uid=fedora,ou=people,dc=server,dc=world"
adding new entry "uid=ubuntu,ou=people,dc=server,dc=world"
adding new entry "uid=debian,ou=people,dc=server,dc=world"
adding new entry "uid=fermi,ou=people,dc=server,dc=world"
```

Thêm nhóm danh sách người dùng vào danh mục LDAP

```
[root@dir ~]#vi ldapgroup.sh
# extract local groups who have 500-999 digit UID
# replace "SUFFIX=***" to your own suffix
# this is an example
#!/bin/bash
SUFFIX='dc=server,dc=world'
LDIF='ldapgroup.ldif'
echo -n > $LDIF
for line in `grep "x:[5-9][0-9][0-9]:" /etc/group`
do
   CN=`echo $line | cut -d: -f1`
   GID=`echo $line | cut -d: -f3`
   echo "dn: cn=$CN,ou=groups,$SUFFIX" >> $LDIF
   echo "objectClass: posixGroup" >> $LDIF
   echo "cn: $CN" >> $LDIF
   echo "gidNumber: $GID" >> $LDIF
   users=`echo $line | cut -d: -f4 | sed "s/,/ /g"`
   for user in ${users} ; do
      echo "memberUid: ${user}" >> $LDIF
   done
   echo >> $LDIF
done
[root@dir ~]#sh ldapgroup.sh
[root@dir ~]#ldapadd -x -D cn=admin,dc=server,dc=world -W -f ldapgroup.ldif
Enter LDAP Password:          # LDAP admin password
adding new entry "cn=cent,ou=groups,dc=server,dc=world"
adding new entry "cn=fedora,ou=groups,dc=server,dc=world"
adding new entry "cn=ubuntu,ou=groups,dc=server,dc=world"
adding new entry "cn=debian,ou=groups,dc=server,dc=world"
adding new entry "cn=fermi,ou=groups,dc=server,dc=world"
```

Nếu muốn xóa người dùng hoặc nhóm người dùng thì có thể dùng các lệnh sau

```
[root@dir ~]#ldapdelete -x -W -D 'cn=admin,dc=server,dc=world'
"uid=cent,ou=people,dc=server,dc=world"
Enter LDAP Password:
[root@dir ~]#ldapdelete -x -W -D 'cn=admin,dc=server,dc=world'
"cn=cent,ou=groups,dc=server,dc=world"
Enter LDAP Password:
```

Test hoạt động của openldap

- Xem file /etc/openldap/slapd.conf với những option mặc định:

- Sửa những dòng sau trong file /etc/openldap/slapd.conf:

- Khởi động dịch vụ ldap

- Soạn thảo file /etc/sample.ldif có nội dung như sau:

- Dùng lệnh ldapadd để add nội dung của file sample.ldif vào ldap server

- Dùng lệnh ldapsearch tiến hành tìm kiếm những dữ liệu vừa import:

- Tìm kiếm entry có "cn=bogus"

- Xóa entry "cn=bogus,dc=example,dc=org":

- Kiểm tra lại:

5.8.2. CẤU HÌNH LDAP CLIENT

```
[root@linux ~]#yum -y install openldap-clients nss-pam-ldapd
[root@linux ~]#vi /etc/openldap/ldap.conf
# add at the last line
# LDAP server's URI
URI ldap://10.0.0.39/
# specify Suffix
BASE dc=server,dc=world
TLS_CACERTDIR /etc/openldap/cacerts
[root@linux ~]#vi /etc/nslcd.conf
# line 131: specify URI, Suffix
uri
ldap://10.0.0.39/
base dc=server,dc=world
ssl no
tls_cacertdir /etc/openldap/cacerts
[root@linux ~]#vi /etc/pam_ldap.conf
```

```
# line 17: make it comment
#host 127.0.0.1
# line 20: specify Suffix
base dc=server,dc=world
# add at the last line
uri ldap://10.0.0.39/
ssl no
tls_cacertdir /etc/openldap/cacerts
pam_password md5
[root@linux ~]#vi /etc/pam.d/system-auth
# add like follows
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so
account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so
password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so
session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond
quiet use_uid
session     required      pam_unix.so
session     optional      pam_ldap.so
# add if you need ( create home directory automatically if it's none )
session     optional      pam_mkhomedir.so skel=/etc/skel umask=077
[root@linux ~]#vi /etc/nsswitch.conf
passwd:     files       ldap  # line 33: add
shadow:     files       ldap  # add
group:      files       ldap  # add
netgroup:   ldap        # line 57: change
automount: files ldap   # line 61: change
```

```
[root@linux ~]#vi /etc/sysconfig/authconfig
# line 18: change
USELDAP=yes
[root@linux ~]#chkconfig nslcd on
[root@linux ~]#shutdown -r now
www.serverlinux.vn login:fermi      # user on LDAP

Password:
Creating directory '/home/fermi'.
[fermi@www ~]$          # just logined
[fermi@www ~]$ passwd   # try to change LDAP password
Changing password for user fermi.
Enter login(LDAP) password:
New password:
Retype new password:
LDAP password information changed for fermi
passwd: all authentication tokens updated successfully.
```

CHƯƠNG 06: QUẢN LÝ CƠ SỞ DỮ LIỆU TRÊN LINUX

6.1. CƠ SỞ DỮ LIỆU MYSQL

6.1.1. CÀI ĐẶT MYSQL

```
[root@linux ~]#yum -y install mysql-server

[root@linux ~]#/etc/rc.d/init.d/mysqld start
Initializing MySQL database:  Installing MySQL system tables...OK
Filling help tables...  OK
……
Please report any problems with the /usr/bin/mysqlbug script!
Starting mysqld:              [  OK  ]

[root@linux ~]#chkconfig mysqld on

[root@linux ~]#mysql -u root
# connect to MySQL
mysql>select user,host,password from mysql.user;
```

```
+------+-----------------+----------+
| user | host            | password |
+------+-----------------+----------+
| root | localhost       |          |
| root | www.server.world |          |
| root | 127.0.0.1       |          |
|      | localhost       |          |
|      | www.server.world |          |
+------+-----------------+----------+
5 rows in set (0.00 sec)
```

```
# set root password
mysql>set password for root@localhost=password('password');
Query OK, 0 rows affected (0.00 sec)
# set root password
mysql>set password for root@'127.0.0.1'=password('password');
Query OK, 0 rows affected (0.00 sec)
# set root password
mysql>set password for root@'www.serverlinux'=password('password');
Query OK, 0 rows affected (0.00 sec)
# delete anonymous user
mysql>delete from mysql.user where user='';
Query OK, 2 rows affected (0.00 sec)
mysql>select user,host,password from mysql.user;
```

```
+------+-----------------+-------------------------------------------+
| user | host            | password                                  |
+------+-----------------+-------------------------------------------+
| root | localhost       | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root | www.server.world | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root | 127.0.0.1       | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+------+-----------------+-------------------------------------------+
3 rows in set (0.00 sec)
mysql>exit # quit
Bye

[root@linux ~]#mysql -u root -p # connect with root
Enter password:   # MySQL root password
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights
reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,and
you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>exit
Bye
```

6.1.2. CÀI ĐẶT VÀ CẤU HÌNH PHPMYADMIN

```
[root@linux ~]#yum --enablerepo=epel -y install phpMyAdmin php-mysql php-
mcrypt
# install from EPEL

[root@linux ~]#vi /etc/httpd/conf.d/phpMyAdmin.conf
# line 14: add IP address you permit
Allow from 127.0.0.1
10.0.0.0/24

[root@linux ~]#/etc/rc.d/init.d/httpd reload
Reloading httpd:          [ OK ]
```

Truy cập 'http://(hostname hoặc IP address)/ trong trình duyệt để truy cập vào cơ sở dữ liệu với user của MySQL.

6.2. CƠ SỞ DỮ LIỆU ORACLE

6.2.1. CÀI ĐẶT ORACLE

```
[root@db01 ~]#yum -y install binutils compat-libstdc++-33 elfutils-libelf
elfutils-libelf-devel glibc glibc-common glibc-devel gcc gcc-c++ libaio
libaio-devel libgcc libstdc++ libstdc++-devel make sysstat unixODBC
unixODBC-devel
```

Chỉnh sửa các tham số kernel

```
[root@db01 ~]#vi /etc/sysctl.conf
# make it comment
#net.bridge.bridge-nf-call-ip6tables = 0
#net.bridge.bridge-nf-call-iptables = 0
#net.bridge.bridge-nf-call-arptables = 0
# add at the last line
net.ipv4.ip_local_port_range = 9000 65500
fs.file-max = 6815744
kernel.shmall = 10523004
kernel.shmmax = 6465333657
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
net.core.rmem_default=262144
net.core.wmem_default=262144
net.core.rmem_max=4194304
net.core.wmem_max=1048576
fs.aio-max-nr = 1048576

[root@db01 ~]#sysctl -p
net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.ip_local_port_range = 9000 65500
fs.file-max = 65536
kernel.shmall = 10523004
kernel.shmmax = 6465333657
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
net.core.rmem_default = 262144
```

```
net.core.wmem_default = 262144
net.core.rmem_max = 4194304
net.core.wmem_max = 1048576
fs.aio-max-nr = 1048576
```

Tạo user cho oracle.

```
[root@db01 ~]#groupadd -g 200 oinstall

[root@db01 ~]#groupadd -g 201 dba

[root@db01 ~]#useradd -u 440 -g oinstall -G dba -d /usr/oracle oracle

[root@db01 ~]#vi /etc/pam.d/login# near line 14: add
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    required     pam_limits.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
-session   optional     pam_ck_connector.so

[root@db01 ~]#vi /etc/security/limits.conf
# add at the last line
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft nofile 1024
oracle hard nofile 65536

[root@db01 ~]#vi /etc/profile
# add at the last line
if [ $USER = "oracle" ]; then
if [ $SHELL = "/bin/ksh" ]; then
ulimit -p 16384
ulimit -n 65536
else
ulimit -u 16384 -n 65536
fi
fi
```

Cài đặt oracle 11g R2

Tải Oracle Databse 11g R2 dành cho Linux tại địa chỉ http://www.oracle.com/technology/software/products/database/index.html

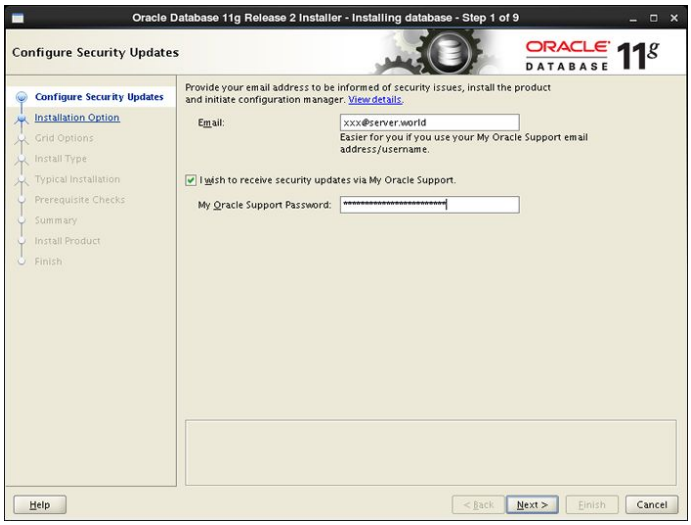
Sau khi tải về tiến hành giải nén theo các bước sau:

```
[oracle@db01 ~]$cd tmp
[oracle@db01 tmp]$unzip linux.x64_11gR2_database_1of2.zip
[oracle@db01 tmp]$unzip linux.x64_11gR2_database_2of2.zip
```

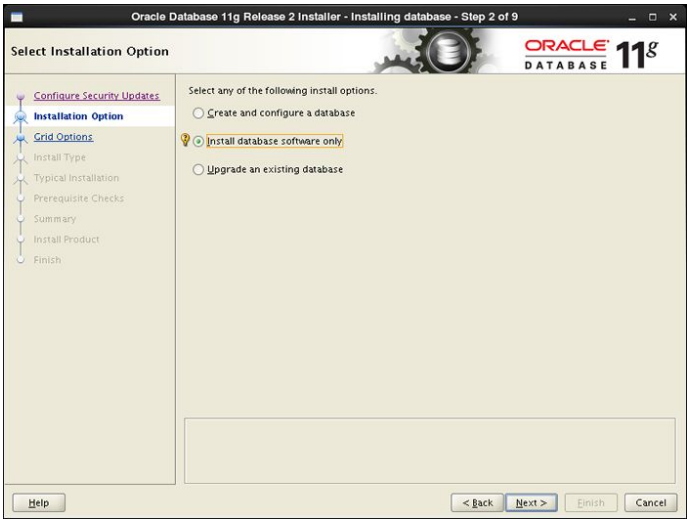
Tiến hành cài đặt

```
[oracle@db01 tmp]$./database/runInstaller
```

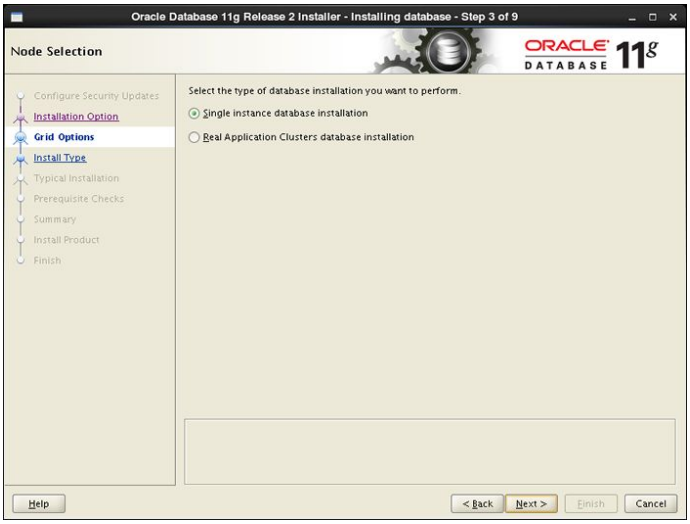
a) Trình cài đặt Oracle khởi động. Đầu tiên, nhập địa chỉ email và password để nhận thông tin từ Oracle như security. Nhấn Next để tiếp tục.



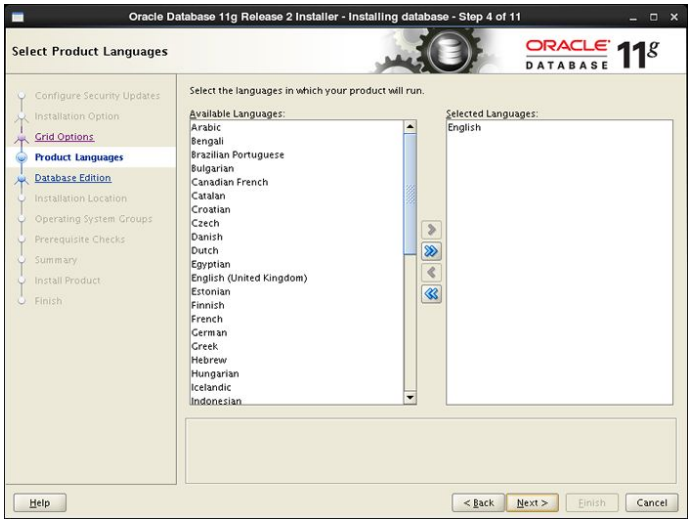
b) Chọn "Install database software only".



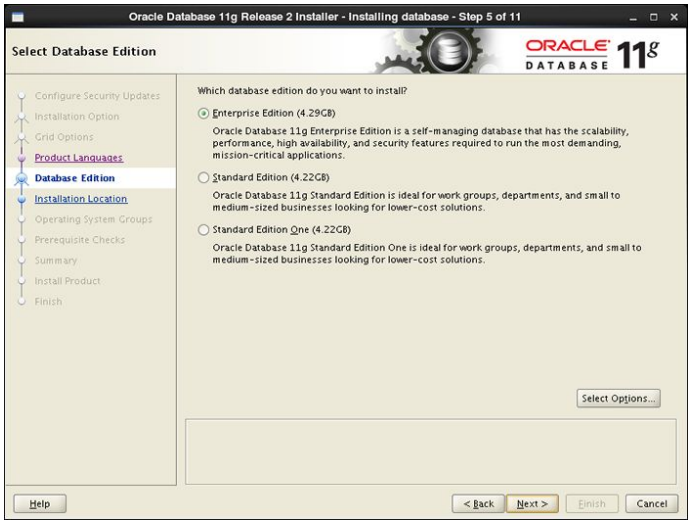
c) Chọn "Single Instance ***".



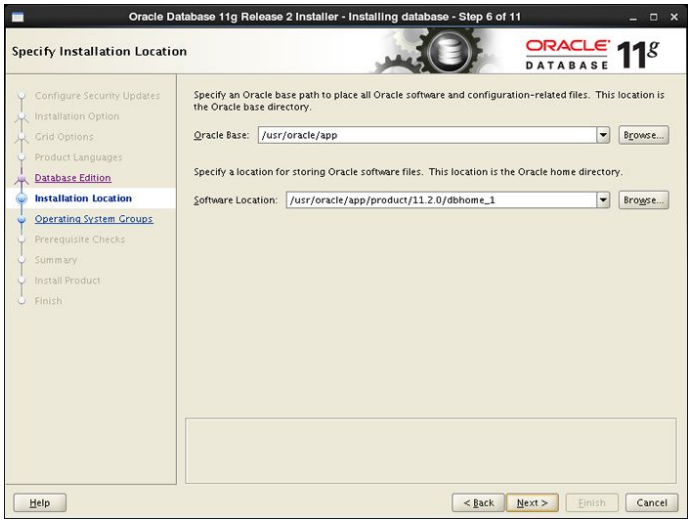
d) Chọn ngôn ngữ.



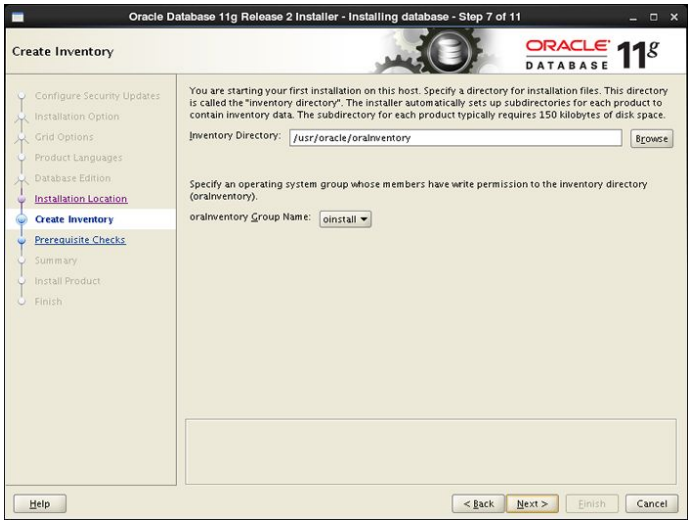
e) Chọn Enterprise edition.



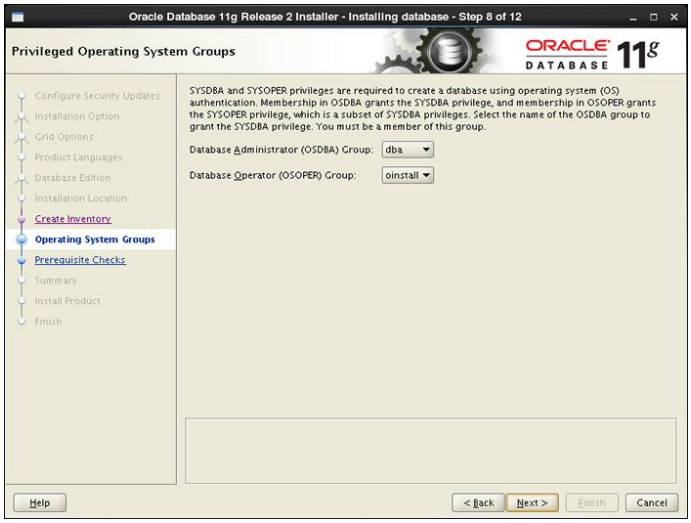
f) Chọn thư mục cài đặt Oracle. Trong ví dụ này, giữ default và nhấn Next để tiếp tục



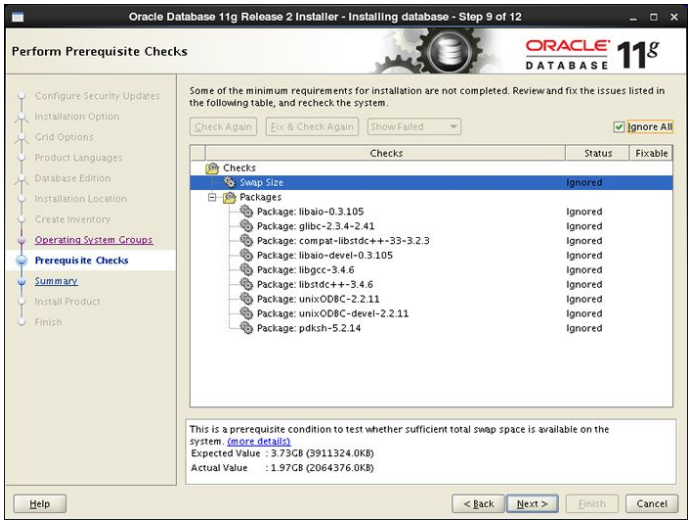
g) Chọn mặc định và tiếp tục.



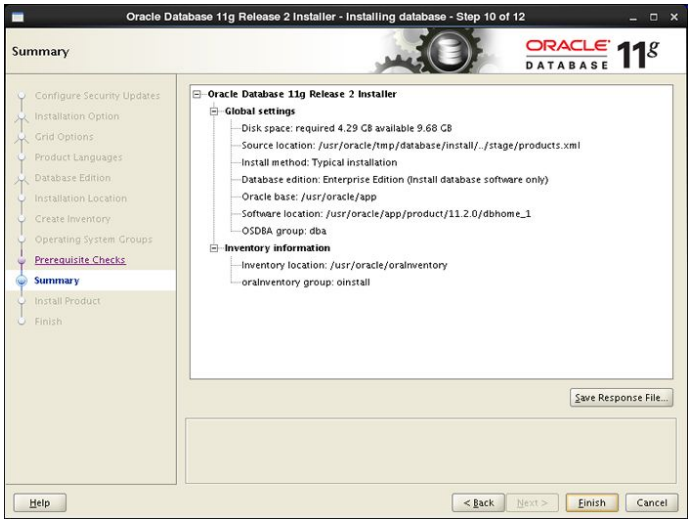
h) Lựa chọn group cơ dữ liệu. Trong ví dụ này chọn default và tiếp tục.



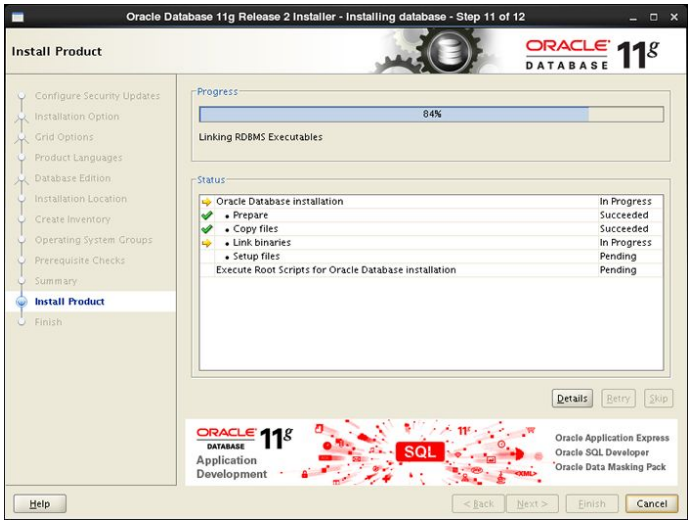
i) Nhấn Next để tiếp tục



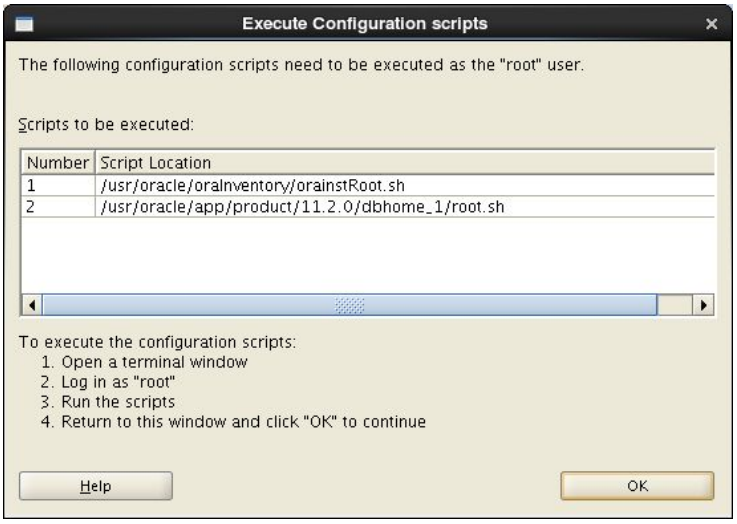
j) Click "Finish" nếu tất cả OK.



k) Trình cài đặt bắt đầu, nhấn nút Finish.

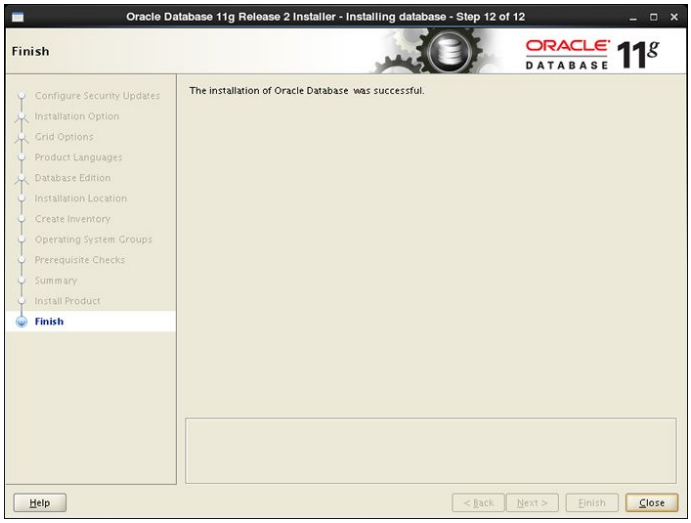


l) Màn hình sau hiển thị, sau đó mở terminal và thực thi các lệnh sau với user root.




