



RHCE

RH302 Study Guide

On

Redhat Enterprise Linux 5

Version 3.1

Leading The Way

in IT Testing And Certification Tools

www.testking.com

Linux is the most widely using Operating as well as raising in the market due to it's feature of open source development model, Unix like Operating System, Secure and Stable. There are lots of Linux Distributor like RedHat, SuSe, Caldera, Mandrek etc. Among them Redhat is the Premier among all the distributor. So, Redhat Saying Leader of Open source.

About Redhat Enterprise Linux 5

Redhat Enterprise Linux is more than just the operating System. It includes the wide variety of commands, applications and utilities. Some new features are added on RedHat Enterprise Linux 5: like SELinux (Security Enhanced Linux), LVM (Logical Volume Manager) Version 2, Mdadm Raid Tools, 2.6.X Version Kernel as well as more performance on Kernel and X Window System.

Redhat also provides the top Level Training and Certification on Linux. When I'm writing this book, Redhat has four Certifications.

- RHCT (Redhat Certified Technician): Which is called the entry level on Redhat Certification, which covers the system Administration level.
- RHCE (Redhat Certified Engineer): Which covers the most of the Network and Security Configuration.
- RHCA (Redhat Certified Architect):
- RHCSS (Redhat Certified Security Specialist)

RH302

Till now all Redhat's Certification is Practical Based exam, so it unique and most challenging then other certifications in the world. That's why it's a professional's choice on number one survey taken by www.certcities.com. To be familiar on Redhat Exam RHCT you can go through the TestKing RH202 Questions and Answers.

Under Red Hat Enterprise Linux 5, the certification exam consists of two parts conducted in a single day. The exam is performance-based, meaning that candidates must perform tasks on a live system, rather than answering questions about how one might perform

- Section I: Troubleshooting and System Maintenance (2.5 hours)
- Section II: Installation and Configuration (3 hours)

In order to pass the Red Hat Certified Engineer exam under Red Hat Enterprise Linux 5, you must meet all of the following requirements:

- a score of 80 or higher on Section I, consisting of five compulsory and five
- successful completion of the five Section I compulsory troubleshooting problems within one hour of that section's start time;
- 70 percent or more on the RHCT-level skills in Section II;
- 70 percent or more on the RHCE-level skills in Section II.

These last two requirements enable RHCEs to demonstrate that they possess both RHCT level and RHCE-level skills, as well as enabling a person who only has RHCT level skills to earn RHCT if they pass the required competencies.

Before Attending to Exam: Are you excellent on following? Can you do independently?

Components of the RHCT exams

The RHCT exam is a subset of the RHCE exam, and is organized as follows:

- Troubleshooting and System Maintenance – 1 hour
- Installation and Configuration – 2 hours

In order to earn RHCT, one must successfully complete all the requirements in Troubleshooting and System Maintenance, and must achieve a score of 70 or higher on Installation and Configuration section.

RHCT skills

Troubleshooting and System Maintenance

RHCTs should be able to:

- boot systems into different run levels for troubleshooting and system maintenance
- diagnose and correct misconfigured networking
- diagnose and correct hostname resolution problems

- configure the X Window System and a desktop environment
- add new partitions, filesystems, and swap to existing systems
- use standard command-line tools to analyze problems and configure system

Installation and Configuration

RHCTs must be able to:

- perform network OS installation
- implement a custom partitioning scheme
- configure printing
- configure the scheduling of tasks using cron and at
- attach system to a network directory service, such as NIS or LDAP
- configure autofs
- add and manage users, groups, and quotas
- configure filesystem permissions for collaboration
- install and update RPMs
- properly update the kernel RPM
- modify the system bootloader
- implement software RAID at install-time and run-time
- use /proc/sys and sysctl to modify and set kernel run-time parameters

Components of the RHCE exams

For RHCE exams given on Red Hat Enterprise Linux 3 and higher, the exam is organized as follows:

RH302

- Troubleshooting and System Maintenance – 2.5 hours
- Installation and Configuration – 3.0 hours

In order to earn RHCE, one must successfully complete all the RHCT-level

Troubleshooting and System Maintenance requirements, and successfully complete

enough additional RHCE items to earn a score of 80 or higher overall on the section.

In addition, one must score 70 or higher on the RHCT items of Installation and

Configuration, and 70 or higher on the RHCE components of that section.

RHCE skills

Troubleshooting and System Maintenance

RHCEs must demonstrate the RHCT skills listed above, and should be able to:

- use the rescue environment provided by first installation CD
- diagnose and correct boot failures arising from bootloader, module, and filesystem errors
- diagnose and correct problems with network services (see Installation and Configuration below for a list of these services)
- add, remove, and resize logical volumes

Installation and Configuration

RHCE must demonstrate the RHCT-level skills listed above, and they must be capable of configuring the following network services:

- HTTP/HTTPS
- SMB
- NFS
- FTP
- Web proxy
- SMTP
- IMAP, IMAPS, and POP3
- SSH
- DNS

For each of these services, RHCEs must be able to:

- install the packages needed to provide the service
- configure the service to start when the system is booted
- configure the service for basic operation
- Configure host-based and user-based security for the service

RHCEs must also be able to:

- configure hands-free installation using Kickstart
- implement logical volumes at install-time
- use PAM to implement user-level restrictions

Getting Red Hat Enterprise Linux 5

The Red Hat exams are based on your knowledge of Red Hat Enterprise Linux 5. When you take the RHCT exam, it is the

RH302

standard PC of intel compatible with better Pentium and at least 256MB RAM.

There are four Edition of RedHat Enterprise Linux are available on Market. They will charge according to your hardware profile, number of system required support from Redhat etc.

- RHEL 4 Advanced Server (AS) : Design to those organization having large network.
- RHEL 4 Enterprise Server (ES) : Design to those organization having middle level of Network
- RHEL 4 Workstation (WS): Client of AS and ES Server.
- Redhat Desktop: Stand alone clients from Redhat, Which provides the most used applications.

How to Prepare for the Exam?

On Every Section I wrote that you should able to do independently, read all carefully do practice more and go through also TestKing Questions and Answer of RH202 which is RHCT exam code.

Section 1

Redhat Enterprise Linux 5 Foundation

Can you do independently ?

- *Linux Filesystem Hierarchy*
- *Identifying the file type*
- *Working with Simple Linux Command i.e cp, mv, rm, mkdir, rmdir etc*
- *Exploring commands using man, info etc*
- *Working with Vi Editor*
- *Working with Removable Device*
- *File Compression, archiving*
- *Variables, functions, aliases etc*
- *Printing the Documents*
- *Finding files and directories*
- *String Processing with head, tail, sort, grep, wc, cut etc*

The Linux File system Hierarchy

<code>/</code>	The root Filesystem also called the top level directory in Linux
<code>/boot</code>	The <code>/boot</code> Directory contains the Kernel and all boot related Files
<code>/bin, /usr/bin</code>	All User commands

Leading the way in IT testing and certification tools, www.testking.com

/sbin, /usr/sbin	Administrative Commands
/etc	Most configuration files.
/var	Also called the Variables, contains the Most Log files, Spooling files etc.
/home	Most user's home directory
/lib	Contains the Shared libraries used by kernel as well as different programs.
/media	Typical Mount Point for Removable Devices ie CDROM, Floppy and USB Flash Disks
/mnt	Mount Point for NFS (Network File Services), SAMBA etc
/dev	All Block Device as well as Character Device files
/proc	Virtual File system contains the information about the Running Kernel.
/selinux	Like /proc Virtual File system, contains the SELinux configuration information.
/root	Home Directory of root (also called the Super User) user.
/tmp	Contains the Temporary files/directories.
/opt	Directory for Third party Products.

Each Directory Mount to different Partition except some directory. Some directory should include with / means you can't create different partition and mount.

Example: /, /lib, /bin, /sbin, /etc, /dev These Directories can't separate from the /.

Working With Linux Command:

Leading the way in IT testing and certification tools, www.testking.com

ls : List the contents of Directory

Syntax: *ls [options] path*

- l → Long Listing
- r → In reverse Order
- s → With Size
- R → With Sub-contents
- a → Normal as well as hidden contents

Example: **ls -a** : it list all hidden as well as normal contents of current directory.

ls -l /etc/ : It list all contents of /etc with long listing.

When you use the **ls -l** command you can see the long listing. i.e

```
-rw-r-xr-x 1 root root 1234 10:25:20 1 April 2006  
narayan.txt
```

First Column contains total 10 characters, Among then first Character represents the Nature of file.

- → Normal File can read using cat command.
- d → Direcotry
- l → Link File

c → Character Device File

d → Block Device File

p → Named Pipe

s → Socket

2,3,4 character represents the permission to owner user.

r → Read

w → Write

x → Execute

Always rwx comes in order if you get - in order that means no permission.

5,6,7 character represents the permission to owner group member

8, 9, 10 character represents the permission to other (neither owner user nor member of owner group).

Permission and file type	Owner User	Owner Group	Size in bytes	Created Date and Time	File Name
-rw-r-xr-x 1	Root	Root	1234	10:25:20 1 April 2006	narayan.txt

cd : Change the Directory.

cd directory → To use the directory

cd .. → To jump to parent directory

cp: Copy Command

Syntax: cp [options] source destination

-i → Interactive

-R → Recursive Copy

-F → Forcely Copy

mv : Move Command

Syntax: mv source destination

mkdir : Create the new directory

Syntax: mkdir directoryname

rmdir: removes the blank directory

Syntax: rmdir directoryname

rm : Removes files as well as directories

Syntax: rm [options] file/directory

-i → Interactive

-f → Forcely

-R → Recursively

cat : Multiple purpose command to read or create the file

cat filename: displays the contents of file on standard output.

cat >filename: Redirects the contents of standard input into file.

cat >>filename: Append the contents of standard input into file.

touch: Creates the blank file.

Example: touch filename

tty: Displays the terminal name

runlevel: Displays the current and previous runlevel

clear: Clears the screen

Exploring with Manual

- man command
- info command
- command --help

Working With Vi Editor

- Vi (Visual Editor) is the Standard Unix as well as Linux Editor.
- Redhat added some features on vi called vim (vi improved) automatically invoked when you open the vi editor.

To Start vi:

- vi

or

- vi filename

Cursor Movements on vi Editor

Shortcuts	Description
H	Moves cursor to Left
J	Moves cursor to Down
K	Moves cursor to Up
L	Moves cursor to right
W	Moves cursor one word ahead
B	Moves cursor one work back
(Moves cursor to one sentence back
)	Moves cursor to one sentence forward
{	Moves cursor to one paragraph above
}	Moves cursor to one paragraph below

- Arrow Keys also supported,
- To change the mode use esc key

Inserting and Append Mode

Shortcuts	Description
A	Append after the Current Cursor Position
I	Insert before the Current Cursor Position
O	Append new blank line below
A	Append to end of line
I	Insert at the beginning of line
O	Append new blank line above

Delete word, line and character

Shortcuts	Description
X	Deletes current Character
Nx	Deletes n characters
Dd	Deletes Current Line
Ndd	Deletes n lines
Dw	Deletes the current word
Ndw	Deletes the n words

Copy and Paste

Shortcuts	Description
-----------	-------------

Yc	Yanks current Character
Yw	Yanks Current Word
Yy	Yanks the Current Line
Nyw	Yanks the n words
Nyy	Yanks the n lines
P	Pastes the data after the current cursor
P	Pastes the data before the current cursor

- u : Undo the recent changes
- U: Undo all changes on current line since the cursor landed on the line
- . or ctrl+r : Redo

Searching the text

Shortcuts	Description
/text	Search the text in forward direction
?text	Search the text in backward direction
N	Find Next in same direction
N	Find Next in opposite direction

Save and Exit

Shortcuts	Description
:wq	Save and Exit
:w	Write into Disk

:q!	Quit without Save
-----	-------------------

www.testking.com

Working with Removable Media

Device Recognition

IDE Drive:

Primary Master /dev/hda

Primary Slave /dev/hdb

Secondary Master /dev/hdc

Secondary Slave /dev/hdd

SCSI Disk:

/dev/sda, /dev/sdb

Floppy Disk: /dev/fd0

Before using any devices you should mount the device on directory. Mounting is the process of activating the Device and creates the link on directory.

Mounting Floppy

i. mount /dev/fd0 /media/floppy

or

mount /media/floppy

Mounting CD-ROM

i. mount /dev/hd? /media/cdrom

Leading the way in IT testing and certification tools, www.testking.com

or

```
mount /media/cdrom
```

Mounting SCSI Flash Disks

In Redhat Enterprise Linux Flash Disks recognition as SCSI disk, to Use Flash Disk:

- i. `mkdir /media/flash`
- ii. `mount /dev/sda /media/flash`

File Compression and Archiving:

tar is the standard archiving tool in Redhat Enterprise Linux, which places more files/directories into a single file so easier to move, backup and store.

To create the archive file:

```
tar cvf tafilename.tar inputfiles
```

example: `tar cvf mytar.tar *` : Which creates the mytar.tar file by taking input of all files from the current directory.

`tar cvf mytar.tar file1 file2 file3` : Which creates the mytar.tar archive file of file1, file2 and file3.

To Test the archive file:

You can test the archive file by listing the all bundles files.

`tar tvf mytar.tar` : Which list all contents of mytar.tar file.

To Extract the archive files:

`tar xvf mytar.tar` : which extract the files from the mytar.tar.

File Compress and uncompress

In Linux you will get lots of tools for compress and uncompress.

- i. **gzip** is the unix standard compression tool, which compress the text files upto 75%. When you compress the file with gzip, you will get the file with .gz extension and you should uncompress using **gunzip** command.
- ii. **bzip2** is the newer linux standard compression tool. When you compress file using **bzip2**, you will get the file with .bz2 extension and you should uncompress using **bunzip2** command.

Variables, Functions and Aliases

Variable: Named Memory Location, containing the values. In Linux System, you will get the two types of variable, one is called shell variable and another is environmental variable.

Shell Variable: Shell Variable available only on particular shell means not available to other shell. You can use the **set** command to display all environmental as well as shell variables.

Environmental Variable: Environmental variable available to all shell. You can use the **env** command to display all environmental variables.

You can declare the variable just by assigning a value into the variable.

```
EMPLOYEE_NAME="ram"
```

You can print the value of variable : `echo $EMPLOYEE_NAME`

Function: Function is a collection of similar statements. You can create the function to execute a series of command.

Creating function in command line

Syntax: `functionname()`

```
{
```

```
command 1
```

```
command 2
```

```
command 3
```

```
}
```

To execute function just call the function by function name : functionname

Aliases: Aliases is called the shortcut of other command.

Example:

```
alias mytar="tar cvf mytar.tar *"
```

use the **alias** command to display all aliases declared in your system and use the **unalias** to clear the shortcut.

Example: unalias mytar

Printing the Documents:

You have just created the document ! it's time to print. The printing system in Redhat Enterprise Linux is very simple and flexible. Printers may be parallel, USB or networked. Support is included for printing to remote CUPS IPP, lpd etc.

You can install the either local or networked printer using **system-config-printer** command

lpr: this command sends the printing job to printer

Example:

lpr filename : It will sends the printing job to default printer

lpr -Pprintername filename : It will sends the printing job to specified printer

lpr -Pprintername -#5 filename: It will sends the printing job to specified printer with 5 copies.

lpq: This command is used to print the queue of printer.

Example:

lpq -Pprintername

lprm: This command helps to remove the queue from the printer.

Example:

lprm printqueueid

www.testking.com

Finding Files and Directories

i. locate or slocate command

much faster but less accurate command to search files or directories. It search in it's database, which is updated by cron daily schedule. If you want to update the database use the **updatebd** command. It will search only on directory having read and execute permission.

Example: locate test

ii. Find command

Now you can work with the most accurate command for search.

Syntax: find [path] [condition] [action]

Example:

1. find /etc -name passwd : it will find the file having name passwd in /etc directory.
2. find /home -user user1 : it will find the files and directories owned by user user1.
3. find /home -group training : it will find the files and directories owned by training group.
4. find / -atime +10 : it will find all files accessed more than 10 days ago. You know that index table contains meta information of files with different timestamp i.e Access Time, Modified Time and Change Time. You can use the atime, mtime and ctime options.

5. `find / -type f` : it will find all normal files, instead of `f` you can use the `b` for block device file, `d` for directory, `c` for character device file, `l` for link file.

on the result of `find` command you can use the different action like, copy, delete, compress, archive etc.

See by example:

i. `find /tmp -type f -exec rm {} \;` : It will search all normal files in `/tmp` and remove all files.

ii. `find /data -size +100M -exec gzip {} \;` : It will search all files having size more than 100M and compress by `gzip` command.

Introduction to String Processing Tools

head : display some lines from the top of file by default 10 lines. You can use the `-n` or `--lines` option to display custom number of lines.

Example:

```
head /etc/passwd
```

```
head -n 5 /etc/passwd
```

tail: display some lines from the bottom of file by default it displays 10 lines. You can use `-n` or `--lines` option to display custom number of lines.

Example:

```
tail /etc/passwd
```

```
tail -n 20 /etc/passwd
```

sort : sorts the text of file in ascending or descending order. By default it displays in ascending order and doesn't make any changes to original file.

Syntax: `sort [options] file`

`-r` : Reverse Order

`-n`: Numeric sort

`-f` : Ignore case

- u : Unique Sort
- t : Field Separator
- k: Field Number

Example: `sort -r -n -t: -k3 /etc/passwd`

Cut: display some specific column from the file. Like if you want to display only certain column data from file then you can use the cut command.

Syntax: `cut [option] file`

- f : Specifies field number
- d: Field separator

example: `cut -f3 -d: /etc/passwd`

wc (Word Count): Prints the number of lines, words and characters of file.

Example: `wc filename`

If you want to print only number of lines or number of words or number of characters you can use the -l or -w or -c option.

grep (General Regular Expression Processor) : displays the lines in a file match a pattern. It can also process standard input.

Example: `grep root /etc/passwd`

Section 2

RedHat Certified Technician (RHCT) Preparation

Can you do independently ?

- *Server Preparation for FTP, HTTP, NFS and Kickstart Installation*
- *Redhat Enterprise Linux Installation through FTP, NFS, HTTP and Kickstart*
- *GRUB Bootloader Configuration and Installation*
- *Linux System Initialization*
- *Init and /etc/inittab*
- *Controlling Standalone and Transient Services*
- *About Virtual File System*
- *Controlling Modules*
- *Creating Partition, File system and mounting*
- *Creating Swap partition, on/off the swap space*
- */etc/fstab file configuration*
- *Mounting NFS, SMB Share*
- *Auto Mount*
- *Network Configuration*
- *IP Forwarding*
- *Controlling Routing Table*
- *DNS Client Configuration*
- *Installing, Upgrading and Removing Packages*

Leading the way in IT testing and certification tools, www.testking.com

- *Installing Kernel*
- *About User, Group and Permission*
- *Managing Users*
- *Managing Groups*
- *Setting Permissions to user, group and others*
- *About Special Permissions*
- *Working with Startup Scripts*
- *NIS Client Configuration*
- *Installing Local and Networked Printer*
- *Managing Printer through HTTP*
- *Scheduling Cron Job*
- *X Window System*
- *Troubleshooting X Window System*
- *Configuring RAID Level 0/1/5/6*
- *Troubleshooting with RAID*
- *Configuring LVM*
- *Troubleshooting with LVM*
- *Quota Implementation*
- *Troubleshooting Linux boot process*

Welcome to you in RHCT Section of this book !

Installing RedHat Enterprise Linux 5

We can install the RedHat Enterprise Linux Either from Local CD-ROM or Network based Installation. In the daily working environment we use the Network based Installation because that is easy for us.

In Network Based Installation you can choose one method from FTP or HTTP or NFS. Before Starting Installation you should prepare the server.

In exam you will not get the question of server preparation for FTP or HTTP or NFS but in your daily administration work it is necessary.

Server Preparation for FTP:

FTP (File Transfer Protocol), which is used to upload or download the files. FTP also can be a best installation method if your site is already configured or going to configure.

By default anonymous as well as real user can access the FTP server but anonymous login into /var/ftp and can access only the /var/ftp hierarchy directory. Similarly Real User login into the user's home directory.

If you are planning to give access to anonymous then you should copy all the contents of your RHEL 4 CD's content under /var/ftp hierarchy.

Go by example:

1. mkdir /var/ftp/rhel4
2. 1st CD
3. mount /media/cdrom
4. cp -rf /media/cdrom/* /var/ftp/rhel4
5. umount /media/cdrom
6. 2nd , 3rd and 4th CD

7. mount /media/cdrom
8. cp -f /media/cdrom/RedHat/RPMS/*
/var/ftp/rhel4/RedHat/RPMS
9. umount /media/cdrom
10. chkconfig vsftpd on
11. service vsftpd restart | start

Server Preparation for HTTP:

HTTP (HyperText Transfer Protocol) , another method for Network based RedHat Enterprise Linux Installation. /var/www/html is the default directory for http service. Just copy all the contents of four CDs into /var/www/html hierarchy directory.

12. mkdir /var/www/html/rhel4
 13. 1st CD
 14. mount /media/cdrom
 15. cp -rf /media/cdrom/* /var/www/html/rhel4
 16. umount /media/cdrom
 17. 2nd , 3rd and 4th CD
 18. mount /media/cdrom
 19. cp -f /media/cdrom/RedHat/RPMS/*
/var/www/html/rhel4//RedHat/RPMS
 20. umount /media/cdrom
 21. chkconfig httpd on
- service httpd restart | start

Server Preparation for NFS (Network File Services):

Linux has the same method of sharing resources as Unix. All sharing directory are listed in /etc/exports file.

```
/data *.example.com(rw,sysnc)
trusted.cracker.org(ro,sysnc) :
```

 which line shares the /data directory from the local server to all the member of example.com domain as well as trusted.cracker.org host. All member of example.com can access the shared data in read and write access mode but the trusted.cracker.org host can access only in read only mode.

For NFS based Installation, you should share the RHEL cd copied directory in /etc/exports.

Suppose I copied in /var/ftp/pub then, I have to write in /etc/exports

Example:

```
/var/ftp/rhel4 *(ro,sysnc)

#service nfs start

#service portmap restart

#chkconfig nfs on
```

Starting Installation:

Minimum Requirements for RHEL Installation:

1. Better Pentium Class CPU
2. 256 MB RAM
3. 2-6 GB Hard Disk.

Leading the way in IT testing and certification tools, www.testking.com

To start the Installation through any network based installation method in client computer, you require the Installation startup disks. That is available in 1st CD of Redhat Enterprise Linux on images folder. From RHEL4 no longer available to support on Floppy, you require the USB disks.

In images folder of 1st CD, you will get the diskboot.img image file, you need to create the image of this image file into usb disk.

Creating the image of diskboot.img:

```
dd < diskboot.img >/dev/sda?
```

Or

```
cat diskboot.img >/dev/sda?
```

If you want to start the installation in client using cd, just write the boot.iso in blank cd, using **cdrecord** command.

When you start the Installation using the boot.iso cd, you will get the boot: prompt where you will get more options. In boot prompt, type **linux askmethod** command, which will ask you to select the different installation method. Select the Language, Keyboard options, if RHEL is already installed in your system, it will ask you either fresh installation or upgrade.

Installation started using either USB disk or boot.iso CD, it will ask you the Installation method,

- i. Select FTP to install through FTP server and click on Next. It will ask for IP address assign either statically or dynamically. Dialog will ask for FTP server and Redhat Enterprise Linux Directory, Specify the Server name and directory:
Example:

In our FTP server preparation, we have copied in /var/ftp/rhel4 suppose server has IP address 192.168.0.254.

Server: 192.168.0.254

RedHat Enterprise Linux Directory: rhel4

Note: When you install as anonymously, automatically anonymous login into /var/ftp directory, so you have to write the path after default directory.

- ii. Select HTTP to install through HTTP server and click on Next. It will ask for IP Address assign either statically or dynamically. Dialog will ask for the HTTP server and Directory. Example:

In our HTTP server preparation, we have copied in /var/www/html/rhel4 suppose server has IP address 192.168.0.254.

Website name: 192.168.0.254

RedHat Enterprise Linux Directory: rhel4

Default Directory for HTTP is /var/www/html, When you use this method to install, you must specify the path of directory after default directory.

iii. Select NFS Image to install from NFS shared directory. When you click on Next it will ask for IP Address for you machine, assign either static IP or from DHCP server if DHCP server is configured.

When you click on Next after assigning IP address, it will ask for the NFS server and RedHat Enterprise Linux Directory:

In our NFS server preparation, we have copied all CD's contents in /var/ftp/rhle4 and shared that directory.

NFS Server: 192.168.0.254

RedHat Enterprise Linux Directory: /var/ftp/rhel4

In NFS based Installation, you should give the shared path for directory. In server /var/ftp/rhel4 directory is shared.

We create the multiple partitions into the single due to the performance, security, quota etc reasons. Generally

Leading the way in IT testing and certification tools, www.testking.com

RH302

RHEL 4 required only two types of partitions one is Linux native and another is swap, but as per standardization, you should create the multiple partitions. to install the RHEL with standardization, you need to create the following partitions.

/	Linux Root directory
/boot	Linux Kernel and Boot related files.
/usr	Contains the User commands and Administrative commands with sub directory
/var	Log files, spooling files, default cache directory
/home	User's Home Directory
/opt	Optional Directory for Third party Products
/tmp	Directory for Temporary files and directory
/root	root's home directory

You can't separate the following directories with /

/etc, /lib, /bin, /sbin, /dev/

After Creating the partitions, select the place for bootloader either in MBR (Master Boot Record) or in First Sector of Boot partition. MBR (Master Boot Record) is the special area in First Hard Disk, which contains the executable code to load the OS from the System.

It will ask for the Firewall and SELinux feature. In Your RHCE exam, disable the firewall and SELinux.

root called the super user in Linux system is created automatically at installation time, set the password for root user.

Select the packages require to you When you get the package selection dialog some default packages are selected, if you require other then default packages select custom packages selection option then select the packages required to you.

After Finishing the Installation, you will get the install.log, install.log.sys and anaconda-ks.cfg file in root's home directory. install.log and install.log.sys files are colled log files created at installation time and anaconda-ks.cfg is the sample kickstart configuration file.

Kickstart Installation:

In Previous I described about the different types of installation. You have to wait in more time to install only on one machine. Suppose now you have to install within 50 machines how much time will to spend !!! and another advantage is customization in Linux system at installation time.

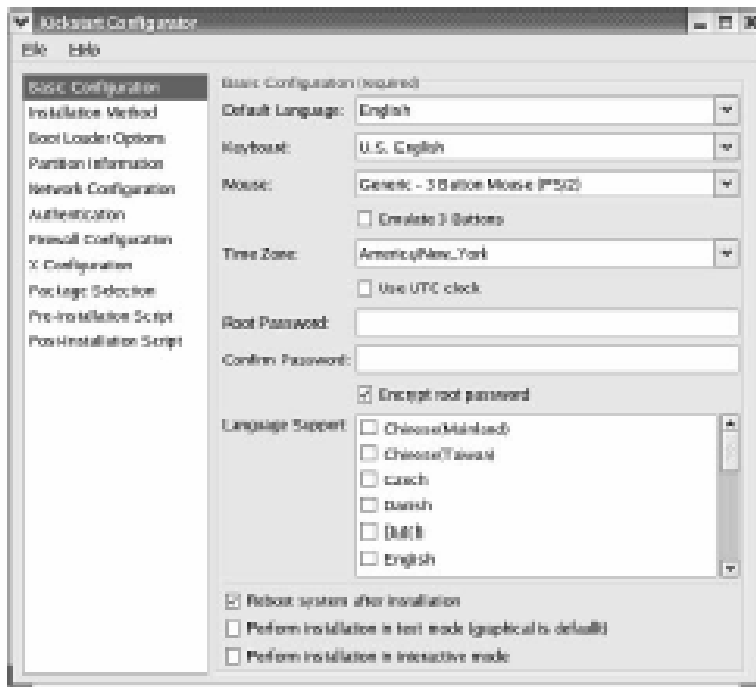
Yes Kickstart is the method, which creates the answer file to install the Linux. When you start to installation you should specify the answer file name and location. Linux will install by reading that answer file.

Preparing Kickstart Installation:

When you install Redhat Enterprise Linux, it creates the anaconda-ks.cfg file, which is called kickstart sample

file. If you can modify that file, modify as per your needs another way you have by using the GUI based kickstart installation file preparation.

```
# system-config-kickstart
```



Select options as per your needs and save into file.

Here is the sample output of Kickstart Installation file:

```
#Generated by Kickstart Configurator
#platform=x86, AMD64, or Intel EM64T

#System language
lang en_US

#Language modules to install
```

Leading the way in IT testing and certification tools, www.testking.com

```
langsupport en_US
#System keyboard
keyboard us
#System mouse
mouse
#System timezone
timezone Asia/Katmandu
#Root password
rootpw --iscrypted $1$YNZXHrUK$nIilW5J5YcibwIcjpgcDM0
#Reboot after installation
reboot
#Install OS instead of upgrade
install
#Use Web installation
url --url ftp://192.168.0.75/pub
#System bootloader configuration
bootloader --location=mbr
#Clear the Master Boot Record
zerombr yes
#Partition clearing information
clearpart --all --initlabel
#Disk partitioning information
part / --fstype ext3 --size 1000
part /boot --fstype ext3 --size 500
part /home --fstype ext3 --size 1000
part /var --fstype ext3 --size 1000
part /usr --fstype ext3 --size 6000
part swap --size 256
#System authorization information
auth --useshadow --enablemd5
```

```
#Network information
network --bootproto=dhcp --device=eth0
#Firewall configuration
firewall --disabled
#XWindows configuration information
xconfig --depth=32 --resolution=800x600 --
defaultdesktop=GNOME
#Package install information
%packages --resolvedeps
@ base-x
@ gnome-desktop
@ editors
@ graphical-internet
@ text-internet
@ office
@ server-cfg
@ web-server
@ mail-server
@ smb-server
@ dns-server
@ ftp-server
@ network-server
@ admin-tools
@ system-tools
@ printing
%post
useradd student
passwd -d student
```

There are options, package selection, Post installation and Pre-installation.

In Package selection it will list all selected packages by group name with starting @, similarly, %pre section is used to write the scripts to execute before starting the Installation and %post section is used to write the scripts to execute after installation. Suppose after installation in my class room, I want to create one user named student with blank password on each and every machine. So I wrote useradd and passwd command.

Starting Installation through Kickstart

After creating the Kickstart installation file, either copy in floppy or usb disk or copy on some directory share through NFS or make accessible through ftp or http

If you would like to start the installation through Kickstart answer file copied in Floppy Disk.

```
boot: linux ks=floppy
```

If you're booting from the Red Hat installation CD-ROM, you can still refer to a Kickstart configuration file on a floppy disk with the following command:

```
boot: linux ks=hd:fd0:/ks.cfg
```

This assumes the Kickstart configuration file is called ks.cfg and is located on the first floppy disk on your PC. Alternatively, you can refer to the Kickstart configuration file on a hard disk with this command:

```
boot: linux ks=hd:hda2:/home/mj/ks.cfg
```

This assumes the Kickstart configuration file is called ks.cfg and is located on the second partition of the first IDE drive in the /home/mj directory. The syntax of this command certainly looks strange; it's been updated for Red Hat Linux 9 and RHEL 3.