```
[root@db01 ~]# /usr/oracle/oraInventory/orainstRoot.sh
Changing permissions of /usr/oracle/oraInventory.
Adding read,write permissions for group.
Removing read,write,execute permissions for world.
Changing groupname of /usr/oracle/oraInventory to oinstall.
The execution of the script is complete.
[root@db01~]#/usr/oracle/app/product/11.2.0/dbhome_1/root.sh
Running Oracle 11g root.sh script...
The following environment variables are set as:
ORACLE_OWNER= oracle
ORACLE_HOME= /usr/oracle/app/product/11.2.0/dbhome_1
Enter the full pathname of the local bin directory: [/usr/local/bin]: #
Enter
Copying dbhome to /usr/local/bin ...
Copying oraenv to /usr/local/bin ...
Copying coraenv to /usr/local/bin ...
Creating /etc/oratab file...
Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
Finished product-specific root actions.
```

m) Cài đặt hoàn thành click nút "Close".



n) Cấu hình cho user Oracle.

```
[oracle@db01 ~]$vi ~/.bash_profile
# add at the last lone
export ORACLE_HOME=$ORACLE_BASE/product/11.2.0/dbhome_1
export PATH=$PATH:$ORACLE_HOME/bin
[oracle@db01 ~]$source ~/.bash_profile
[oracle@db01 ~]$rm -rf tmp
```

o) Tạo danh sách Oracle Net Listener

Create a Oracle Net Listener that is a network service on Oracle.

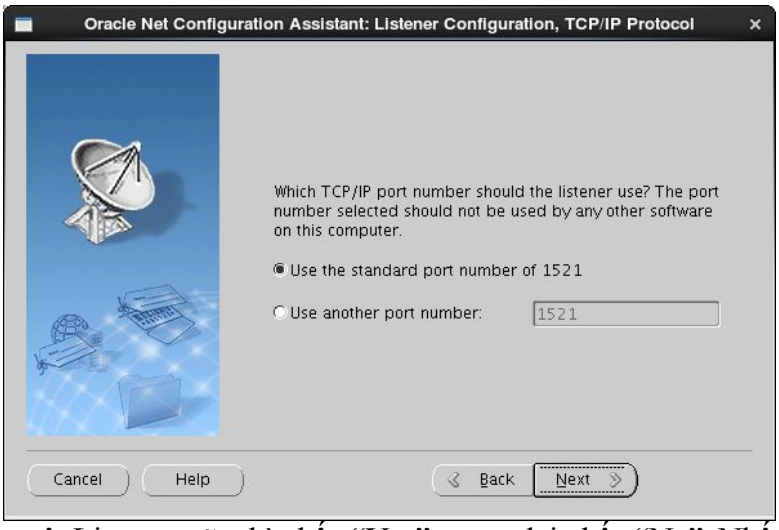
Login tài khoản Oracle và nhập vào lệnh "netca", sau khi sau xuất hiện. Check vào nút "Listener Configuration" và nhấn next.

Nhấn Next.

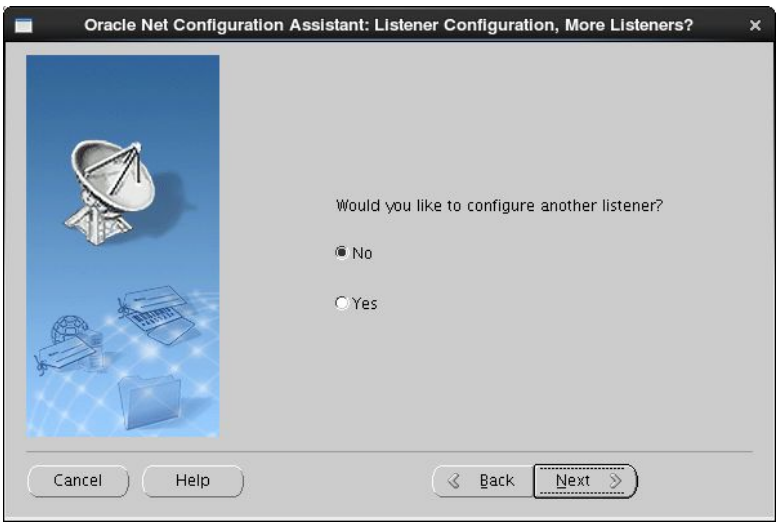
Nhập tên Listner mà bạn thích (tên gì cũng được)

Trong ví dụ này giữ mặc định "TCP". Có thể thay đổi các giá trị mặc định này.

Nhập port. Trong ví dụ này giữ mặc định. Có thể thay đổi các giá trị này.



Nếu muốn tạo tiếp một Listener nữa thì nhấn "Yes" ngược lại nhấn "No". Nhấn "No" để tiếp tục



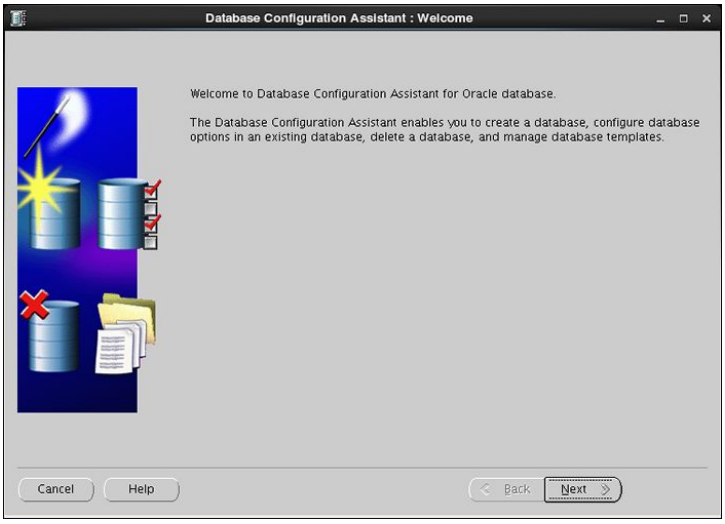
Cấu hình hoàn thành

Click "Finish" để kết thúc. Sau khi hoàn thành, nhập lại trạng thái bằng lệnh "netstat".

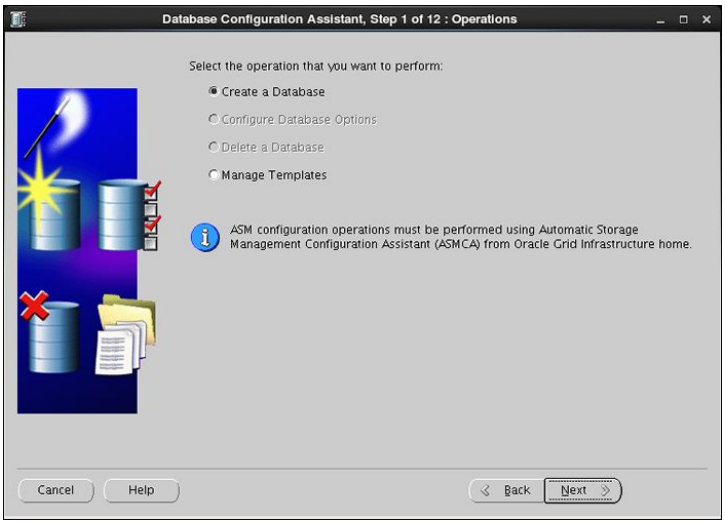
6.2.2. TRIỂN KHAI THIẾT LẬP CSDL SỬ DỤNG ORACLE