You don't need to get a Kickstart file from a DHCP server. To boot from a specific NFS or HTTP server on the network,

RH302

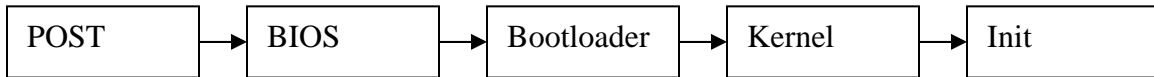
say with an IP address of 192.168.0.254, from the /kicks/ks.cfg file, type one of the following commands:

```
boot: linux ks=nfs:192.168.0.254:/kicks/ks.cfg
```

```
boot: linux ks=http:192.168.0.254:/kicks/ks.cfg
```

However, even if you've specified a static IP address in ks.cfg, this installation looks for IP address information from a DHCP server. If not found, Anaconda continues with a standard installation, not using the Kickstart file.

Linux System Initialization:



When power on the system first it perform the POST (Power on Self Test), then BIOS will initialize. BIOS initialize the devices and select the boot priority device.

BIOS executes the IPL (Initial Program Locator) to execute the Bootloader from MBR to load Operating System. In RHEL 4 GRUB (Grand Unified Boot Loader) is the standard as well as default boot loader.

/boot directory contains the kernel, Initial ramdisks file and boot loader configuration file.

/boot/grub/grub.conf is the main configuration file for grub bootloader. /boot/grub/grub.conf's Symbolic link is created in /etc/grub.conf.

GRUB is the most useful and more flexible boot loader in Linux, which support for MD5 encrypted passwords as well as provides the command prompt to modify or edit the boot loader parameter.

For more details of boot loader commands and other shortcuts see on the grub display screen. i.e c for command, e for edit and a for append.



I explain how to work with grub command prompt at boot time in troubleshooting sections.

Here is the sample configuration of grub boot loader.

default=0 : This line define to make default OS 0 means First Title will be the default OS

timeout=5 : This line define the time to load the default OS

splashimage=(hd0,0)/grub/splash.xpm.gz : This line define the path and filename of splash image. By default Splash Image is in /boot/grub/splash.xpm.gz. (hd0,0) means first partition of first hard disk.

Leading the way in IT testing and certification tools, www.testking.com

hiddenmenu : This line define whether hidden the title menu or not.

title Red Hat Enterprise Linux WS (2.6.9-5.EL) : Title of OS to display on grub menu

root (hd0,0) : Assume the boot partition as a root (/)

kernel /vmlinuz-2.6.9-5.EL ro root=LABEL=/ rhgb quiet
: Path of Kernel file, mounting the root (/) file system as a Read only mode. rhgb quiet defines whether start the X server to display progress bar at boot time or not.

initrd /initrd-2.6.9-5.EL.img : Initial RAM disk file.

To install Grub Boot loader:

grub-install /dev/hda : Which install the grub bootloader on MBR.

Protecting Boot loader and Operating System.

If anyone can access physically the system, then can go for the single user mode from the grub prompt and will change the password. Is GRUB Secure ? Noting is 100% secure, it is your responsibility to make secure the system.



Grub in Edit Mode

We can set password for passing kernel argument and another is to boot the operating system. You have choice whether want to enter plain text password or encrypted !

To encrypt the password:

```
#grub-md5-crypt
```

Enter the password, it will display the output in encrypted format. You can set either encrypted or plain text password.

```
Default=0
```

```
timeout=5
```

```
splashimage=(hd0,0)/grub/splash.xpm.gz
```

Leading the way in IT testing and certification tools, www.testking.com

```
#password=redhat : Setting plain text password for kernel arguments
```

```
password --md5 output of grub-md5-crypt :- Setting encrypted password for passing kernel argument. When user enter this password only then can modify the boot loader parameters from grub prompt at boot time.
```

```
/boot/grub/splash.xpm.gz.
```

```
hiddenmenu
```

```
title Red Hat Enterprise Linux WS (2.6.9-5.EL)
```

```
#password=redhat : Setting OS load password, when user try to load Operating System, it will ask for the password, if user will give correct then only Operating System will load.
```

```
password --md5 output of grub-md5-crypt
```

```
root (hd0,0)
```

```
kernel /vmlinuz-2.6.9-5.EL ro root=LABEL=/ rhgb quiet  
initrd /initrd-2.6.9-5.EL.img : Initial RAM disk file.
```

When you select the Operating System from Bootloader, then kernel of OS starts to boot the system. Kernel will recognize the devices connected on system, loads modules (driver) to recognize the devices or to support extra file systems.

When Kernel perform these tasks, it will hangover to the init program. Init is the most import program in Linux Operating, which perform non-TCP/IP services in Linux by reading the configuration from /etc/inittab.

Here is the sample /etc/inittab Confiuration file:

```
id:5:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
```

RH302

```
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a
# few minutes
# of power left.  Schedule a shutdown for 2 minutes from
# now.
# This does, of course, assume you have powerd installed
# and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure;
System Shutting Down"

# If power was restored before the shutdown kicked in,
# cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled"

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
```

```
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Standard Run Level in Linux

```
0 - halt
1, s , single - Single user mode
2 - Multiuser
3 - Full multiuser mode
4 - unused
5 - Multi user with GUI (Graphical User Interface).
6 - reboot
```

runlevel command displays the current and previous runlevel.

init runlevel changes the runlevel in current session.

init program reads the configuration from /etc/inittab to identify the default runlevel as well as to execute the runlevel specific scripts.

id:5:initdefault:

The above line in /etc/inittab file defines the default runlevel to boot system. If you left blank in the runlevel value, System will boot in runlevel 9 that is undefined.

RH302

If you pass the other runlevel from bootloader it will override to default runlevel specified in /etc/inittab.

Example:

Press a shortcuts in grub prompt and type the runlevel to boot the system.

```
ro root=LABEL=/ rhgb quiet s
```

When you pass `s` arguments, system will boot in single user mode.

The below lines defines the System Initialization and run level specific scripts.

```
si::sysinit:/etc/rc.d/rc.sysinit : System Initialization  
Scripts, init executes first rc.sysinit scripts to  
initialize the system.
```

```
l0:0:wait:/etc/rc.d/rc 0 : Runlevel specific Scripts for  
runlevel 0
```

```
l1:1:wait:/etc/rc.d/rc 1 : Runlevel specific Scripts for  
runlevel 1
```

```
l2:2:wait:/etc/rc.d/rc 2 : Runlevel specific Scripts for  
runlevel 2
```

```
l3:3:wait:/etc/rc.d/rc 3 : Runlevel specific Scripts for  
runlevel 3
```

RH302

14:4:wait:/etc/rc.d/rc 4 : Runlevel specific Scripts for
runlevel 4

15:5:wait:/etc/rc.d/rc 5 : Runlevel specific Scripts for
runlevel 5

16:6:wait:/etc/rc.d/rc 6 : Runlevel specific Scripts for
runlevel 6

init program reads the /etc/inittab file and provides by
default 6 terminals for Console Logins and One for GUI
Logins.

1:2345:respawn:/sbin/mingetty tty1

2:2345:respawn:/sbin/mingetty tty2

3:2345:respawn:/sbin/mingetty tty3

4:2345:respawn:/sbin/mingetty tty4

5:2345:respawn:/sbin/mingetty tty5

6:2345:respawn:/sbin/mingetty tty6

You can add more terminals in /etc/inittab file

8:2345:respawn:/sbin/mingetty tty8

After writing this line either reboot the system or use the
init q command to re-examine the /etc/inittab file.

Controlling Services:

Daemon is service runs on background and provides the system services. In Redhat Enterprise Linux two types of services are available.

- i. Standalone**
- ii. Transient or controlled by xinetd**

Standalone services are located in /etc/init.d. They can start or stop without the dependency of other services.

To check the status of services:

```
# service servicename status
```

To start the service:

```
# service servicename start
```

To restart the service:

```
#service servicename restart
```

To stop the Service

```
# service servicename stop
```

service command start or stop the service for current session. To start or stop the service automatically at next reboot, you should set on or off status using chkconfig or ntsysv or system-config-services command.

RH302

#chkconfig --list : List all services with runlevel specific on or off status.

chkconfig servicename on : Service will automatically start on reboot.

#chkconfig servicename off : Service will not start on reboot.

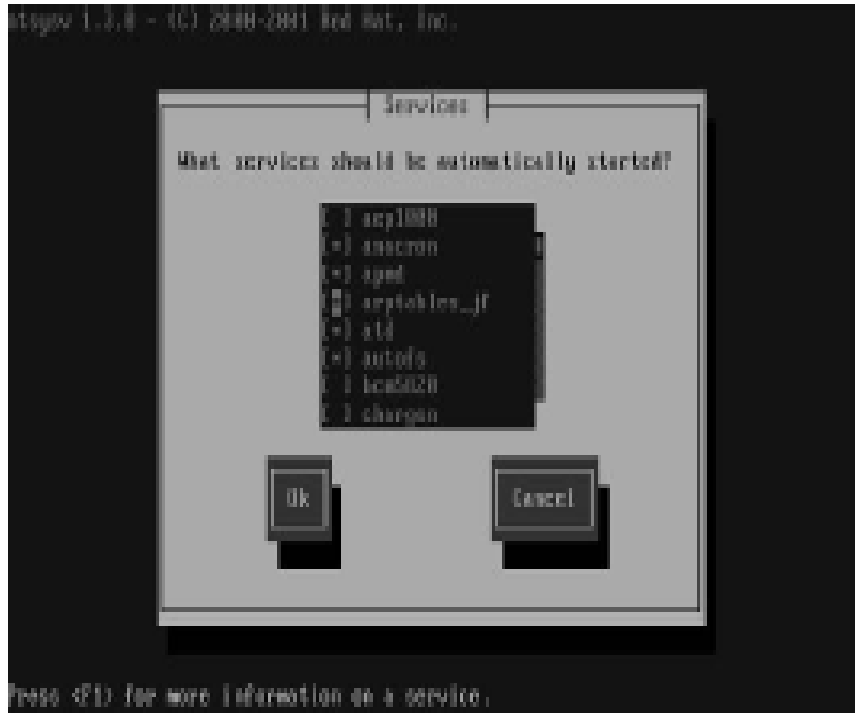
#chkconfig --add servicename : Service will add on service list

#chkconfig --del servicename : Service will delete from service list.

Another way of on or off the serve is using ntsysv tool.

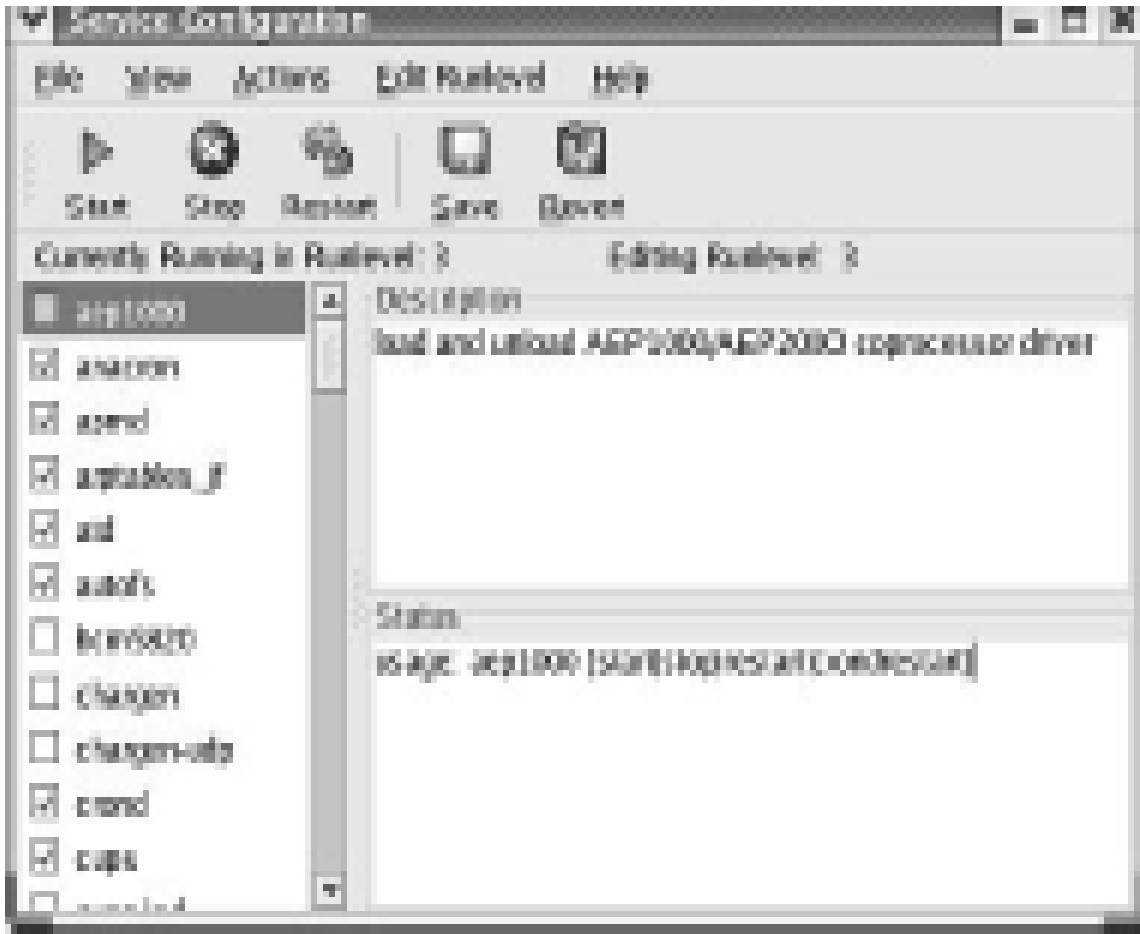
When you entered ntsysv command on console command, you will get dialog like, you can select the service, which you want start at boot time and can de-select to do not start at boot time.

Dialog of ntsysv



if you enjoy working with the GUI version tools there is a tool to manage to service named `system-config-service`, using this dialog you can start or stop or restart the service for current session. As well as on or off the service for next boot.

Dialog of system-config-service



Transient Service:

Transient service also background service controlled by xinetd super daemon. All transient daemon will reside in /etc/xinetd.d directory. Eg telnet, rlogin etc are called transient daemon.

To start or stop transient service

```
#chkconfig telnet on or off
```

To list the status of transient daemon

```
#chkconfig -list servicename
```

After changing the status of every transient services, you should restart the xinetd service.

```
#service xinetd restart
```

Virtual File System

/proc is called the virtual file system, which file system creates at boot time and clean all at shutdown time.

/proc contains lots of files and subdirectory

```
1      2039  2336  3021  buddyinfo      fs              meminfo
sys
107    2059  2349  31    bus            ide             misc
sysrq-trigger
1420   2093  2360  3130  cmdline        interrupts      modules
sysvipc
1421   21    2369  3132  cpuinfo        iomem           mounts
tty
1422   2161  2370  3164  crypto         ioports         mtrr
uptime
1423   2171  2371  32    devices        irq             net
version
1424   2183  2372  33    diskstats      kallsyms
partitions  vmstat
189    2261  2373  4     dma            kcore           pci
```

2	2271	2374	5	driver	kmsg	self
20	2281	2873	994	execdomains	loadavg	slabinfo
2007	2307	3	acpi	fb	locks	stat
2011	2326	30	asound	filesystems	mdstat	swaps

- Numbers are called Process ID running on Current Session
- cmdline : Contains the parameter passed at boot time for GRUB.
- cpuinfo : Information about CPU.
- devices : All Devices recognized by the kernel
- filesystems : Module loaded to support filesystem
- partitions : All partitions record created in your system
- mdstat : Status of Software RAID Device
- swaps : Virtual Memory (swap)
- modules : Currently Loaded modules by kernel
- ide : Information about IDE drive
- scsi : Information about SCSI drive

Enabling IP Forwarding:

Linux System can use as a Router Box. Router helps for inter-network communication. To use the Linux System as a Router, you should enable the IP Forwarding.