Tạo cơ sở dữ liệu.

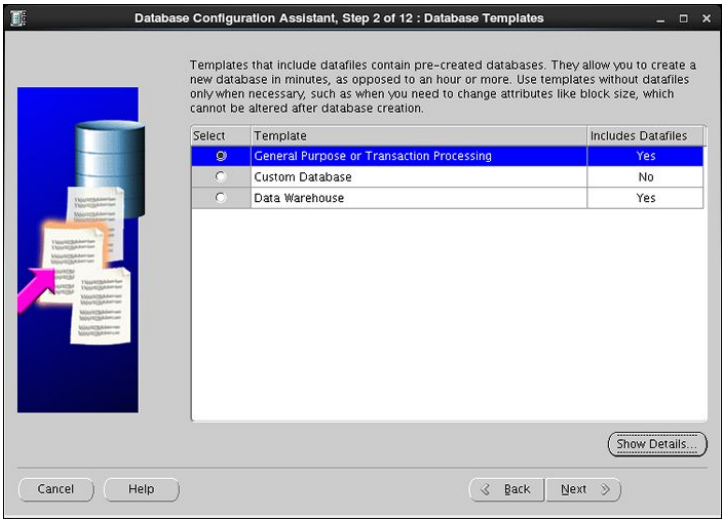
a) Login vào user trong Oracle và nhập vào lệnh "dbca", nhấn "Next" để tiếp tục



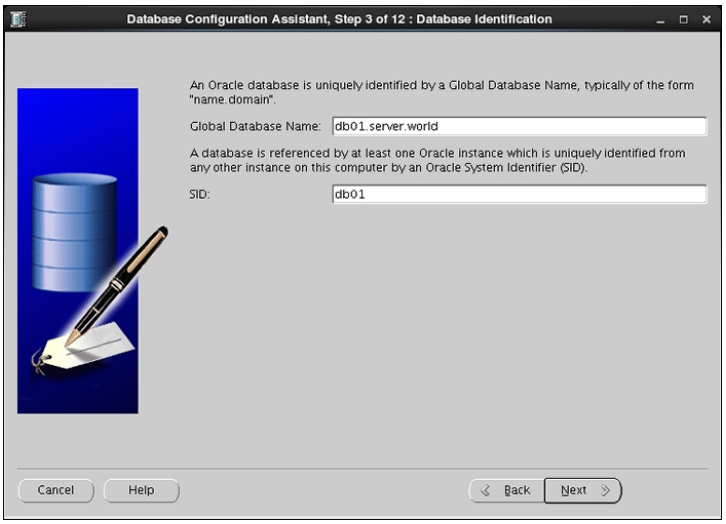
b) Chọn "Create Database" và nhấn next



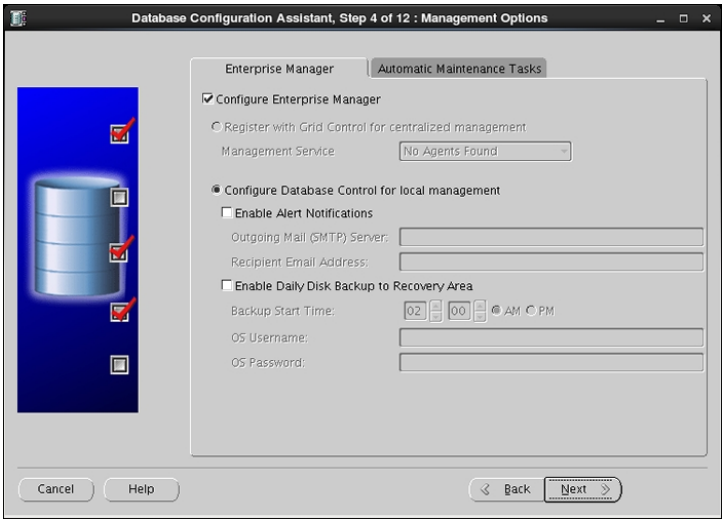
c) Chọn "General Purpose ***" và tiếp tục



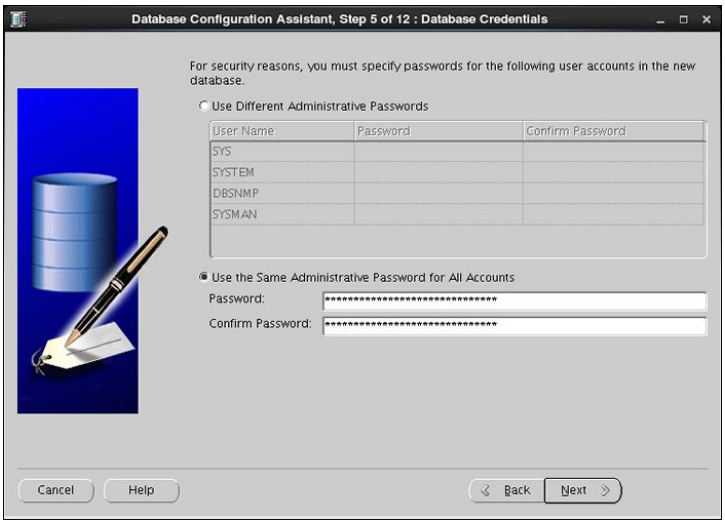
d) Nhập tên Grobal Database và SID như bên dưới.



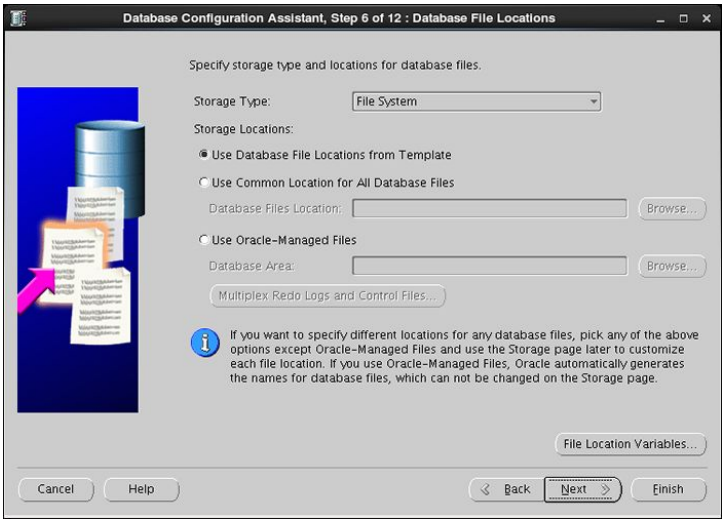
e) Giữ giá trị mặc định và tiếp tục



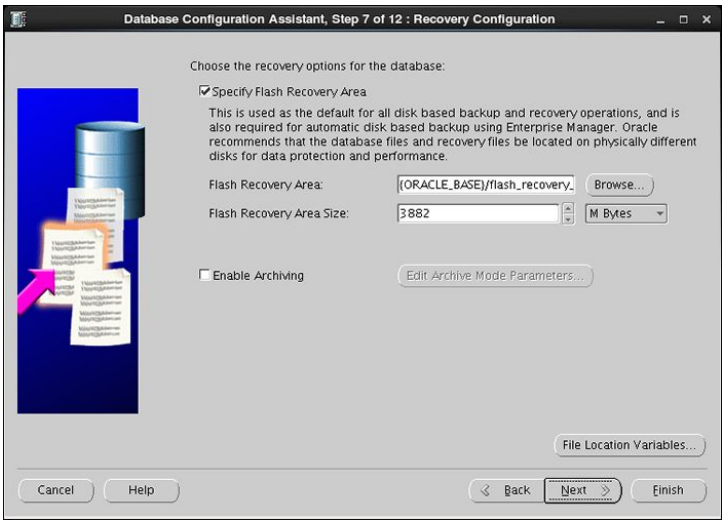
f) Nhập passwords. Nên nhập mật khẩu có tính bảo mật cao



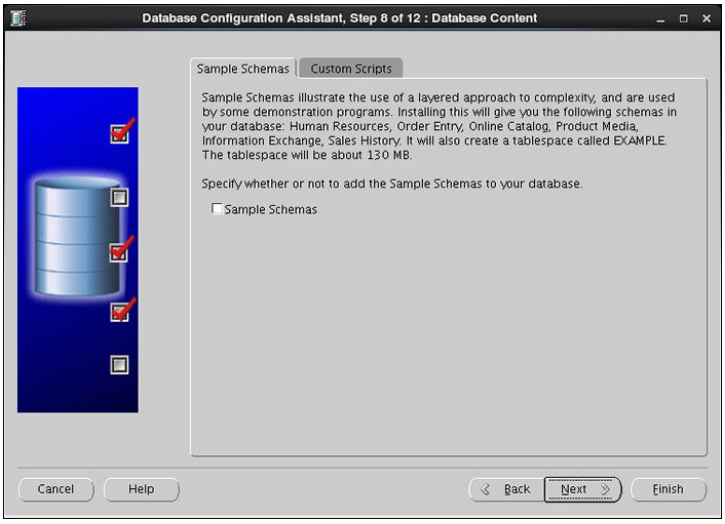
g) Giữ giá trị mặc định là "File System".



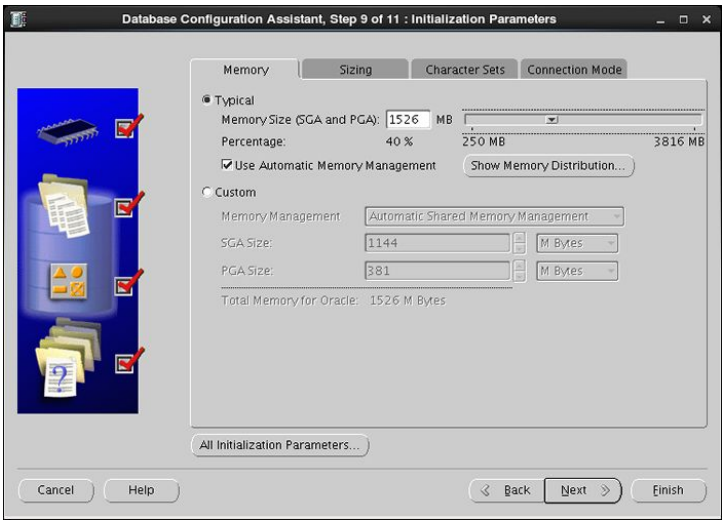
h) Configure recovery settings. If you'd like to change it, Set it.



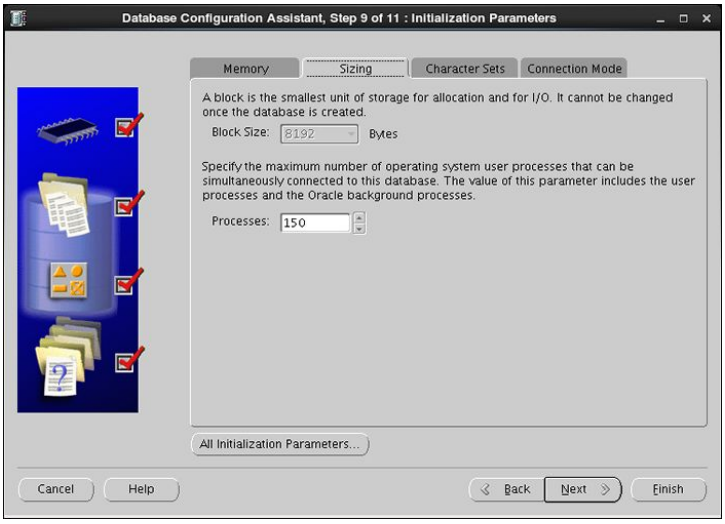
i) Configure sample schema and scripts. If you'd like to add them, Set them.



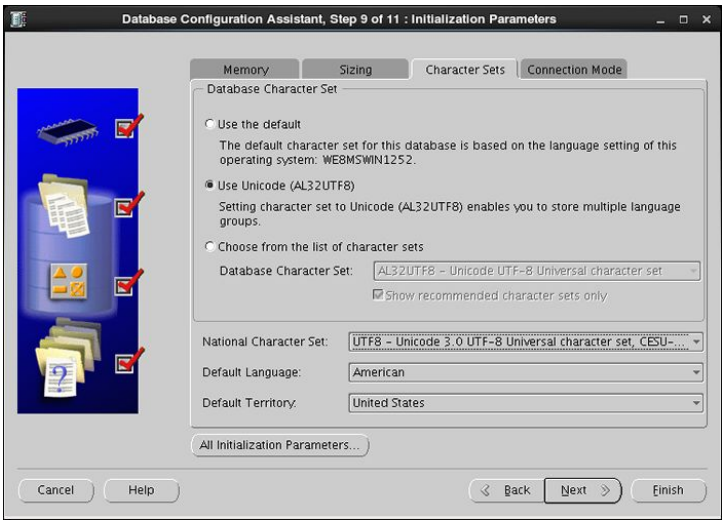
j) Configure memory setting. After setting, go to next tab.



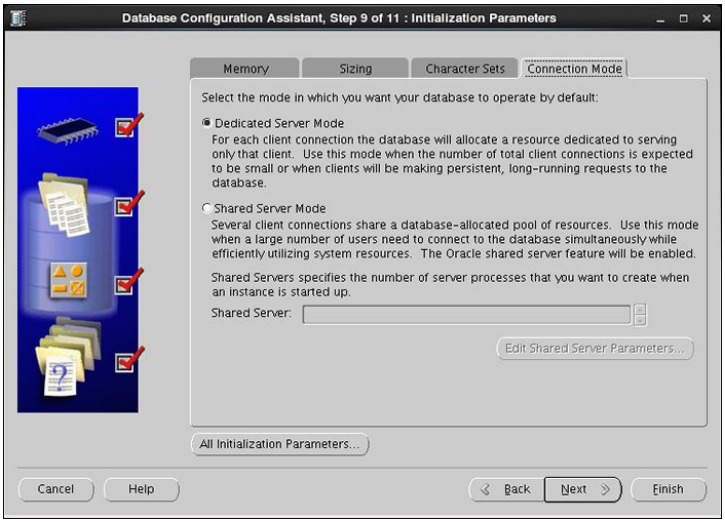
k) Specify max processes.



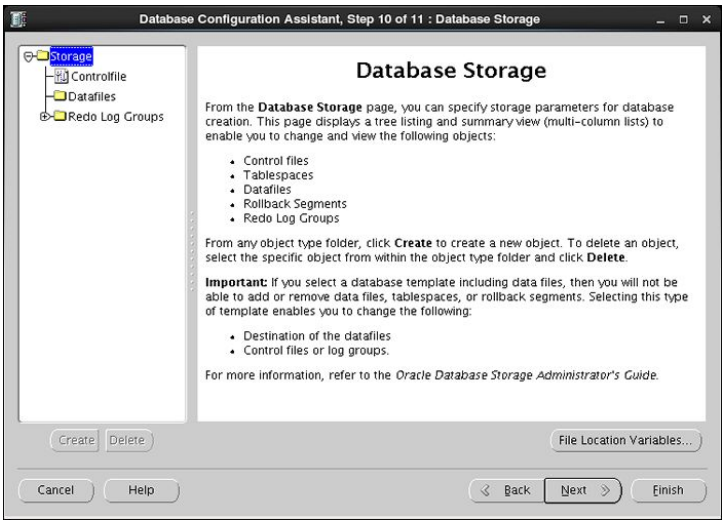
l) Set Character setting.



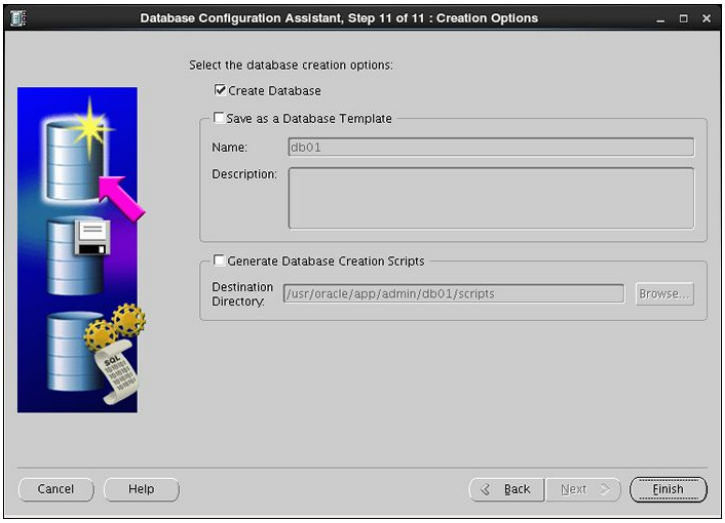
m)Select connection mode. If your server does not have many clients, Select Dedicated server mode. If your server has many clients, Select Shared server mode.



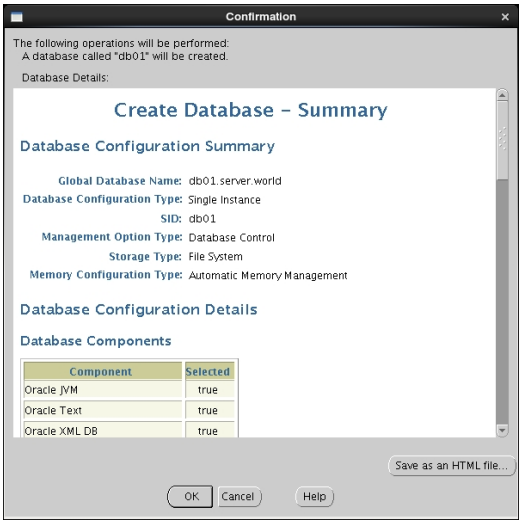
n) Confirm parameters for Storage settings. If you'd like to change, set them.



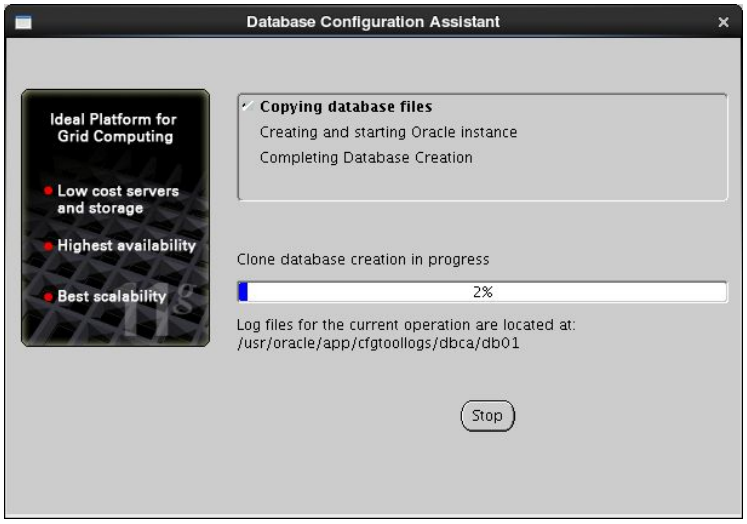
o) Configuration completed. Click "Finish" button to finish.



p) Confirm settings and Click "OK" if all are OK.



q) Database creation starts.



r) Sau khi cơ sở dữ liệu tạo xong nhân "Exit" để hoàn thành.

s) Access to a URL that is shown on finished screen above with web browser, then follwing screen is shown. Input a user name and password that you configured on the section

Create a init Scriptmake Oracle start automatically on system booting.

t) Change like folows first.