```
# echo "1" >/proc/sys/net/ipv4/ip_forward
```

If ip_forward's value is 1, it means enable IP Forwarding, if 0 means disable the IP Forwarding.

Modification of proc filesystem is for current boot session. When you change the value in /proc it will brings

recently changes in kernel. Means when you set the ip_forward value to 1, it will set only for current session. If you want to make automatically enable the IP Forwarding on next boot time, net.ipv4.ip_forward = 1 should set on /etc/sysctl.conf

Controlling Modules:

Linux Kernel loads the module to support hardware as well as some supplementary file system. Generally Modules are resident in /lib/modules/<Kernel Version> Directory. At boot time to recognize the device or to support the supplementary file system loads the modules.

/lib/modules/<Kernel Version>/modules.dep file contains the list of module dependencies generated by depmod command.

Command	Description
Lsmmod	List all loaded modules
modprobe	Program to add or remove modules from Linux Kernel
Depmod	Generates the module dependencies file
Modinfo	Displays the Module information
Insmmod	Program Insert the module on Kernel

Rmmod	Program remove the module from Kernel
--------------	---------------------------------------

/etc/modprobe.conf files contains the alias to module name , alias name and parameters. Which alias will create at Linux boot time. See the sample of /etc/modprobe.conf.

```
alias eth0 8139too
```

```
alias snd-card-0 snd-intel8x0
```

```
options snd-card-0 index=0
```

```
install snd-intel8x0 /sbin/modprobe --ignore-install snd-intel8x0 && /usr/sbin/alsactl restore >/dev/null 2>&1 || :
```

```
remove snd-intel8x0 { /usr/sbin/alsactl store >/dev/null 2>&1 || : ; }; /sbin/modprobe -r --ignore-remove snd-intel8x0
```

```
alias usb-controller ehci-hcd
```

```
alias usb-controller1 uhci-hcd
```

In First line of the /etc/modprobe.conf contains the alias name eth0 with module 8139too. User use the device by name eth0 (First Ethernet card device name), but it is not actually the device just alias to device modules.

Creating and Managing Partitions

We divide the Single large size disk into multiple partitions for performance, security and can implement the quotas on individual filesystem. Partitions can be either primary or Logical. Primary partitions contains the Operating System's file to load the OS and Logical partitions created under the extended partitions.

Device Conventions:

/dev/hda : Primary Master

/dev/hdb : Primary Slave

/dev/hdc : Secondary Master

/dev/hdd : Secondary Slave

Example: /dev/hda3 : Third partition of Primary Hard disk.

/dev/fd0 : Device of First Floppy Disk

/dev/sda : First SCSI Disk

You can create partition on hard disk using different tools example fdisk, sfdisk, GNU parted etc. There is limitation of creating the partitions using fdisk because you only able to create the maximum 16 partitions.

```
# fdisk -l : List All partitions created in your Linux System
```

```
# fdisk /dev/hda :Enter into the fdisk mode
```

```
[root@example ~]#  
[root@example ~]# fdisk /dev/hda  
  
The number of cylinders for this disk is set to 4982.  
There is nothing wrong with that, but this is larger than 1024,  
and could in certain setups cause problems with:  
1) software that runs at boot time (e.g., old versions of LILO)  
2) booting and partitioning software from other OSs  
   (e.g., DOS FDISK, OS/2 FDISK)  
  
Command (m for help): █
```

you can use the m shortcut to display all available options. Some important option

n : Create new Partition

d : Delete existing Partition

t: Change System ID Type

q : Quit without save

w: Write and Save

Create the partition with your desire size, System ID then save and exit from the partitions. By default partition will create having Linux Native 83 System ID. Like swap has 82 system ID, Raid partitions has fd and LVM has 83 etc. So to change the System ID as your require use the t shortcut and change.

```

[root@example ~]#
[root@example ~]# fdisk /dev/hda

The number of cylinders for this disk is set to 4982.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): n
First cylinder (1316-4982, default 1316):
Using default value 1316
Last cylinder or +size or +sizeM or +sizeK (1316-4982, default 4982): █

```

Creating Filesystem

We have mkfs or mke2fs command to create the ext2, ext3, vfat etc file system in Linux.

Syntax :

```
# mkfs -t <fstype> device
```

```
# mke2fs <options> device
```

Example: # mkfs -t ext3 /dev/hda8 Which creates the ext3 filesystem on /dev/hda8.

Mounting Filesystem:

Mount process brings the external device or other device as a hierarchy of Linux System. Before accessing any other filesystem, it must bring in Linux Filesystem tree. Mount command brings other filesystem in Linux system tree.

Syntax: # mount -t <fs type> -o options device mount point

RH302

Filesystem type can be ext2, ext3, vfat, iso9660 etc. When you mount without specifying any mount options, default options be rw, suid, exec, dev, auto, nouser and async.

Mount Options

Options	Description
rw	Mount on Read and Write mode
suid	Mount with SUID bit
exec	Can execute files on this filesystem
auto	Automount
nouser	Other user can't unmount or remount the filesystem
async	Mount on async mode
You can use other opposite mount options ro, nosuid, noexec, nodev, noauto, user and sysnc.	

Example:

```
# mount -t ext3 -o ro /dev/hda16 /data
```

```
# mount -t iso9660 -o ro /dev/hdb /media/cdrom
```

When you mount the filesystem using the mount command, it mounts only for current session only. To mount automatically at boot time, you need to write in /etc/fstab file. At boot time rc.sysinit file mounts all filesystem written in /etc/fstab.

Pattern of /etc/fstab

Leading the way in IT testing and certification tools, www.testking.com

```
Device      mountpoint      fielsystem      mountoptions    dump
frequency  fsck order
```

Example:

```
/dev/hda16    /data    ext3 defaults  0 1
```

Setting Label on device

We can set the label name on ext2/ext3 formatted filesystem using `e2label` command or at filesystem creating time using `-l` option with `mke2fs` command. One of the benefits of setting label is that no need to remember the device name to access just by label name can use the device.

```
# e2label /dev/hda16 /mydrive
```

Now mount using label Name

```
# mount -L /mydrive /data
```

or

```
# mount LABEL=/mydrive /data
```

Similarly in `/etc/fstab` also filesystem can mount using the label name.

Example:

```
LABEL=/mydrive    /data    ext3 defaults  0 0
```

Mounting Other Filesystem like NFS

Devices are locally connected on the system but you should be able to mount the NFS (Network File Services) Share on your Local System.

showmount command helps to display all shared directory from the particular system.

```
# showmount -e server
```

```
# mount -t nfs server:/path mountpoint
```

 It will mount the nfs share for the current session.

If you would like to mount the nfs share automatically at boot time there is fstab file. Which helps to mount the filesystem automatically at boot time.

Syntax of fstab file:

Device	mount point	filesystem	mounting	options
--------	-------------	------------	----------	---------

dump	frequency	fsck	order	
------	-----------	------	-------	--

Example: server1.example.com:/data /data nfs defaults
0 0 : It will mount the directory /data shared from server1.example.com into local directory /data.

Samba Client:

NFS service is used to share the resources between the Linux or Unix environment. If you Microsoft Windows and Linux, to access the resources you require the samba. Samba Client is the tool use the access the windows share in Linux.

RH302

```
# smbclient -L //windows1 -U username : List all share from windows1
```

```
# smbclient //windows1/test -U username : Connect to shared directory test to download or upload files
```

```
# smbmount -o username=user1 //windows1/test /mnt/samba : Mounts the test directory of windows1 system into samba directory in /mnt.
```

```
# smbmount /mnt/samba : Unmounts the samba mounted on /mnt/samba
```

```
# mount -t smb -o username=user1 //windows1/test /mnt/samba : Mounts the test directory of windows1 system into samba directory in /mnt.
```

```
# umount /mnt/samba : Unmount the samba mounted on /mnt/samba
```

Network Configuration

Linux System Recognize the Network devices eth0, eth1 etc for First Ethernet card, tr0, tr1 etc for Token Ring and fddi0, fddi1 etc for FDDI Interface.

To recognize all these network devices kernel loads the Modules from /lib/modules directory.

/etc/sysconfig/network file is called the global network configuration file contains global parameter for network configuration.

```
NETWORKING=yes | no
```

```
HOSTNAME=station?.example.com
```

```
GATEWAY=X.X.X.X
```

```
NISDOMAIN=example.com
```

To enable the network on you system value of NETWORKING should be yes. Some services are dependable on this parameter, which required NETWORKING=yes. There is **hostname** command, which prints or set the host name for current session but to set the host name permanently on your system, you should specify the hostname in HOSTNAME=parameter. GATEWAY parameter defines the global default gateway and last one is NISDOMAIN, which defines the domain for NIS.

/etc/sysconfig/network-scripts/ifcfg-eth? File is called the interface specific file use to configure the specific

interface. Generally interface specific file contains following parameters:

DEVICE=devicename

ONBOOT=yes | no

BOOTPROTO=static | dhcp

IPADDR=X.X.X.X

NETMASK=X.X.X.X

GATEWAY=X.X.X.X

Device parameter define the device name of configuration that is same as ifcfg-eth?. Onboot parameter defines whether bring up interface automatically at boot time or not. If you set yes, it will enable the Interface at boot time otherwise you should manually start the interface. Bootproto define the boot protocol either static or dhcp. If you use static, you should assign the IP Address, Subnet mask manually and if you set dhcp, ip address, netmask and other information will assign by DHCP server. GATEWAY is the interface specific Gateway parameter, which overrides the global gateway parameter.

#ifconfig : Command used to display the information about interface connected into the system.

ifdown eth0 : Which downs the interface

ifup eth0 : which brings up the interface

Whenever you change the configuration of /etc/sysconfig/network file, you should restart the network service. Similarly after changing the configuration of interface should down and up once.

Assigning Multiple IP Address on Interface

For Routing you can assign multiple IP Addresses on same Interface. On One Physical Interface we can assign upto 256 IP Addresses.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0:0
```

```
    IPADDR=x.x.x.x
```

```
    NETMASK=x.x.x.x
```

```
# ifdown eth0
```

```
#ifup eth0
```

If you want to assign more IP Address by range

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0-rangeX
```

```
    IPADDR_START=x.x.x.x
```

```
    IPADDR_END=x.x.x.x
```

```
    CLONENUM=x
```

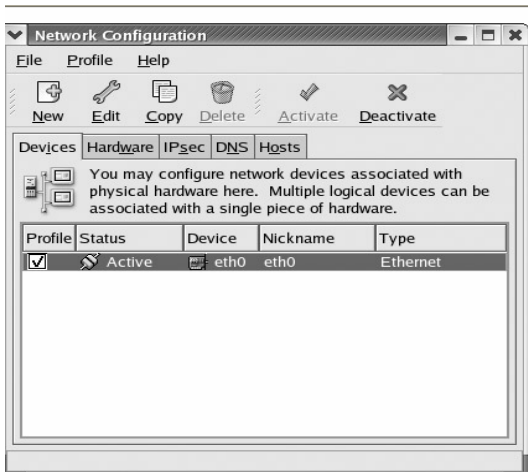
```
#ifdown eth0
```

```
#ifup eth0
```

Now, you can verify using `ifconfig` command.

There is one console based tool to configure is `netconfig`. You can assign IP Address, Netmask, Gateway and DNS server using `netconfig` tool.

If you enjoy working with Redhat's GUI Environment, there is another tools to configure Network: `system-config-network`



Working with routing Table

You can configure the routing table to distribute the routing path. If you are using the Linux as a Router box, you should maintain the routing table.

`#route -n` or `netstat -rn` command prints routing table configured in Linux System.

`# route add -net 192.168.1.0 255.255.255.0 gw server1.example.com` : Which adds in the routing table that

Leading the way in IT testing and certification tools, www.testking.com

packets for 192.168.1.0 network should go through server1.example.com.

```
# route add -net 192.168.5.0 255.255.255.0 dev eth1 :  
Packets to 192.168.5.0 network should go through eth1  
device.
```

Static Routing:

Static route set on per-interface basis . To create the static route

```
# vi /etc/sysconfig/network-scripts/eth?.route
```

```
ADDRESS0=x.x.x.x
```

```
NETMASK0=x.x.x.x
```

```
GATEWAY0=x.x.x.x
```

Address and netmask parameter represents the address of remote network and subnet mask. Gateway parameter define the path to reach on remote network.

DNS Client Configuration

DNS (Domain Name Server) Resolve Name to IP and IP to Name as well DNS defines the Mail Exchanger for the particular Domain. When user try to access by name request goes to DNS server to resolve than name to IP Address because system always works on Logical Address. So we can specify the DNS server in /etc/resolv.conf file.

Example: /etc/resolv.conf

```
nameserver x.x.x.x
```

```
nameserver x.x.x.x
```

```
# host www.abc.com host command sends request to DNS server to resolve www.abc.com and displays the IP Address associate with www.abc.com
```

```
#dig www.abc.com dig command sends requests to DNS server to resolve www.abc.com and displays the IP Address associate with www.abc.com.
```

```
#nslookup www.theexamking.com nslookup also DNS client tool, which sends the request to DNS server to resolve into IP Address.
```

Package Management

The RedHat Package Manager (RPM) provides the standard way of managing the package on Enterprise Linux. Using RedHat Package Manager, we can install, upgrade, remove the groups of applications or utilities.

Generally we need to check the integrity of package, install, upgrade, remove etc. RPM package manager maintains the local rpm database in /var/lib/rpm directory. When you sends the queries regarding the package either installed or not, installed version, all installed package, integrity of package, it will check in local database.

Querying the Package

```
#rpm -q setup
setup-2.5.27-1
```

When you query for specific package if package is installed on system it will display with package version and full name from the local RPM database.

Querying and list All Installed Package

```
# rpm -qa
```

Checking the owner package

```
[root@example ~]# rpm -qf /bin/echo
coreutils-5.2.1-31
```

To install the package:

```
# rpm -ivh packagename
```

Where i means install, v means verbose and h means display the hash mark of progress.

To Upgrade Package

```
# rpm -Uvh packagename
```

Where U means upgrade if lower version is installed else installed new copy, v and h verbose and hash mark. When you upgrade the package, configuration file of old package is renamed by adding the .rpmsave extension.

```
# rpm -Fvh packagename
```

Where F means Upgrade package if lower version is installed only, v means verbose and h means display the hash mark.

To query the information of package

```
# rpm -qi packagename
```

To List all files belongs to package

```
# rpm -ql packagename
```

When you install the package package's record will maintain in local database /var/lib/rpm. Later you can verify the size, owner, permission, MD5 sum and modify time against the RPM database.

```
# rpm -V or --verify packagename
```

Example:

```
[root@example ~]# rpm -V httpd  
S.5....T c /etc/httpd/conf/httpd.conf
```

There are some output regarding the verification. While verifying the package you can get the following characters:

S	File Size differs
M	Mode differs (includes permissions and file type)
5	MD5 sum differs
D	Device major/minor number mismatch

L	readLink(2) path mismatch
U	User ownership differs
G	Group ownership differs
T	mTime differs

When you use the Redhat distributed Redhat Enterprise Linux, Redhat signs all package file with the GPG private signature. You can get one file name RPM-GPG-KEY file containing the signature of all packages. First you should import that key into your local database then before installing any package you can verify the integrity of package.

```
# rpm --import RPM-GPG-KEY
```

```
# rpm --checksig packagename
```

RPM Dependencies Resolution

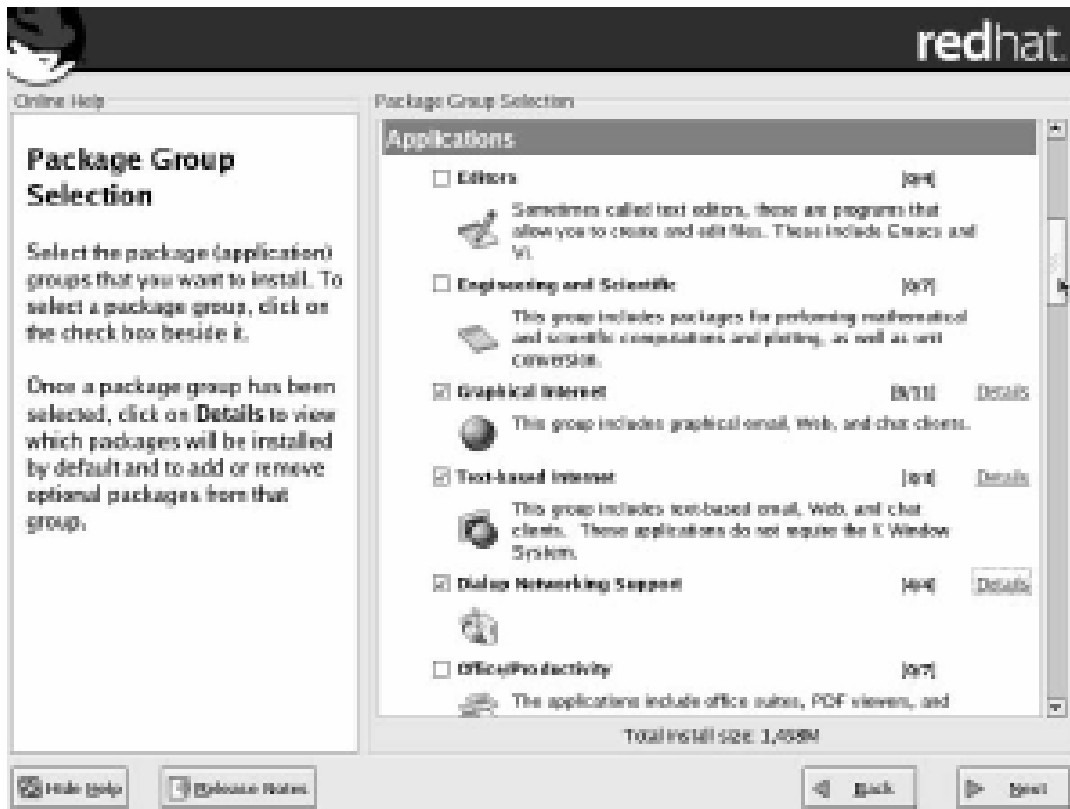
When you try to install the new package, it display the messages of dependencies. It takes long time by identifying and install the dependencies packages. There one options --aid which automatic resolv the dependencies.

```
# rpm -ivh --aid packagename
```

Installing Package using Package Management tool

There is one graphical package management tool to manage the package.

```
# system-config-packages
```



When you open this dialog it checks the backup of all package from the local cd. If you want to specify alternative location.

```
# system-config-packages --
tree=ftp://server1.example.com/pub

#system-config-packages --
tree=http://server1.example.com/rhel4

#system-config-packages --tree=/backup
```

Installing Kernel

Leading the way in IT testing and certification tools, www.testking.com

RH302

Kernel called the core of Operating System. You should able to install, uninstall the kernel provided in rpm format. You should think one caution before upgrading the kernel. When you upgrade it removes the lower version of kernel. Suppose if any hardware wouldn't support by your new kernel what will happen ?? Needs to re-install. So better in case of kernel, install new kernel, check every performance, hardware support of new kernel and remove manually old version of kernel.

```
# rpm -ivh kernel-version
```

When you install new kernel record will automatically add in boot loader configuration file.

User and Group Administration

When you login to the system needs to supply your identity to the system that is called the user. One user can belong to more groups, group is the representative name of users. /etc/passwd file is called the user database file, which maintains the record of all created users. /etc/shadow file contains the MD5 encrypted user's password.

See the example:

```
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
news:x:9:13:news:/etc/news:
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
```

Pattern of /etc/passwd file is
 loginname:password:UID:GID:comment:home directory:login
 shell

Similarly users encrypted password stores in /etc/shadow file

RH302

```
root:$1$pPOCmMEL$GpUuTtSZUcFh0QQnbrNyS0:13352:0:99999:7:::
```

```
bin:*:13345:0:99999:7:::
```

```
daemon:*:13345:0:99999:7:::
```

```
adm:*:13345:0:99999:7:::
```

```
lp:*:13345:0:99999:7:::
```

```
sync:*:13345:0:99999:7:::
```

```
shutdown:*:13345:0:99999:7:::
```

```
halt:*:13345:0:99999:7:::
```

In Redhat Enterprise Linux, when you create the user at same time group also created with the same user name. That group is called the user's private group. When you create either User or Group, systems will assign a new unique ID called User ID and Group ID. All created group information stores in /etc/group file.

```
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
```

```
tty:x:5:
```

disk:x:6:root

lp:x:7:daemon,lp

mem:x:8:

kmem:x:9:

wheel:x:10:root

mail:x:12:mail

news:x:13:news

uucp:x:14:uucp

man:x:15:

games:x:20:

gopher:x:30:

dip:x:40:

Command	Description
Id	Displays user and Group ID
Groups	Displays all belongs group name and ID
whoami	Displays Logon name
w, who , users	Displays all logged on users name
Useradd	Adds the user on System
Userdel	Deletes the user from system
groupadd	Adds the group on System
groupdel	Deletes the group from System

Passwd	Changes the password of user
---------------	------------------------------

Example:

```
# useradd user1

# passwd user1

#groupadd training

#groupdel training
```

When you create the user named user1, system adds the record in /etc/passwd file, /etc/shadow file, /etc/group file, /var/spool/mail/user1 file as well as creates the home directory. By default it creates same group name with user crates and make belongs that user primarily to that group.

Generally primary group is used to define the ownership either file/directory or process group owner will be the primary group of the user but supplementary group is used to access the resources.

In Linux Every file or directory is owned by some user or some group. As well as permission also defined to owner user, owner group member and others.

```
-rw-r--r-- 1 user1 admin 5 Jul 26 14:46 rhce
```

See second, third and fourth character represents the permission to owner user user1. Fifth, Sixth and Seventh represents permission to admin group member. Eight, nine

and tenth characters represents the permission to others. Here others means neither owner user nor owner group member these are called others.

Modifying User Accounts

usermod command helps to modify the user accounts. By default user's home directory creates in /home, password never expire, normal users user id start to assign from 500 etc. This default properties reads from /etc/default/useradd and /etc/login.defs file.

When user create in linux system, one group will create with same user name and user makes belongs to primarily to that group.

Syntax: usermod [options] username

Options	Description	Example
-s	By default bash assigns to every user in RHEL 4. using -s option is usermod command you can change the password.	usermod -s /bin/sh user1
-d	By default user's home directory creates in /home/username, using -d option can change the user's home directory.	usermod -d /rhome/user1 user1
-g	By default user belongs primarily to group created at user creating time, using -g	usermod -g training user1

	option can change the primary group of user.	
-G	Using G option we can make user belongs to more than one group to access permission	usermod -G admin user1
-L	Lock the user account	usermod -L user1
-U	Unlock the user account	usermod -U user1
-e	Set the account expire time	usermod -e date user1

Setting password policies

In RHEL 4 password is never expire by default as well as there is no any force to change the user's password. When creating user in Linux System, it reads the default configuration to assign to users from /etc/login.defs and /etc/default/useradd file. You can see on this file that password is never expire.

Here is the default Configuration of /etc/login.defs

```
# *REQUIRED*

#   Directory where mailboxes reside, _or_ name of file, relative to
the

#   home directory.   If you _do_ define both, MAIL_DIR takes
precedence.

#   QMAIL_DIR is for Qmail

#

#QMAIL_DIR      Maildir
```

RH302

```
MAIL_DIR          /var/spool/mail

#MAIL_FILE        .mail

# Password aging controls:

#

#     PASS_MAX_DAYS   Maximum number of days a password may be used.

#     PASS_MIN_DAYS   Minimum number of days allowed between password
changes.

#     PASS_MIN_LEN    Minimum acceptable password length.

#     PASS_WARN_AGE   Number of days warning given before a password
expires.

#

PASS_MAX_DAYS     99999

PASS_MIN_DAYS     0

PASS_MIN_LEN      5

PASS_WARN_AGE     7

#

# Min/max values for automatic uid selection in useradd

#

UID_MIN           500
```

RH302

```
UID_MAX                60000

#

# Min/max values for automatic gid selection in groupadd

#

GID_MIN                500

GID_MAX                60000

#

# If defined, this command is run when removing a user.

# It should remove any at/cron/print jobs etc. owned by

# the user to be removed (passed as the first argument).

#

#USERDEL_CMD           /usr/sbin/userdel_local

#

# If useradd should create home directories for users by default

# On RH systems, we do. This option is ORed with the -m flag on

# useradd command line.

#
```

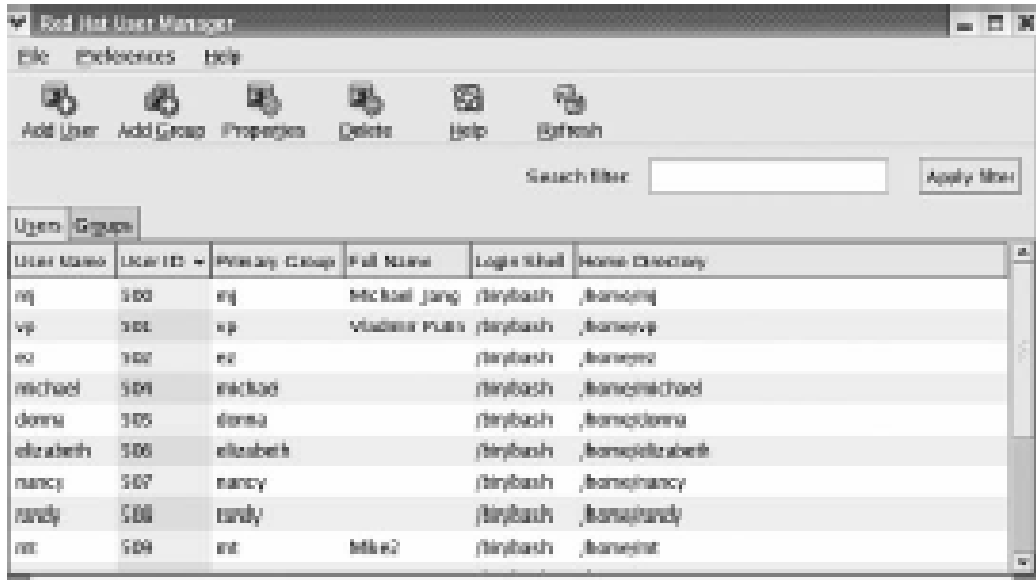
Syntax: chage [options] user

Options	Description	Example
-M	Maximum number of days a password may be used	Chage -M 20 user1
-m	Minimum number of days allowed between password changes.	Chage -m 10 user1
-W	Number of days warning given before a password expires.	Chage -W 5 user1
-I	Number of days account should be inactive before password expires.	Chage -I 2 user1

Redhat User and Group Manager

If you enjoy working with the Redhat's User and Group Manager, you can use the GUI Version of this tool to create, delete, modify the user accounts.

- Click Applications → System Settings → User and Group



Changing Ownership

Every resources are owned by one particular user as well as user's private group. Later administrator can change the ownership of file or directory using the `chown` or `chgrp` command.

Syntax: `chown [-R] user:group file/directory`

Where `-R` options is called recursive. It changes the owner of all files as well as all sub-directories.

Example: `chown -R user1:admin /data` Which changes the owner of `/data` to `user1` user and `admin` group owner.

If you would like to change the group ownership only you can use the chgrp command.

Example: chgrp admin /data : Which changes the group owner of /data to admin.

Changing Permission

Every Resources are controlled by the owner user, owner group member and others permission.

```
-rw-r--r-- 1 narayan admin 5 Jul 26 14:46 rhce
```

chmod command is used to change the permission of file or directory.

```
# chmod u+rwx /data : Which set the read, write and execute permission on /data directory to owner user.
```

```
#chmod g+rwx /data : Which set the read, write and execute permission on /data to owner group member
```

```
# chmod o-rwx /data : Which removes the read, write and execute permission to others.
```

Here + operator works to add the permission and - removes the permission. You can assign the permission by numeric method also.

Read : 4

Write : 2

Execute : 1

Total Permission is 7.

```
# chmod 770 /data : Which assigns the read, write and execute permission to owner user and all owner group member but no any permission to others.
```

```
#chmod 754 /data : Which assigns the read, write and execute permission to owner user, read and execute permission to group member and read only permission to others.
```

Special Permission:

1. SUID or SGID bit on Executable File:

Like files or directories, process also on under the some ownership. By default process start under the ownership of executer. Means who is going to execute the command, process start under the ownership or security context of that user or group.

When SUID or SGID bit is set the executable file, process starts under the security context of file owner then executer.

Example: When user1 uses the cat command, process start on user1's ownership. But when we set the SUID or SGID bit on cat command, always process start on root's ownership because root is the owner of cat command.

```
# chmod u+s file
```

```
#chmod g+s file
```

```
#chmod u-s file
```

Before setting SUID or SGID permission is like this

```
-rwxr-xr-x 1 root root 19140 Oct 5 2004 /bin/cat
```

When you set the SUID and SGID bit you will get

```
-rwsr-sr-x 1 root root 19140 Oct 5 2004 /bin/cat
```

SUID or SGID bit appear on user and group permission in place of x. If s appear small that means with execute permission. If s appear S then SUID or SGID without x permission.

2. SGID bit on directory

By default files or directory creates with ownership of user and user's primary group. When we set the SGID bit on directory, the group owner of file or sub-directory created on that directory automatically will be the group owner of parent group.

Example:

```
drwxrwx--- 3 root admin 12324 July 20 2006 12:30 data
```

In Output permission is only to owner user and to owner group member. When user1 which belongs to admin group create the file in /data owner will be user1 as well as user1's primary group.

```
# chmod g+s /data
```

When you set the SGID bit on directory, when user user1 creates the file in /data group owner will be admin.

3. Sticky Bit

When one directory can access in read, write and execute mode by more than one user, one user can remove other user's file. Sticky Bit preserve to delete by other user.

```
#chmod o+t /data
```

```
drwxrwx--T 3 root admin 12324 July 20 2006 12:30 data
```

Sticky Bit appears by t character in execute position. If t appear in small case it means with execute permission and if t appears in T then it means without execute permission.

Assigning Permission on individual User/Group basis

There is another commands setfacl and getfacl commands, which sets the permission to individual user or to individual group.