```
[root@db01 ~]#vi /etc/oratab
db01:/usr/oracle/app/product/11.2.0/dbhome_1:Y# change
```

```
[root@db01 ~]#vi /usr/oracle/.bash_profile
# add your SID at the last line
export ORACLE_SID=db01
```

u) Create a init Script

```
[root@db01 ~]#vi /etc/rc.d/init.d/oracle
# this is an example
#!/bin/bash
# oracle: Start/Stop Oracle Database 11g R2
#
# chkconfig: 345 90 10
# description: The Oracle Database is an Object-Relational Database
Management System.
#
# processname: oracle
. /etc/rc.d/init.d/functions
LOCKFILE=/var/lock/subsys/oracle
ORACLE_HOME=/usr/oracle/app/product/11.2.0/dbhome_1
ORACLE_USER=oracle
case "$1" in
'start')
   if [ -f $LOCKFILE ]; then
      echo $0 already running.
      exit 1
   fi
   echo -n $"Starting Oracle Database:"
   su - $ORACLE_USER -c "$ORACLE_HOME/bin/lsnrctl start"
   su - $ORACLE_USER -c "$ORACLE_HOME/bin/dbstart $ORACLE_HOME"
   su - $ORACLE_USER -c "$ORACLE_HOME/bin/emctl start dbconsole"
   touch $LOCKFILE
   ;;
'stop')
   if [ ! -f $LOCKFILE ]; then
      echo $0 already stopping.
      exit 1
   fi
   echo -n $"Stopping Oracle Database:"
   su - $ORACLE_USER -c "$ORACLE_HOME/bin/lsnrctl stop"
   su - $ORACLE_USER -c "$ORACLE_HOME/bin/dbshut"
   su - $ORACLE_USER -c "$ORACLE_HOME/bin/emctl stop dbconsole"
   rm -f $LOCKFILE
   ;;
'restart')
```

```
   $0 stop
   $0 start
   ;;
'status')
   if [ -f $LOCKFILE ]; then
      echo $0 started.
      else
      echo $0 stopped.
   fi
   ;;
*)
   echo "Usage: $0 [start|stop|status]"
   exit 1
esac
exit 0
```

```
[root@db01 ~]#chmod 755 /etc/rc.d/init.d/oracle
[root@db01 ~]#/etc/rc.d/init.d/oracle start
Starting Oracle Database:
LSNRCTL for Linux: Version 11.2.0.1.0 - Production on 12-JUL-2011 23:41:57
Copyright (c) 1991, 2009, Oracle.  All rights reserved.
Starting /usr/oracle/app/product/11.2.0/dbhome_1/bin/tnslsnr: please
wait...
TNSLSNR for Linux: Version 11.2.0.1.0 - Production
System parameter file is
/usr/oracle/app/product/11.2.0/dbhome_1/network/admin/listener.ora
Log messages written to
/usr/oracle/app/diag/tnslsnr/db01/listener/alert/log.xml
Listening on:
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=db01.serverlinux)(PORT=1521)))
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=db01.serverlinux)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 11.2.0.1.0 -
Production
Start Date                12-JUL-2011 23:41:57
Uptime                    0 days 0 hr. 0 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
```