```
#getfacl filename or directory : Displays the permission assigned to users and groups.
```

```
# setfacl -m u:user10:rwX filename/directory : Which sets the read, write and execute permission to user10
```

```
# setfacl -m g:admin:rwX filename/directory: Which sets the read, write and execute permission to admin group member.
```

```
#setfacl -x u:user10 file/directory : Which removes the permission assigned to user user10
```

RH302

```
# setfacl -x g:admin file.directory
```

Remember that to assign the permission with acl filesystem should mount with acl option.

www.testking.com

NIS Client Configuration

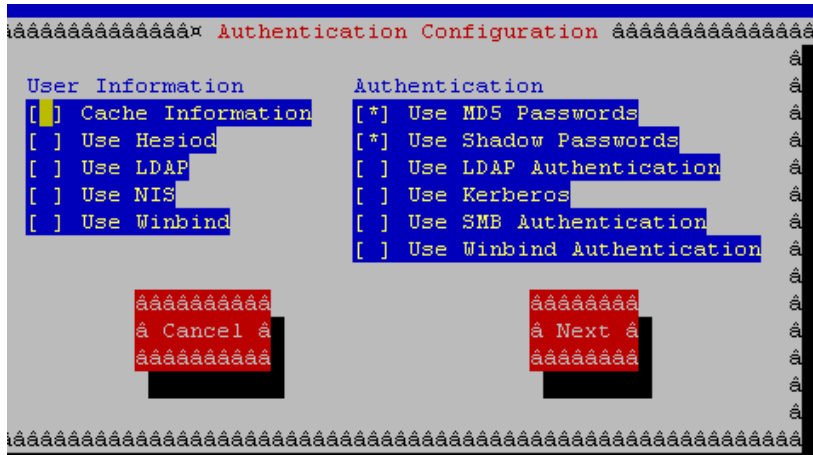
NIS (Network Information Server) is a traditional directory service, use for centralized to manage user accounts. Using NIS, you can't apply all policy for user.

NIS is a RPC (Remote Procedure Call) Service needs to run portmap service also in server. As well as NIS is not based on DNS (Domain Name Services), it is directly bind the domain name with IP Address.

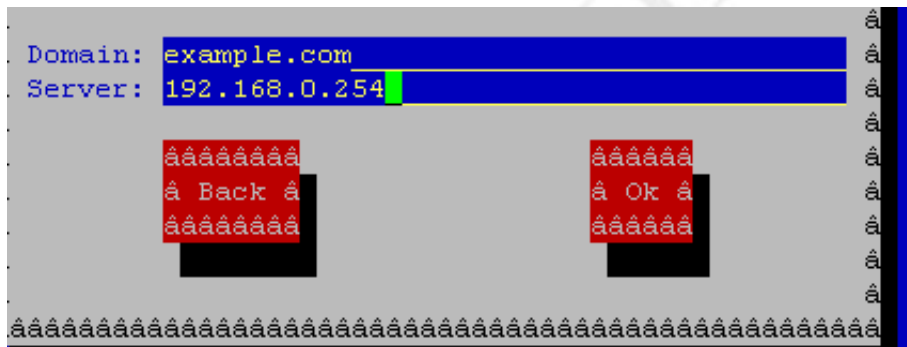
For RHCT, you should know how to configure the NIS Client in already server configured environment.

Let configure the NIS Client by taking some NIS server Information:

- i. NIS domain name is example.com
 - ii. NIS Server is 192.168.0.254
 - iii. NIS user's home directory is in /nisusers
- a. Type `authconfig` or `system-config-authentication` command



- b. Select on use NIS then click on Next
- c. Type Domain : example.com
- d. Server : 192.168.0.254



- e. Click on ok

It means users are authenticated from the NIS server 192.168.0.254. When user login on your Client machine, home directory should present in logged on system.

I already written about the Automount feature. We can mount the user's home directory in client machine to make present user's home directory.

- a. mkdir /nisusers

b. `vi /etc/auto.master`

```
/nisusers /etc/auto.home      --timeout=60
```

This line specify the mount point by reading /etc/auto.home as well as unmount the /nisusers if user doesn't use within 60 seconds.

c. `vi /etc/auto.home`

```
* -rw,soft,intr 192.168.0.254:/nisusers/&
```

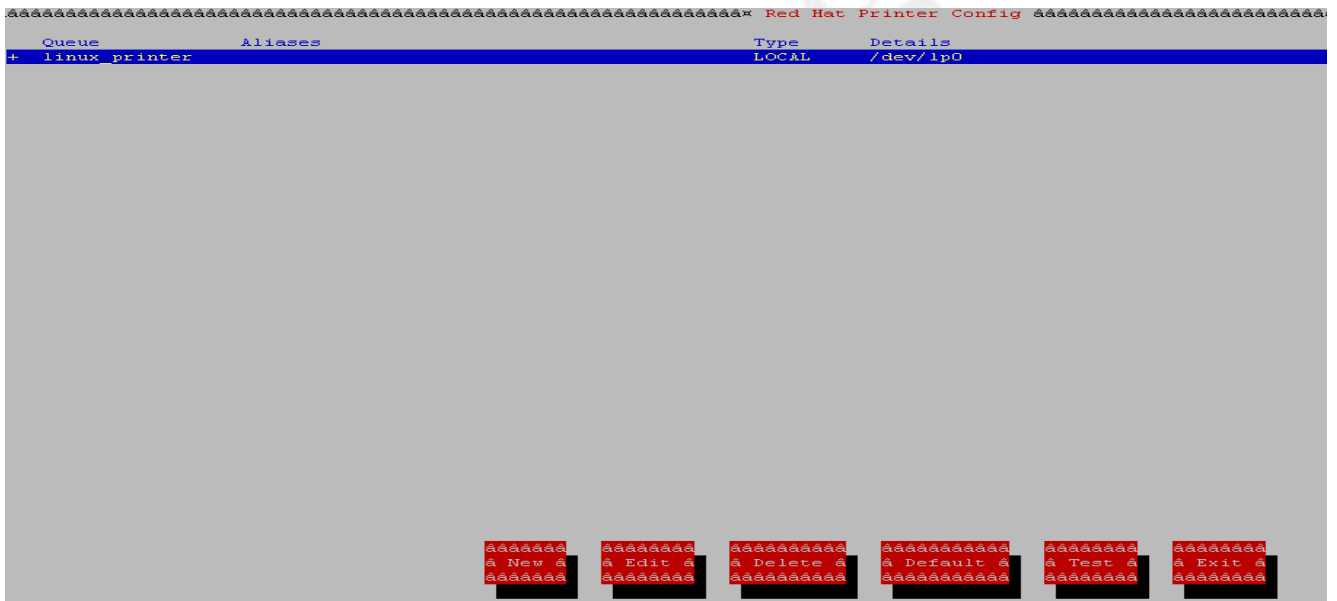
Which line specify to mount all the contents of /nisusers directory from server.

- d. `service autofs restart` : autofs service controls the auto mount feature of linux system. After changing configuration, need to restart the autofs service.
- e. Now login as server's users.

Managing Printer

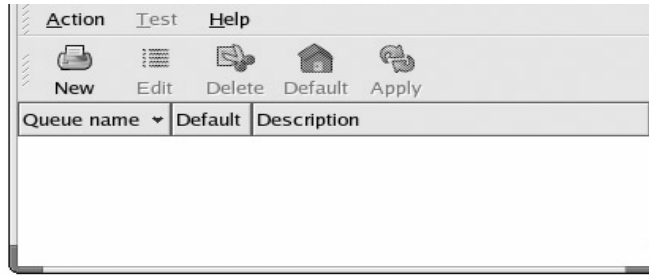
CUPS (Common Unix Printing System) the default printing service in Redhat Enterprise Linux supports many features like IPP (Internet Printing Protocol) based service, can control printing jobs etc.

- a. Installing Locally connected printer
 - Type system-config-printer command

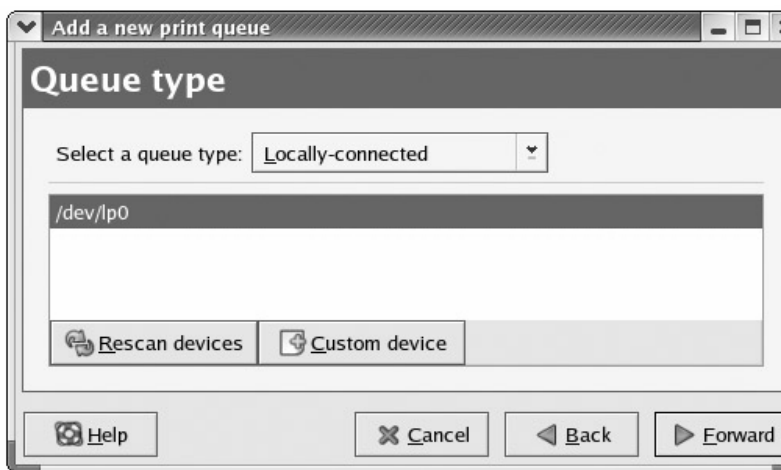


- Click on New
- Type Queue Name (Printer Name)
- Select Queue Type

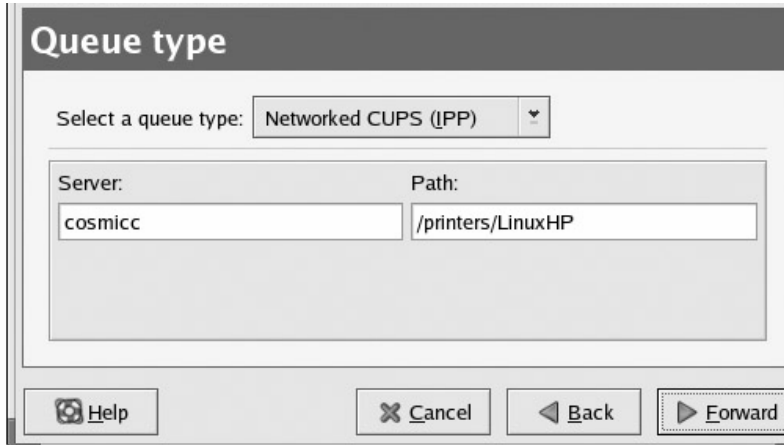
In GUI You will get the screen like:



- you should select locally connected if printer is locally connected



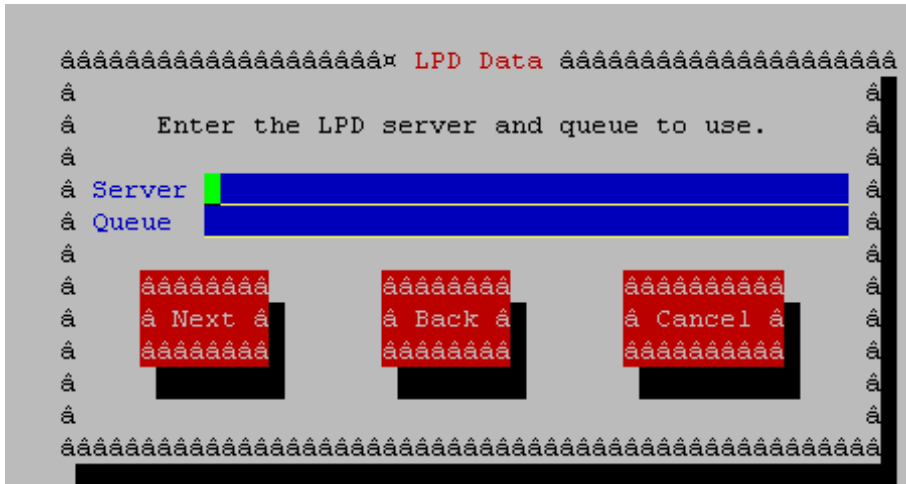
- If your Printer server is Unix based then you should select Unix Print Queue
- In GUI version of Printer Management tool you will get Network CUPS and Unix LPD, if CUPS is using as printing server, you should use the Network CUPS and if LPRng is using you should use Unix LPD.
- When you use CUPS specify the server and printer name /printers/printername and when LPRng is using use server and just printer name



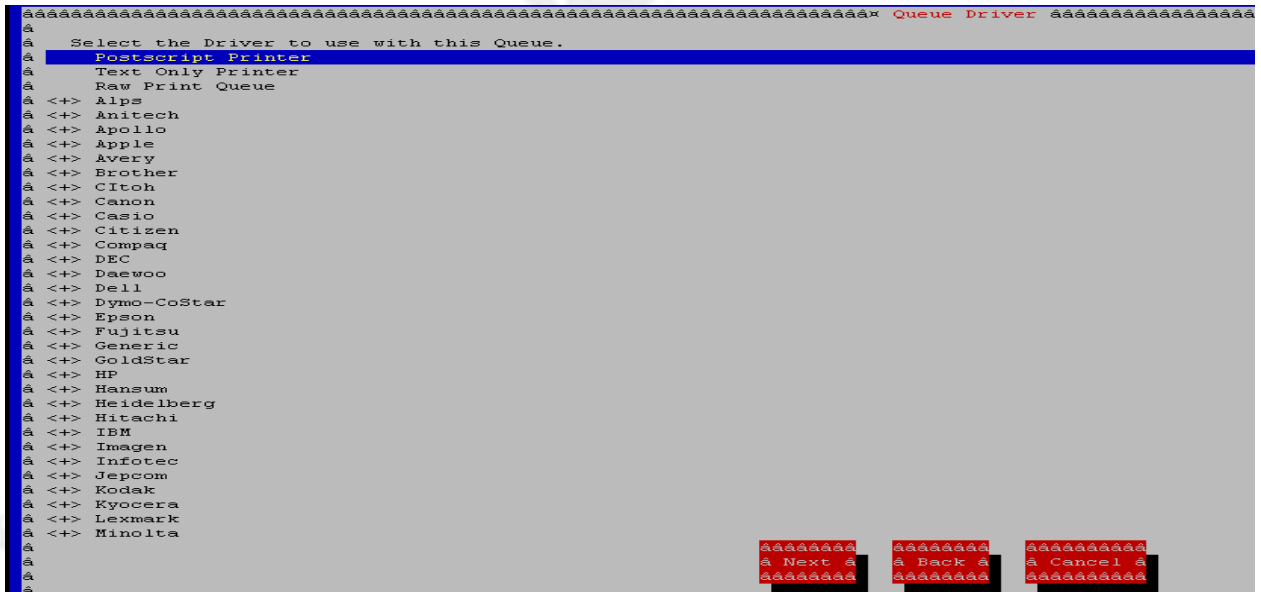
- If your Printer server is Windows based then you should select Windows Print Queue
- If your Printer Server is Novell based then you should select Novell printer
- If your Printer is standalone printer select Jetdirect Print queue.

When you select Local printer device, you need to give the device name where your printer is connected. If your printer is connected it parallel port use /dev/lp0 if printer connected on usb the use /dev/usb/lp0.

If you are going to install the Network based printer, you need to pass the printer server name and print queue name.



While specifying device or server and queue name, you need to select the manufacturer and model of printer.



- Select the Manufacturer and Model then click on next.
- Click on Finish
- CUPS printing service is controlled by cups daemon.

- While you start the cups service it reads the file
 - o /etc/cups/printers.conf
 - o /etc/cups.cupsd.conf

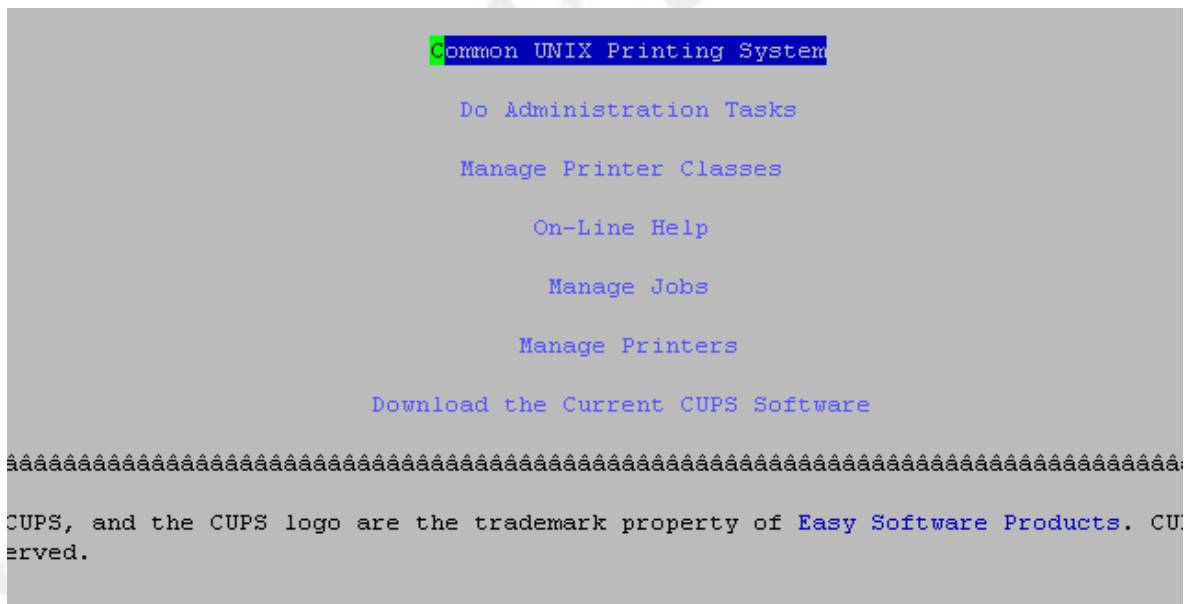
/etc/cups/printers.conf file contains all printers name and other printer related parameters.

/etc/cups/cupsd.conf is the main configuration file.

Managing Printer through HTTP

CUPS has new feature that can manager through Browser.

- Type <http://localhost:631> on your browser



```
Common UNIX Printing System
Do Administration Tasks
Manage Printer Classes
On-Line Help
Manage Jobs
Manage Printers
Download the Current CUPS Software
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
CUPS, and the CUPS logo are the trademark property of Easy Software Products. CUP
erved.
```

Now you will get the main cups page from where you can manage jobs, printer class, queues etc.

Here I'm going to show you how to install the network based printer.

- When you get the CUPS main page, click on Manager Printers
- Click on Add printer
- Type root and password

```
Common UNIX Printing System
Admin
Add New Printer
Name: _____
Location: _____
Description: _____
[ Continue ]
```

- Type Queue Name, Location and Description then continue
- Select Device for printer, if you are going to install network based printer then select either http or ipp.