```
Listener Parameter File
/usr/oracle/app/product/11.2.0/dbhome_1/network/admin/listener.ora
Listener Log File
/usr/oracle/app/diag/tnslsnr/db01/listener/alert/log.xml
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=db01.serverlinux)(PORT=1521)))
The listener supports no services
The command completed successfully
Processing Database instance "db01": log file
/usr/oracle/app/product/11.2.0/dbhome_1/startup.log
Oracle Enterprise Manager 11g Database Control Release 11.2.0.1.0
Copyright (c) 1996, 2009 Oracle Corporation.  All rights reserved.
https://db01.serverlinux:1158/em/console/aboutApplication
Starting Oracle Enterprise Manager 11g Database Control ........ started.
------------------------------------------------------------
Logs are generated in directory
/usr/oracle/app/product/11.2.0/dbhome_1/db01.serverlinux_db01/sysman/log
```

```
[root@db01 ~]#chkconfig --add oracle
[root@db01 ~]#chkconfig oracle on
```

6.2.3. CÀI ĐẶT JAVA DEVELOPMENT ENVIRONMENT

Cài đặt Java SE Development Kit (JDK)

a) Tải jdk-7-linux-x64.rpm từ địa chỉ http://download.oracle.com/otn-pub/java/jdk/7/jdk-7-linux-i586.rpm hoặc và địa chỉ của Oracle (http://www.oracle.com/technetwork/java/javase/downloads/java-se-jdk-7-download-432154.html)

b) Cài đặt JDK

```
[root@linux ~]#rpm -Uvh jdk-7-linux-x64.rpm
Preparing...      ########################################### [100%]
   1:jdk          ########################################### [100%]
Unpacking JAR files...
        rt.jar...
        jsse.jar...
        charsets.jar...
```

```
        tools.jar...
        localedata.jar...

[root@linux ~]#vi /etc/profile
# add at the last line
export JAVA_HOME=/usr/java/default
export PATH=$PATH:$JAVA_HOME/bin
export
CLASSPATH=.:$JAVA_HOME/jre/lib:$JAVA_HOME/lib:$JAVA_HOME/lib/tools.jar
[root@linux ~]#source /etc/profile
```

c) Test thử bằng cách tạo chương trình sau

```
[root@linux ~]#vi day.java
import java.util.Calendar;
class day {
   public static void main(String[] args) {
      Calendar cal = Calendar.getInstance();
      int year = cal.get(Calendar.YEAR);
      int month = cal.get(Calendar.MONTH) + 1;
      int day = cal.get(Calendar.DATE);
      int hour = cal.get(Calendar.HOUR_OF_DAY);
      int minute = cal.get(Calendar.MINUTE);
      System.out.println(year + "/" + month + "/" + day + " " + hour + ":"
+ minute);
   }
}
[root@linux ~]#javac day.java             # compile
[root@linux ~]#java day                   # execute
2011/7/30 21:7
```

6.2.4. **JAVA APPLICATION SERVER - TOMCAT 7**

a) Cài đặt và cấu hình Tomcat 7

```
[root@linux ~]#wgethttp://ftp.riken.jp/net/apache/tomcat/tomcat-
7/v7.0.23/bin/apache-tomcat-7.0.23.tar.gz

[root@linux ~]#tar zxvf apache-tomcat-7.0.16.tar.gz

[root@linux ~]#mv apache-tomcat-7.0.16 /usr/tomcat7

[root@linux ~]#useradd -d /usr/tomcat7 tomcat
```

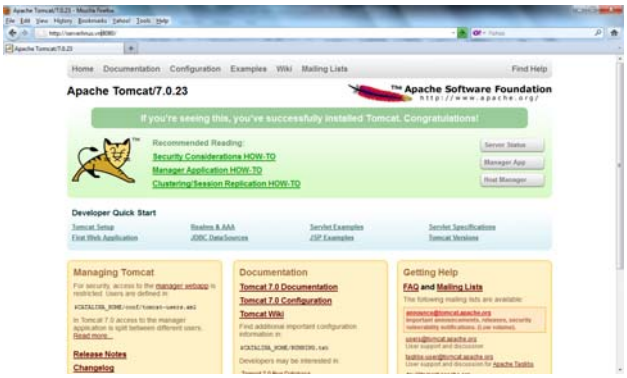
```
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
[root@linux ~]#chown -R tomcat. /usr/tomcat7
```

b) Tạo script INIT

```
[root@linux ~]# vi /etc/rc.d/init.d/tomcat7
#!/bin/bash

# Tomcat7: Start/Stop Tomcat 7
#
# chkconfig: - 90 10
# description: Tomcat is a Java application Server.

. /etc/init.d/functions
. /etc/sysconfig/network

CATALINA_HOME=/usr/tomcat7
TOMCAT_USER=tomcat
LOCKFILE=/var/lock/subsys/tomcat

RETVAL=0
start(){
   echo "Starting Tomcat7: "
   su - $TOMCAT_USER -c "$CATALINA_HOME/bin/startup.sh"
   RETVAL=$?
   echo
   [ $RETVAL -eq 0 ] && touch $LOCKFILE
   return $RETVAL
}

stop(){
   echo "Shutting down Tomcat7: "
   $CATALINA_HOME/bin/shutdown.sh
   RETVAL=$?
   echo
   [ $RETVAL -eq 0 ] && rm -f $LOCKFILE
   return $RETVAL
}

case "$1" in
   start)
      start
```

```
      ;;
   stop)
      stop
      ;;
   restart)
      stop
      start
      ;;
   status)
      status tomcat
      ;;
   *)
      echo $"Usage: $0 {start|stop|restart|status}"
      exit 1
      ;;
esac
exit $?

[root@linux ~]#chmod 755 /etc/rc.d/init.d/tomcat7

[root@linux ~]#/etc/rc.d/init.d/tomcat7 start

Starting Tomcat7:
Using CATALINA_BASE:          /usr/tomcat7

Using CATALINA_HOME:          /usr/tomcat7

Using CATALINA_TMPDIR:        /usr/tomcat7/temp

Using JRE_HOME:               /usr/java/default

Using CLASSPATH:  /usr/tomcat7/bin/bootstrap.jar:/usr/tomcat7/bin/tomcat-
juli.jar
[root@linux ~]#chkconfig --add tomcat7

[root@linux ~]#chkconfig tomcat7 on
```

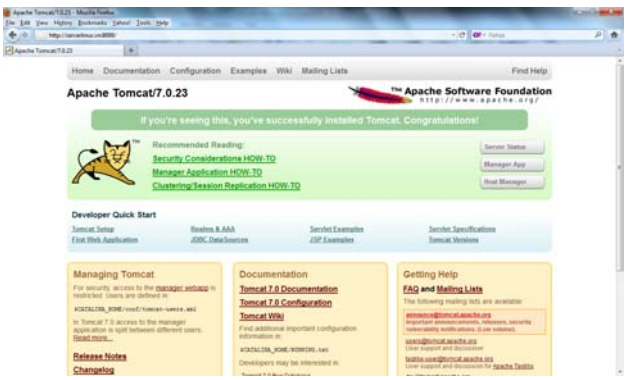
c) Truy cập vào trình duyệt web theo địa chỉ Access to "http://(your hostname or IP address):8080/, trong ví dụ này là http://serverlinux.vn:8080/



d) Cấu hình truy cập với port khác port 8080 trong URL.

```
[root@linux ~]#vi /etc/httpd/conf.d/proxy_ajp.conf
# add at the last line
ProxyPass /tomcat/ ajp://localhost:8009/
#Khởi động lại dịch vụ web
[root@linux ~]#/etc/rc.d/init.d/httpd restart

Stopping httpd:                            [  OK  ]
Starting httpd:                            [  OK  ]
```

e) Truy cập vào trình duyệt theo địa chỉ http://(your hostname or IP address)/tomcat/" với port mới 8009 như ở bước c



f) Tạo bài test servlet hiển thị giờ và ngày hiện tại của hệ thống

```
[root@linux ~]#mkdir /usr/tomcat7/webapps/ROOT/WEB-INF/classes

[root@linux ~]#chown tomcat. /usr/tomcat7/webapps/ROOT/WEB-INF/classes
```

```
[root@linux ~]#cd /usr/tomcat7/webapps/ROOT/WEB-INF/classes

[root@linux classes]#vi daytime.java
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.util.Calendar;

public class daytime extends HttpServlet {
   public void doGet(HttpServletRequest request
      ,HttpServletResponse response)

   throws IOException, ServletException{
      response.setContentType("text/html");
      PrintWriter out = response.getWriter();
      Calendar cal = Calendar.getInstance();
      out.println("<html>");
      out.println("<head>");
      out.println("<title>DayTime</title>");
      out.println("</head>");
      out.println("<body>");
      out.println("<div style=\"font-size: 40px; text-align: center; font-
weight: bold\">");
      out.println(cal.get(Calendar.YEAR) + "/" + (cal.get(Calendar.MONTH) +
1) + "/" +
      cal.get(Calendar.DATE) + " " + cal.get(Calendar.HOUR_OF_DAY) + ":" +
cal.get(Calendar.MINUTE));
      out.println("</div>");
      out.println("</body>");
      out.println("</html>");
   }
}

[root@linux classes]#javac -classpath /usr/tomcat7/lib/servlet-api.jar
daytime.java

[root@linux classes]#vi /usr/tomcat7/webapps/ROOT/WEB-INF/web.xml
# add follows between <web-app> - </web-app>

<servlet>
   <servlet-name>daytime</servlet-name>
   <servlet-class>daytime</servlet-class>
</servlet>
```

```
<servlet-mapping>
   <servlet-name>daytime</servlet-name>
   <url-pattern>/daytime</url-pattern>
</servlet-mapping>
```

g) Truy cập vào trình duyệt theo địa chỉ http://(your hostname or IP address)/tomcat/daytime

CẤU HÌNH MỘT SỐ DỊCH VỤ KHÁC

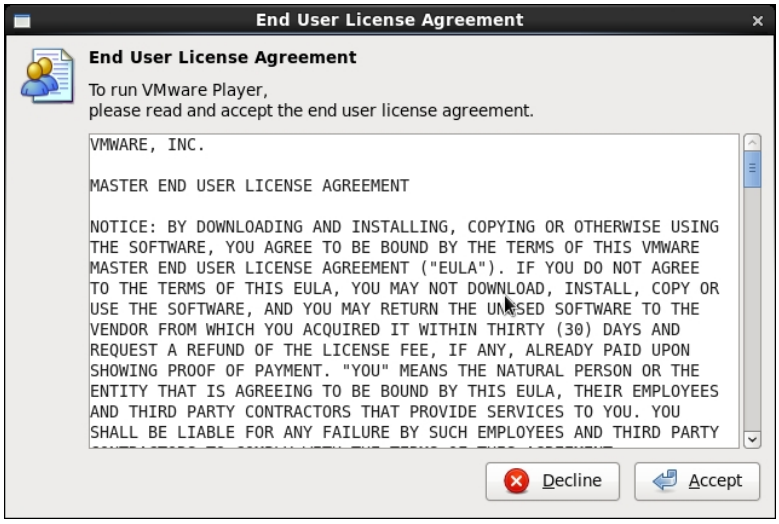
7.1. CÀI ĐẶT VÀ CẤU HÌNH VMWARE PLAYER

a) Tải phần mềm VMware-Player-3.1.4-385536.x86_64.bundle từ website của Vmware (http://www.vmware.com/products/player/)

b) Cài đặt VMWare Player

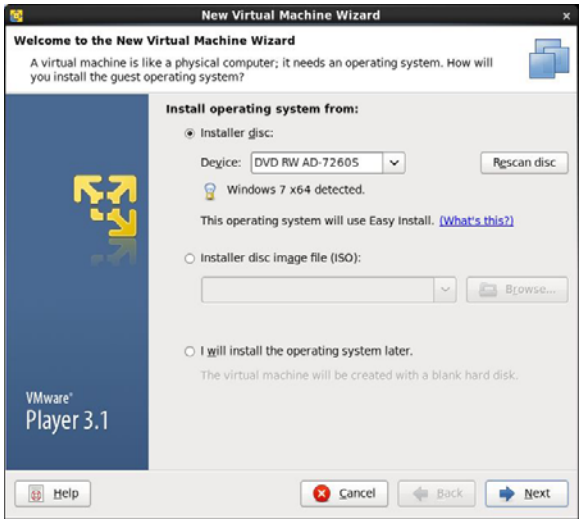
```
[root@linux ~]#chmod 700 VMware-Player-3.1.4-385536.x86_64.bundle

[root@linux ~]#./VMware-Player-3.1.4-385536.x86_64.bundle

Extracting VMware Installer...done.
Would you like to check for product updates on startup? [yes]:
# Enter
Would you like to help make VMware software better by sending
anonymous system data and usage statistics to VMware? [yes]:
# Enter
The product is ready to be installed. Press Enter to begin
installation or Ctrl-C to cancel.
# Enter
Installing VMware Player Application 3.1.4
    Configuring...
[###########################################################] 100%
Installation was successful.
```

c) Từ giao diện đồ họa vào 'System tools'→ 'VMware Player'

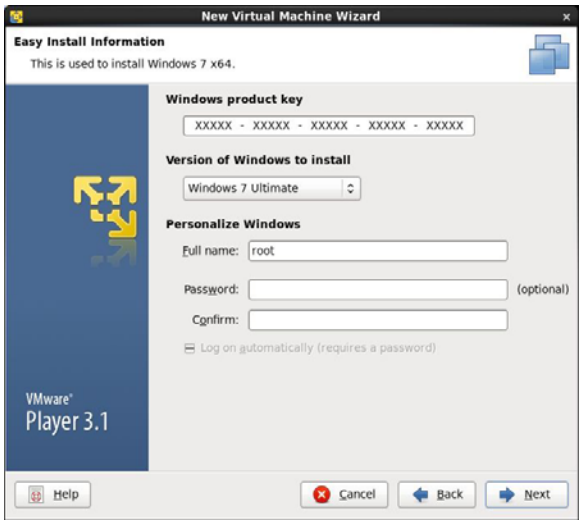


d) Click 'Create a New Virtual machine'.

e) Đặt đĩa cài đặt vào ổ đĩa và nhấn next

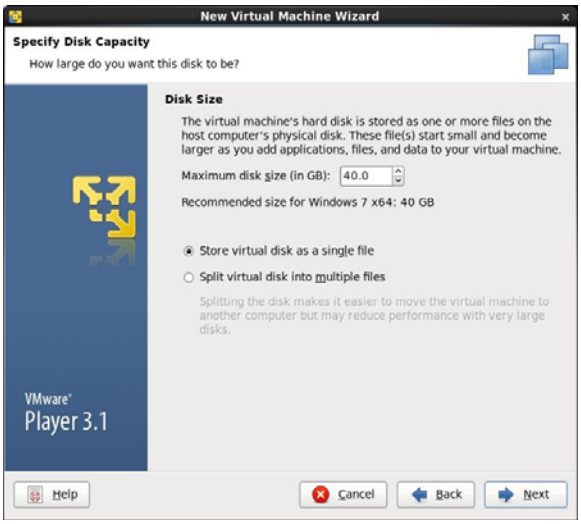


f) Nhập vào thông tin của Windows.

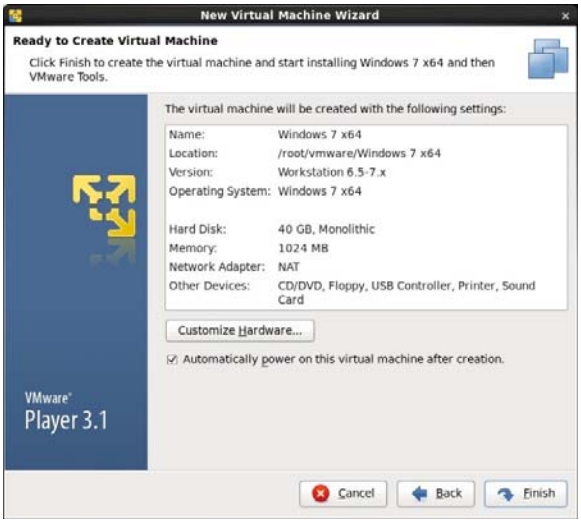


g) Nhập tên và vị trí lưu Virtual Machine.

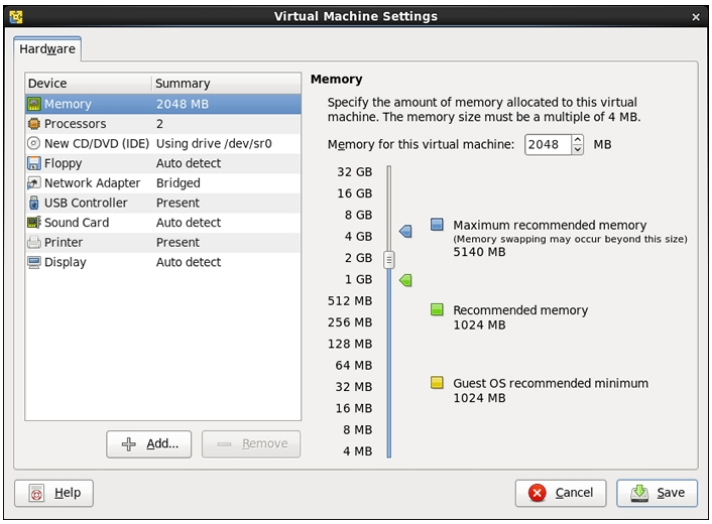
h) Chọn size ổ đĩa



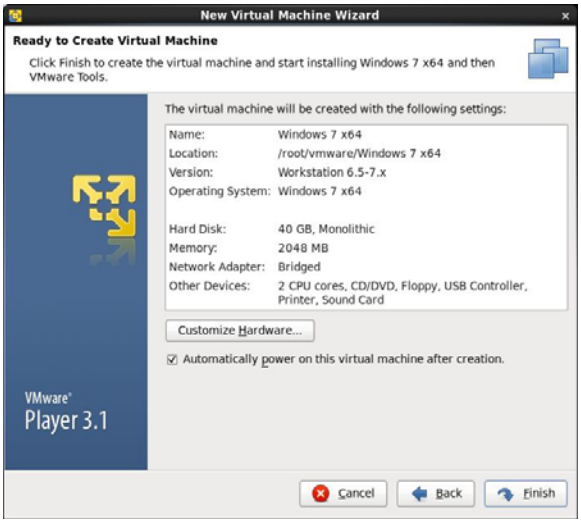
i) Click 'Cistomize Hardware'



j) Thay đổi thông tin Virtual Machine nếu cần thiết



k) Click 'Finish'



l) Khởi động Virtual Machine và tiến hành cài đặt

7.2. CÀI ĐẶT VÀ CẤU HÌNH PXE SERVER

a) Cài đặt một số phần mềm cần thiết

```
[root@pxe ~]#yum -y install syslinux xinetd tftp-server
[root@pxe ~]#mkdir /var/lib/tftpboot/pxelinux.cfg
[root@pxe ~]#cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/
```

b) Khởi động TFTP

```
[root@pxe ~]#vi /etc/xinetd.d/tftp
# line 14: chnage
disable = no

[root@pxe ~]# /etc/rc.d/init.d/xinetd start
Starting xinetd:        [  OK  ]

[root@pxe ~]#chkconfig xinetd on
```

c) Khởi động DHCP Server

```
[root@pxe ~]#vi /etc/dhcp/dhcpd.conf
option domain-name-servers    10.0.0.30;
# near line 8: add

filename    "pxelinux.0";
next-server       10.0.0.70;
```

```
# IP address of PXE Server

[root@pxe ~]#/etc/rc.d/init.d/dhcpd restart
Shutting down dhcpd:          [  OK  ]
Starting dhcpd:               [  OK  ]
```

d) Cấu hình PXE hoàn thành

7.3. CÀI ĐẶT VÀ CẤU HÌNH OPENVPN

This example shows to configure on the environment like follows. (use Bridge mode) ([172.16.2.1] is actually for private IP addtess, though, replace it to your global IP address.)

(1) VPN server	[172.16.2.1]	- Global IP address
	[10.0.0.50]	- eth0 (real IP address)
	[10.0.0.60]	- br0 - set new as a Bridge
(2) VPN Client(Windows)	[192.168.0.244]	- real IP address
	[10.0.0.??]	- automatically set from VPN Server

Bằng cách này, rất neccesary để thiết lập một vài thiết đặt trên router của bạn cho NAT\/cổng chuyển tiếp. Giao thức được sử dụng và nghe cổng mặc định trên hệ phục vụ VPN là UDP\/1194. Phát biểu vào một ví dụ ở đây, yêu cầu để 1194 với UDP từ internet là cần thiết để chuyển tiếp đến 10.0.0.60:1194 trong mạng LAN.

a) Cài đặt và cấu hình OpenVPN

```
[root@vpn ~]#yum --enablerepo=epel -y install openvpn bridge-utils

# install from EPEL
[root@vpn ~]#cp /usr/share/doc/openvpn-*/sample-config-files/server.conf
/etc/openvpn/
[root@vpn ~]#vi /etc/openvpn/server.conf
# line 53: change
dev
tap0
# line 78: change like follows
ca
/etc/openvpn/easy-rsa/keys/ca.crt
cert
/etc/openvpn/easy-rsa/keys/server.crt
key
/etc/openvpn/easy-rsa/keys/server.key
# line 87: change
dh
```

```
/etc/openvpn/easy-rsa/keys/dh1024.pem
# line 96: make it comment
#
server 10.8.0.0 255.255.255.0
# line 103: make it comment
#
ifconfig-pool-persist ipp.txt
# line 115: uncomment and chnage ( [VPN server's IP] [subnetmask] [the
range of IP for client] )
server-bridge
10.0.0.60 255.255.255.0 10.0.0.200 10.0.0.254
# line 138: add ( [network VPN server in] [subnetmask] )
push "route 10.0.0.0 255.255.255.0"
# line 275: change
status
/var/log/openvpn-status.log
# line 284: uncomment and change
log
/var/log/openvpn.log
log-append
/var/log/openvpn.log
```

b) Tạo CA certificate và CA key

```
[root@vpn ~]#cp -R /usr/share/openvpn/easy-rsa/2.0 /etc/openvpn/easy-rsa

[root@vpn ~]#cd /etc/openvpn/easy-rsa

[root@vpn easy-rsa]#mkdir keys

[root@vpn easy-rsa]#vi vars
# line 64: change to your environment

export KEY_COUNTRY="JP"
export KEY_PROVINCE="Hiroshima"
export KEY_CITY="Hiroshima"
export KEY_ORG="GTS"
export KEY_EMAIL="xxx@serverlinux"

[root@vpn easy-rsa]#source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on
/etc/openvpn/easy-rsa/keys

[root@vpn easy-rsa]# ./clean-all
```

```
[root@vpn easy-rsa]# ./build-ca
Generating a 1024 bit RSA private key
.................++++++
......++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [JP]:              # Enter
State or Province Name (full name) [Hiroshima]: # Enter
Locality Name (eg, city) [Hiroshima]:           # Enter
Organization Name (eg, company) [GTS]:          # Enter
Organizational Unit Name (eg, section) []:      # Enter
Common Name (eg, your name or your server's hostname) [GTS CA]:
vpn.serverlinux               # input FQDN
Name []:server-ca             # set
Email Address [xxx@serverlinux]:                # Enter
```

c) **ca.crt được tạo tại** "/etc/openvpn/easy-rsa/keys", transfer it to your client PC via FTP or SFTP

d) Tạo certificate và key cho server.