```
Common UNIX Printing System
Admin
Device for printer1
Device: [Internet Printing Protocol (http)]
[ Continue ]
=====
are Products, All Rights Reserved. The Common UNIX Printing System, CUPS
her trademarks are the property of their respective owners.
```

- Type Device URL or Address

Example: <http://server1.example.com/printers/printer1>

```

Common UNIX Printing System

Admin

Device URI for printer1
Device URI: http _____
Examples:

file://path/to/filename.prn
http://hostname:631/ipp/
http://hostname:631/ipp/port1
ipp://hostname/ipp/
ipp://hostname/ipp/port1
lpd://hostname/queue
socket://hostname
socket://hostname:9100

[ Continue ]

```

Above example shows that installing network based printer installed in server1.example.com named printer1.

- Select Manufacturer as well as Model
- Click on Finish

Now You can test using the some printing command.

Commands	Description
lpr	Sends Printing job to printer
Lpq	Prints all printing queue of printer
lprm	Removes the queue of printer

The X Window System

X Windows System is the foundation class, which provides the Graphical User Interface on Linux. X Window system is

Leading the way in IT testing and certification tools, www.testking.com

very flexible and more transparent, which developed on client and server architecture.

On Redhat Enterprise Linux, X window System is the system having multiple Desktop Environment, Display Manager and File Manager.

- i. GNOME is the default desktop on Redhat Enterprise Linux.
- ii. KDE another excellent Desktop on Redhat Enterprise Linux.

Different desktop having different Display Manager.

- i. GDM Display Manager of GNOME
- ii. KDM Display Manager of KDE
- iii. XDM Display Manager of X Window

Similarly, there are different file manager metacity for GNOME, kwm for KDE and for X window System.

Global Default desktop and display manager is specified in /etc/sysconfig/desktop file.

```
DISPLAYMANAGER="KDE"
```

```
DESKTOP="KDE"
```

Which calls by /etc/X11/prefdm scripts executes on X window system loading time.

User can create user specific default desktop then global settings using **switchdesk** command. Which creates ~/.Xclients and ~/.Xclients-default file. While user

login into GUI first checks whether user specific default desktop is specified or not. If exists loads the user's desktop otherwise reads from /etc/sysconfig/desktop and loads the default desktop specified in global file.

```
#switchdesk "GNOME"
```

When Display Manager is GDM, it appears as below figure.



When Display Manager is kdm, Login Screen appears as follow figure



ion tools, www.testking.com

When Display Manager is xdm, Login Screen appears as follow figure



To start the X window System, runlevel should be 5 or manually can load by using startx command

```
# init 5
```

```
#startx
```

While Loading X Window System, You can face different Problem.

i. Misconfiguration of Video card, Monitor, Resolution etc.

After Installation, you can configuration Video card, Monitor type, Resolution etc by using

```
# system-config-display command.
```



When you select the Options , it will write in /etc/X11/xorg.conf file. While loading the GUI it checks the configuration in /etc/X11/xorg.conf file. If file is missing it gives problem at that time you can solve using system-config-display command.

Similarly xfs service provides the server of font rendering for Graphical Interface. You should check whether this server is running or not.

```
# service xfs status
```

```
#service xfs start
```

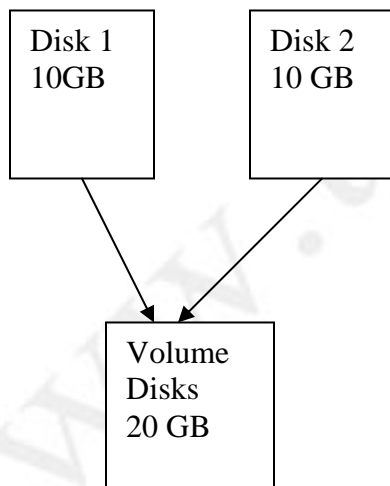
Software RAID (Redudant Array of Inexpensive Disks)

While you use the single disk to store data what will happen if your disk crashed. You lose all data from your disk. Yes, RAID is comes here for fault tolerance. If you are storing the data in RAID device, data is available if one disk become fail.

There different level of RAID generally we use RAID Level 0, RAID Level 1 and RAID Level 5 in our daily works.

RAID Level 0 Also called stripping without parity

RAID level is called stripping it's like volume, which is combines of multiple disks.

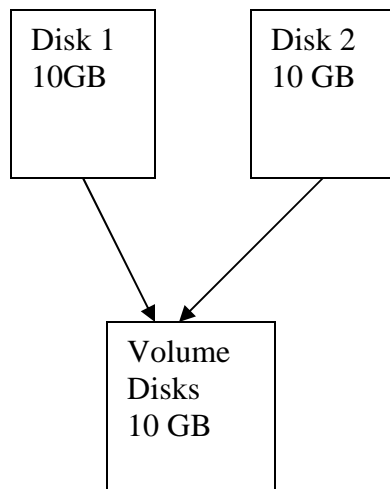


See on the above Figure that when you use two disks in RAID Level 0, you will get new volume with combined size of two disks.

Using the RAID Level 0 is just to make Volume or to increase the performance of disk.

RAID Level 1 : Mirroring

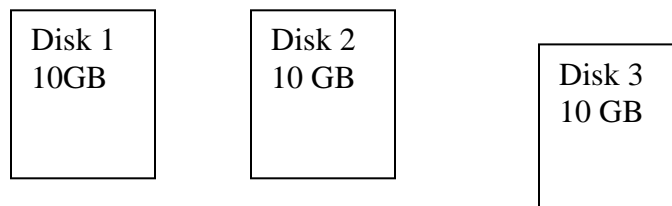
RAID Level 1 is called Mirroring, when you write the data it writes in more than one disks at a time. So, when one disk become fail, data can recover from another disk.



When you configure the RAID Level 1, it automatically mirrors the data written on one disk into another disk. So one disk is used to write mirrored data. When one disk crashed, data can recover from another disk. For RAID Level 1 minimum 2 disks are required.

RAID Level 5 : Stripping with Parity

RAID Level 5 is called Stripping with Parity, when you write the data it writes parity information into another disk. So, when one disk becomes fail, data can recover from another disk. In comparison with RAID Level 1, RAID Level 5 has good data read performance. But for RAID Level 5 minimum 3 disks are required.



Leading the way in *IT testing and certification tools*, www.testking.com

Volume Disks 20 GB

When you configure the RAID Level 5, it writes the parity information into another disk, so when one disk crashed, data can recover from another disk.

Creating RAID Level 0

```
#mdadm -C /dev/md0 --level=0 --raid-devices=2 /dev/hda1  
/dev/hdb1
```

using mdadm command can create the RAID device. The above example creates the First RAID device md0 using /dev/hda1 and /dev/hdb1 devices.

Creating RAID Level 1

```
#mdadm -C /dev/md0 --level=1 --raid-devices=2 /dev/hda1  
/dev/hdb1 --spare-devices=1 /dev/hdc1
```

Which creates the device /dev/md0 of RAID Level 1. When we writes data into /dev/md0 it mirror into hda1 and

hdb1 both devices. As well as one disk specified the spare disk, which automatically used when disk either hda1 or hdb1 become crashed in RAID Array.

Creating RAID Level 5

```
#mdadm -C /dev/md0 --level=5 --raid-devices=3 /dev/hda1  
/dev/hdb1 /dev/hdc1 --spare-devices=1 /dev/hdd1
```

Which creates the device md0 of RAID Level 5. When we writes the data into md0 device it uses disks to write data as well as one disk is used to write the parity information.

Remember that you need to create these partitions in Software RAID Type with System ID 'FD'.

After Creating the RAID Device, you need to create the filesystem

```
#mkfs -t ext3 /dev/md0
```

Or

```
# mke2fs -j /dev/md0
```

Mounting RAID Device

```
# mkdir /data
```

```
#mount /dev/md0 /data
```

RH302

You need to write into `/etc/fstab` file to mount automatically at boot time

```
/dev/md0    /data    ext3 defaults 0 0
```

Checking RAID Status:

```
# mdadm --detail /dev/md0
```

Simulating fail of RAID Array Disk

```
#mdadm --set-faulty /dev/md0 /dev/hda1
```

Removing failed Disks from RAID Array

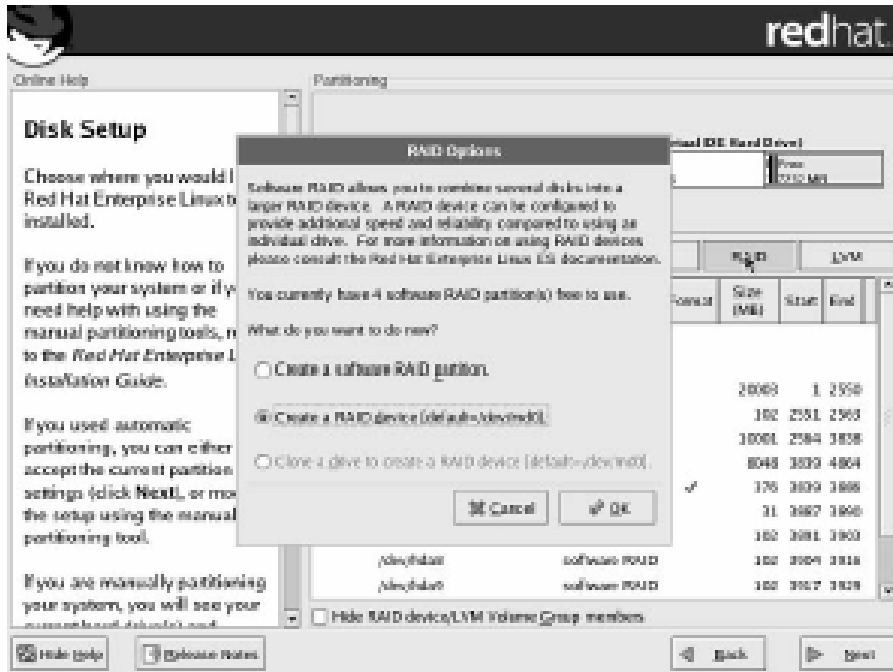
```
#mdadm --remove /dev/md0 /dev/hda1
```

Adding New Disk into RAID Array

```
#mdadm --add /dev/md0 /dev/hdd1
```

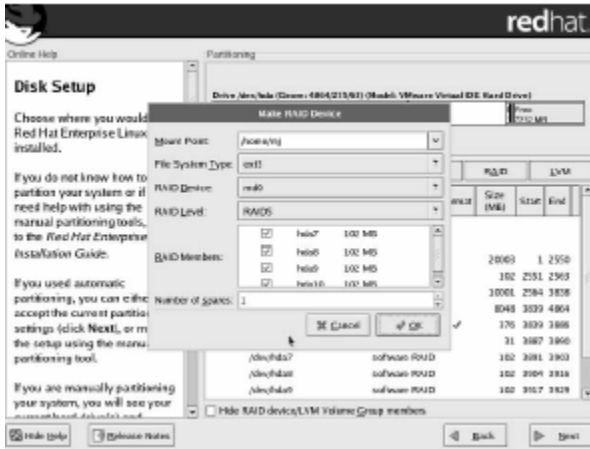
Creating RAID Device At installation Time

See sample Here



At Installation time also you can create the RAID device. Just you need to create the partitions with Software RAID FileSystem Type. After that click on RAID button. Then type the mount point, choose file system type, RAID device, RAID Level , RAID members and type the number of disks used as spare disks.

See sample here



Logical Volume Manager (LVM)

I would like to introduce about LVM through the example :
I created /usr partition with size 5000 MB and /var/ with 1000 MB. After some time you require more space in /var/ due to log file management, you have free space in /usr. Can you manage the space of partition by dynamically increasing or decreasing the size of partitions. Normally no, you need to create the LVM.

In LVM you need to create the Physical volume, Volume Group and Logical Group.

Creating Logical Volume

- i. Create the partitions having 8e system ID.
- ii. Synchronize with partition table using partprobe command

Create the Physical Volume

First Steps of creating the Logical Volume is by creating the Physical Volume. Only the physical Volume disks can be member of Volume Group.

```
#pvcreate /dev/hda12 /dev/hda13 : This example creates the /dev/hda12 as well as /dev/hda13 as a physical Volume.
```

Creating Volume Group

Volume Group is the group name of all member having combined size of all belongs physical Volume.

```
# vgcreate vol0 /dev/hda12 : This example creates the  
vol0 Volume Group named vol0 with the member of  
/dev/hda12.
```

Creating Logical Volume

Logical Volume is the distributed Volume of Volume Group.
We use the Logical Volume.

```
# lvcreate -n data1 -L 50M vol0 : This example creates  
the Logical volume named data1 with the size 50M.
```

Similarly you can create multiple Logical volume on same
Volume Group.

```
# lvcreate -n data2 -L 100M vol0 : Which creates the  
second Logical Volume named data2 with 100M size.
```

Now to use the Logical Volume you need to create the file
system on Logical Volume.

```
# mkfs -t ext3 /dev/vol0/data1
```

```
#mkfs -t ext3 /dev/vol0/data2
```

Now mount the Logical Volume

```
#mount -t ext3 /dev/vol0/data1 /data1
```

```
#mount -t ext3 /dev/vol0/data2 /data2
```

If you want mount automatically at boot time you need to
write in /etc/fstab file.

RH302

```
/dev/vol0/data1 /data1 ext3 defaults 1 2
```

As I described the feature of Logical Volume, we can resize Logical Volume dynamically. Let's increase or decrease the size of Logical Volume and bring it online.

```
# lvextend -L+20M /dev/vol0/data1 : Which increase the size of Logical Volume data1 by 20M.
```

If you check the size using `df` command of directory `/data1`, you will get the initial size, if you want as same as Logical Volume, you need to bring the Logical Volume online by using the `ext2online` command.