```
[root@vpn easy-rsa]#./build-key-server server
Generating a 1024 bit RSA private key
........++++++
.......++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [JP]:        # Enter
```

```
State or Province Name (full name) [Hiroshima]: # Enter
Locality Name (eg, city) [Hiroshima]:           # Enter
Organization Name (eg, company) [GTS]:          # Enter
Organizational Unit Name (eg, section) []:      # Enter
Common Name (eg, your name or your server's hostname) [server]:
vpn.serverlinux   # input FQDN
Name []:server    # set
Email Address [xxx@serverlinux.vn]: # Enter
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'JP'
stateOrProvinceName     :PRINTABLE:'Hiroshima'
localityName            :PRINTABLE:'Hiroshima'
organizationName        :PRINTABLE:'GTS'
commonName              :PRINTABLE:'vpn.serverlinux'
name                    :PRINTABLE:'server'
emailAddress            :IA5STRING:'xxx@serverlinux'
Certificate is to be certified until Jul 12 09:30:07 2021 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

e) Đặt tham số Diffie Hellman (DH)

```
[root@vpn easy-rsa]# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
```

f) Tạo certificate và key cho client

```
[root@vpn easy-rsa]#./build-key-pass client
Generating a 1024 bit RSA private key
..................++++++
..................++++++
writing new private key to 'client.key'
Enter PEM pass phrase:              # set pass-phrase
Verifying - Enter PEM pass phrase:  # confirm
```

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [JP]:              # Enter
State or Province Name (full name) [Hiroshima]: # Enter
Locality Name (eg, city) [Hiroshima]:           # Enter
Organization Name (eg, company) [GTS]:          # Enter
Organizational Unit Name (eg, section) []:      # Enter
Common Name (eg, your name or your server's hostname)
[client]:vpn.serverlinux                        # input FQDN
Name []:client          # set
Email Address [xxx@serverlinux]:    # Enter
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'JP'
stateOrProvinceName     :PRINTABLE:'Hiroshima'
localityName            :PRINTABLE:'Hiroshima'
organizationName        :PRINTABLE:'GTS'
commonName              :PRINTABLE:'vpn.serverlinux'
name                    :PRINTABLE:'client'
emailAddress            :IA5STRING:'xxx@serverlinux'
Certificate is to be certified until Jul 12 09:31:14 2021 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

g) **client.crt và client.key được tạo tại thư mục** "/etc/openvpn/easy-rsa/keys", chuyển chúng đến client thông qua FTP hoặc SFTP

h) Khởi động OpenVPN

```
[root@vpn ~]#cp /usr/share/doc/openvpn-*/sample-scripts/bridge-stop
/etc/openvpn/

[root@vpn ~]#cp /usr/share/doc/openvpn-*/sample-scripts/bridge-start
/etc/openvpn/

[root@vpn ~]#chmod 755 /etc/openvpn/bridge-start

[root@vpn ~]#chmod 755 /etc/openvpn/bridge-stop

[root@vpn ~]#vi /etc/openvpn/bridge-start
# line 17-20: change
eth="eth0"              # chnage if needed

eth_ip="10.0.0.60"      # IP address for bridge
eth_netmask="255.255.255.0"   # subnetmask
eth_broadcast="10.0.0.255"    # broadcast address
[root@vpn ~]#vi /etc/rc.d/init.d/openvpn
start)
echo -n $"Starting openvpn: "
# line 126: add
/etc/openvpn/bridge-start
# line 205: add
/etc/openvpn/bridge-stop
   success; echo
   rm -f $lock
[root@vpn ~]#/etc/rc.d/init.d/openvpn start
Starting openvpn: tun: Universal TUN/TAP device driver, 1.6
tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
Fri Jul 15 18:33:02 2011 TUN/TAP device tap0 opened
Fri Jul 15 18:33:02 2011 Persist state set to: ON
Bridge firewalling registered
device eth1 entered promiscuous mode
device tap0 entered promiscuous mode
br0: port 2(tap0) entering learning state
br0: port 1(eth1) entering learning state       [ OK ]
[root@vpn ~]#chkconfig openvpn on
```

7.4. CẤU HÌNH RAID 1

a) Tạo Partition RAID trong đĩa cứng . Kiểu của partition RAID là "fd". Sau khi tạo partion RAID, tiến hành kiểm tra trạng thái của nó như sau.

```
[root@linux ~]#sfdisk -l /dev/sdb
Disk /dev/sdb: 20886 cylinders, 255 heads, 63 sectors/track
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0
Device  Boot      Start End   #cyls       #blocks     Id    System
/dev/sdb1         0+    20885 20886-      167766763+  fd    Linux raid
autodetect

/dev/sdb2         0     -     0           0           0     Empty

/dev/sdb3         0     -     0           0           0     Empty

/dev/sdb4         0     -     0           0           0     Empty
```

b) Cấu hình RAID 1

```
[root@linux ~]#mdadm --create /dev/md0 --level=raid1 --raid-devices=2
/dev/sdb1 /dev/sdc1
mdadm: Note: this array has metadata at the start and
    may not be suitable as a boot device. If you plan to
    store '/boot' on this device please ensure that
    your boot-loader understands md/v1.x metadata, or use
    --metadata=0.90
Continue creating array?y

mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
```

```
[root@linux ~]#vi /etc/mdadm.conf
# mdadm.conf written out by anaconda
MAILADDR root
AUTO +imsm +1.x -all
# add

DEVICE /dev/sd[a-z]*
ARRAY /dev/md0 level=raid1 devices=/dev/sdb1,/dev/sdc1
```

```
[root@linux ~]#cat /proc/mdstat
# show status ( it's OK if it shows "[UU]" )
```

```
Personalities : [raid1]
md0 : active raid1 sdc1[1] sdb1[0]
    104855127 blocks super 1.2 [2/2] [UU]
    [==========>.........] resync = 50.1% (52600064/104855127)
finish=4.2min speed=206060K/sec
unused devices: <none>
# after few minutes later, syncronizeing will complete and the status turns
like follows
```

```
[root@linux ~]#cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdc1[1] sdb1[0]
    104855127 blocks super 1.2 [2/2] [UU]
unused devices: <none>
```

c) Cấu hình hoàn thành RAID sau đó mount /home vào nó

```
[root@linux ~]#pvcreate /dev/md0
  Physical volume "/dev/md0" successfully created

[root@linux ~]#vgcreate vg_home /dev/md0
  Volume group "vg_home" successfully created

[root@linux ~]#lvcreate -L 50G -n lv_home vg_home
  Logical volume "lv_home" created

[root@linux ~]#mkfs -t ext4 /dev/vg_home/lv_home

[root@linux ~]#mount /dev/vg_home/lv_home /mnt

[root@linux ~]#cp -pR /home/* /mnt/

[root@linux ~]#umount /mnt

[root@linux ~]#mount /dev/vg_home/lv_home /home

[root@linux ~]#df -h
Filesystem        1M-blocks   Used  Available   Use%  Mounted on
/dev/mapper/vg_dlp-lv_root
                  20G         6.9G  12G         37%   /
tmpfs             3.9G        0     3.9G        0%    /dev/shm
/dev/sda1         485M        34M   426M        8%    /boot
/dev/mapper/vg_home-lv_home
```

```
                  50G         182M  47G         1%    /home
[root@linux ~]#vi /etc/fstab
# add RAID ARRAY
/dev/mapper/vg_home-lv_home   /home ext4  defaults    1 2
```

d) Khởi động mdmonitor để điều khiển RAID ARRAY

```
[root@linux ~]#/etc/rc.d/init.d/mdmonitor start

Starting mdmonitor:                 [ OK ]

[root@linux ~]#chkconfig mdmonitor on
```

e) Nếu ổ cứng RAID ARRAY bị Failure, có thể re-configure RAID 1 giống như sau

```
[root@linux ~]#cat /proc/mdstat
Personalities : [raid1]
md0 : active (auto-read-only) raid1 sdb1[0]
    104855127 blocks super 1.2 [2/1] [U_]
unused devices: <none>
# change to new disk and create a raidautodetect partition on it again
# next, do like follows

[root@linux ~]#mdadm --manage /dev/md0 --add /dev/sdc1
# add new partition in RAID ARRAY
mdadm: added /dev/sdc1

[root@linux ~]#cat /proc/mdstat
# syncronizing starts
Personalities : [raid1]
md0 : active raid1 sdc1[2] sdb1[0]
    104855127 blocks super 1.2 [2/1] [U_]
    [>.....................] recovery = 4.9% (5200000/104855127)
finish=7.9min speed=208000K/sec
unused devices: <none>
# after few minutes later, syncronizeing will complete and the status turns
like follows

[root@linux ~]#cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdc1[2] sdb1[0]
    104855127 blocks super 1.2 [2/2] [UU]
unused devices: <none>
```

7.5. CẤU HÌNH TRUY CẬP TCP WRAPPER

a) Cài đặt TCP Wrapper

```
[root@linux ~]#yum -y install tcp_wrappers
```

b) Kiểm tra hoạt động của wrap

```
[root@linux ~]#ldd /usr/sbin/sshd | grep wrap
    libwrap.so.0 => /lib64/libwrap.so.0 (0x00007f01b4e2a000)
```

c) Cấu hình điều khiển TCP Wrapper trong '/etc/hosts.allow' và '/etc/hosts.deny' với truy cập sshd từ 10.0.0.0/24.

```
[root@linux ~]#vi /etc/hosts.deny
sshd: ALL
[root@linux ~]#vi /etc/hosts.allow
sshd: 10.0.0.
```

d) Ví dụ truy cập vsftpd từ 'host.example.domain'.

```
[root@linux ~]#vi /etc/hosts.deny
vsftpd: ALL
[root@linux ~]#vi /etc/hosts.allow
vsftpd: host.example.domain

[5]   For the case to allow access to all services that can be under TCP
Wrapper control only from 'example.domain' and '10.0.1.0/24'.

[root@linux ~]#vi /etc/hosts.deny
ALL: ALL
[root@linux ~]#vi /etc/hosts.allow
ALL: .example.domain 10.0.1.
```

CÂU HỎI ÔN TẬP