```
# ext3online -d /dev/vol0/data1
```

Now `/data1` directory knows that the size of `data1` Logical Volume is 70M. You can verify by using the `df` command.

You can display the properties of Logical Volume, Volume Group, Logical Volume by using

`pvdisplay`, `vgdisplay` and `lvdisplay` command.

Example:

```
#pvdisplay /dev/hda12
```

```
#vgdisplay vol0
```

```
#lvdisplay /dev/vol0/data1
```

Similarly you can use `lvresize` command to resize as well as `vgextend` to add new physical volume into the Volume Group.

Example:

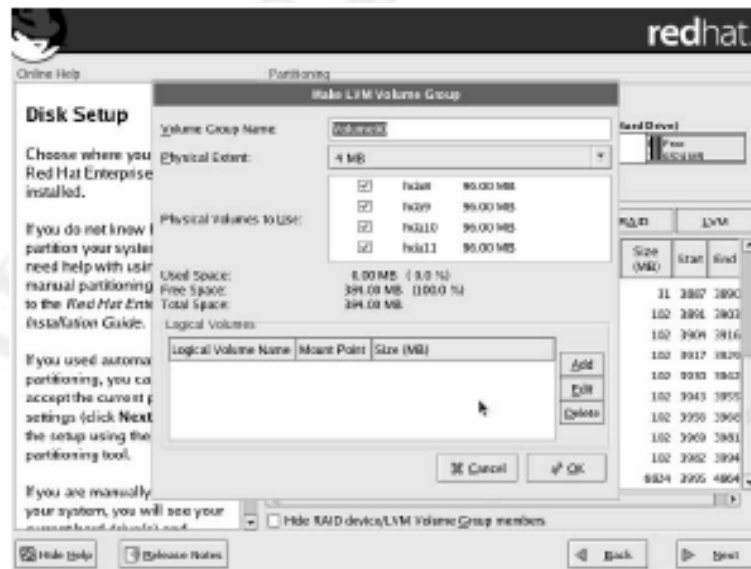
If you want to add `/dev/hda13` into the Volume `vol0`

```
#vgextend vol0 /dev/hda13
```

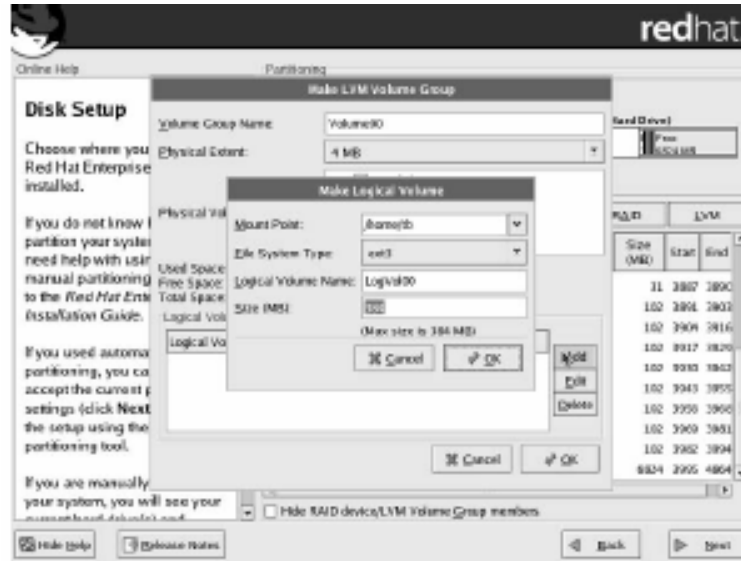
Verify using the `vgdisplay` command.

Configuring LVM at Installation Time

If you want to configure the LVM at Installation time, just create the partitions having Logical Volume File System. Then click on LVM, specify the Volume Group.



After specifying the Volume Group Name, Click on Add button and type Logical Volume name, mount point, size and filesystem.



Implementing User Quotas

Quota keeps individual user or group from occupied all space available on the individual partitions.

Administrator can apply the quotas policy per user or per group basis on number of blocks or number of inodes.

Here I'm going to implement the quota on user's home directory. We can apply the rules of how much individual user can occupied the space or how many inodes can use.

Quota feature is implemented in Linux Kernel just you have to enable on file system using `usrquota` or `grpquota` options while mounting the file system.

At boot time to mount the filesystem `rc.sysinit` reads the file `/etc/fstab` file so you should specify the option in this file.

```
LABEL=/home /home      ext3
    defaults,usrquota,grpquota 1 2
```

`usrquota` options enable the user quota on `/home` file system and `grpquota` option enable the group quota on `/home` file system.

To enable this options either you should reboot the system or re-mount the file system.

```
# mount -o remount /home
```

Now create the blank file to store the information of user quota and group quota information.

```
#touch /home/aquota.user
```

```
#touch /home/aquota.group
```

Now initialize the quota database of user and group using the quotacheck command.

```
# quotacheck -ugfm /home
```

By default user quota option only enable so if you are going to implement group quota, you should use the g option.

```
# quotaon -ug /home
```

Just on the quota on /home for user and group

If you want to off the quota use the quotaoff command

Now set the policy for user and group using the edquota command.

```
# edquota -u user1 /home
```

Disk quotas for user ez (uid 504)

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/hdda6	300	400	500	20	0	0

In the above example, user1 already occupied 300 KB, and now set the 400 soft limit to give the warning and 500 KB

is the hard limit that user user1 can't exceeds the hard limit.

Similarly you can set the quota limit by using the number of inodes. Just specify the hard limit and soft limit on inodes.

Similarly we can set the quota to group member.

#edquota -up user1 user2 user3 user4 : Which transfer the policy of user1 to other user user2 user3 and user4.

Monitoring Quota of users

#repquota /home : Which reports the quota information of /home

#quota username : Which reports the quota information of individual user.

Troubleshooting

In real time working you can get different types of problem and should face as well as solve. I can't explain what problem will you face. Here I try to explain some important file as well as important parameters of files.

1. Troubleshooting with networking:

i. Check whether file `/etc/sysconfig/network` file exists or not as well as this parameter

`NETWORKING=yes`

`HOSTNAME=?`

`GATEWAY=?`

`NISDOMAIN=?`

ii. Check the interface configuration file

`/etc/sysconfig/network-scripts/ifcfg-eth0`

`DEVICE=eth0`

`ONBOOT=yes`

`BOOTPROTO=static OR dhcp`

`IPADDR=x.x.x.x`

`NETMASK=x.x.x.x`

`GATEWAY=x.x.x.x`

Leading the way in IT testing and certification tools, www.testking.com

```
# check whether device is down
```

```
# ifconfig, ifdown eth0, ifup eth0 etc
```

- iii. Check Whether Module of device is loaded or not using lsmod command and try to manage modules using insmod, rmmod, depmod, modprobe command.
- iv. Check aliases is created or not in /etc/modules.conf file
- v. Check the Routing Table or Gateway

```
# route -n command
```

Remove if incorrect routing table is added using route add command.

```
# route add -net x.x.x.x netmask x.x.x.x gw x.x.x.x
```

```
# route del -net x.x.x.x netmask x.x.x.x gw x.x.x.x
```

2. Troubleshooting with X Window System

Sometime you will face problem while booting the system in Runlevel 5. There are some cases, in which you face problem while loading the GUI.

- i. Check whether file /etc/X11/xorg.conf
- ii. If doesn't exists configure Video card, monitor, resolution etc using system-config-display.
- iii. Check whether xfs service is running or not.
- iv. Check the default runlevel
- v. Check whether Hard limit quota is touched.

3. Troubleshooting with System Boot

Leading the way in IT testing and certification tools, www.testking.com

This is the most important and most give mind to solve the boot related problem. You should which, which files used at boot time and how to troubleshoot.

i. Boot loader

Check whether MBR (Master Boot Record) is crashed, if MBR become crashed, Boot loader can't load OS, whether Boot loader is mis-configured ?

If problem with boot loader, check the configuration. When you boot the system, you will get the grub screen to select Operating System from the List.

In grub screen there lots of option available. Press c for Grub Prompt, e to edit the parameters, b to boot, a to append etc.

See the sample of grub prompt,

```
Grub>root (hd0,0)
```

```
Grub>kernel /vmlinuz-2.6.9-5.EL ro root=LABEL=/ rhgb quiet
```

```
grub> initrd /initrd-2.6.9-5.EL.img
```

```
Grub>boot
```

Now if passed parameters are correct, you successfully able to boot the System.

Similarly use different shortcuts to edit or trouble shoot. Like e, a etc.

If you forget the root's password what you will do ? I already explained that there are different runlevels. You need to boot your system in Single user mode.

Just press the a key in grub screen

You will get line like:

```
kernel /vmlinuz-2.6.9-5.EL ro root=LABEL=/ rhgb quiet s
```

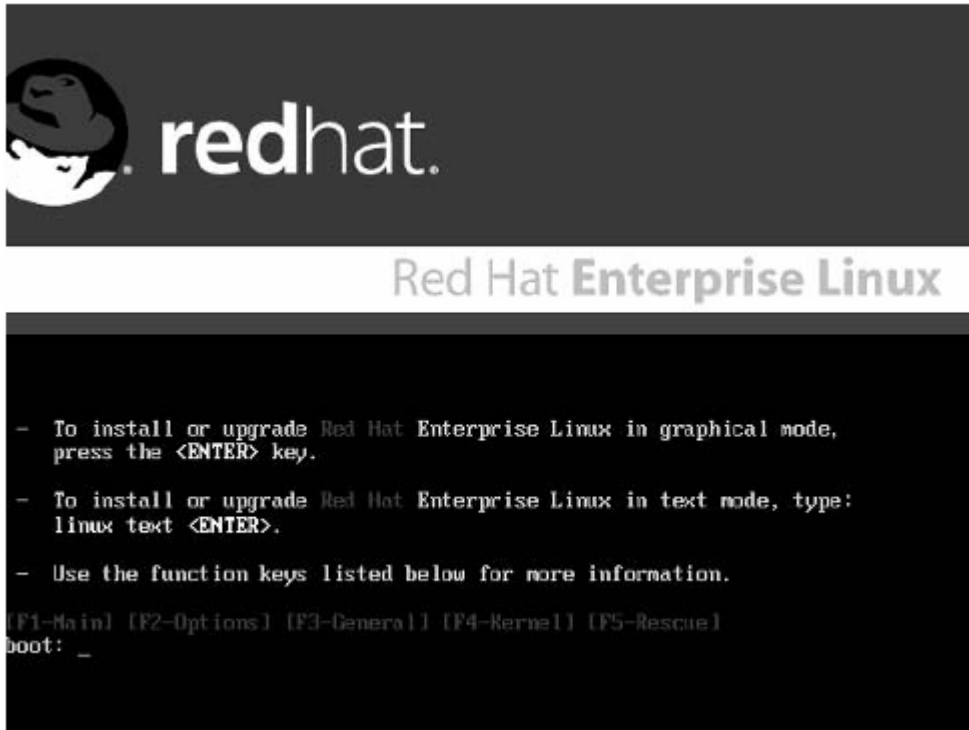
Type s at the end of line then press enter key, now your system will boot in single user mode, root will automatically logged in bash shell, just change the password and boot.

If boot loader crashed, you need to re-install new boot loader. At that time, you need to start the system in Rescue mode.

Booting system in Rescue Mode

- i. Start the system with RHEL 4 1st CD or boot.iso cd

You will get the screen like this



- ii. Type linux rescue in boot prompt.
- iii. Select the General Options
- iv. Select option to use or not to use Ethernet card and assign the IP Address
- v. Click on Continue
- vi. Check the message that, previous partitions are mounted in /mnt/sysimage directory.
- vii. Now change the Root file system

```
# chroot /mnt/sysimage
```

Now Install the Boot loader

```
# grub-install /dev/hda
```

- ii. Kernel File : Check whether Kernel file is crashed or removed from the system, at that time, you can install at rescue mode.
- iii. Check the init configuration file /etc/inittab configuration
- iv. Check the /etc/fstab that writing in in-proper ways or writing in-proper file system. Remember that when problem in /etc/fstab file, system will boot in emergency mode, that is called file system maintenance mode. you can manually boot the system in emergency mode

```
Grub>kernel /vmlinuz-2.6.9-5.EL ro root=LABEL=/ rhgb quiet  
emergency
```

Just provide the root password, remount the root (/) filesystem in read and write mode, edit the /etc/fstab file.

Section 3

RedHat Certified Engineer (RHCE) Preparation

Can you do independently ?

- *Can Configure DNS Master Server ?*
- *Can Configure and Maintain Slave DNS server ?*
- *Can Configure DNS Global Options ?*
- *Can Configure FTP Server ?*
- *Can deny or allow real user or anonymous login via FTP ?*
- *Can Configure NFS server as per needs ?*
- *Can Configure NFS Client ?*
- *Can Share Data through Samba for Windows Users ?*
- *Can Share with Different Security Options ?*
- *Can Share with user or hosts based Authentication ?*
- *Can Share as per user needs ?*
- *Can Configure Sendmail Server ?*
- *Can Configure procmail and fetchmail ?*
- *Can Configure Apache Web server for IP based web site hosting ?*
- *Can Configure Apache web server for Name based web site hosting ?*
- *Can Configure Apache web Server with user or hosts based Authentication ?*

Leading the way in IT testing and certification tools, www.testking.com

RH302

- *Can Configure Apache web server by implementing SSL ?*
- *Can Configure Squid Proxy Server ?*
- *Can Configure NIS Master and Slave Server ?*
- *Can Configure Time, Origin based Login ?*
- *Can Limit number of process or logins to users ?*
- *Can Secure Stand Alone with TCP_Wrappers ?*
- *Can Secure Transient Services with TCP_Wrappers ?*
- *Can Secure Transient Services with xinetd mechanism ?*
- *Can you Configure the Iptables firewall ?*

RHCE is the 100% practical Exam so you should know every thing above mentioned topics.

Domain Name Server (DNS)

First you should know what DNS will do, I would like to go through by example, when you try to access the `www.testking.com`, it will work and easy to remember. But system works on the basis of Logical Address called IP Address but difficult to remember `202.2.2.2` etc. So there will DNS comes, which converts the Name to IP and IP to Name as well as define the Mail Exchanger of the Domain.

- i. Resolve the host name into IP Address called Forward Lookup
- ii. Resolve the IP Address into host name called Reverse Lookup

In Redhat Enterprise Linux, BIND (Berkerenly Internet Name Domain) is used as a DNS System, which is world's most used Software.

Let's go through by example of configuring the Forward Lookup:

First you need to define the zone, which is called the part of domain. All zone information will write into `/etc/named.conf`.

```
#vi /etc/named.conf

zone "example.com" IN {

    type master;
```

Leading the way in IT testing and certification tools, www.testking.com

```
file "example.com.zone";

};
```

Figure of /etc/named.conf

```
// generated by named-bootconf.pl
options {
    directory "/var/named";
    /*
     * If there is a firewall between you and nameservers you want
     * to talk to, you might need to uncomment the query-source
     * directive below. Previous versions of BIND always asked
     * questions using port 53, but BIND 8.1 uses an unprivileged
     * port by default.
     */
    // query-source address * port 53;
};
// a caching only nameserver config
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
zone "." IN {
    type hint;
    file "named.ca";
};
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; };
};
include "/etc/rndc.key";
```

Generally DNS server are in two types one is called master, which has all configuration data and another is called slave, which has the backup of master configuration. When Master DNS become fails, slave provides the service to client.

named-checkconf : which checks the configuration of /etc/named.conf configuration

/etc/named.conf is the file where we write the zone, type of zone and database of zone configuration. If you check in this file at the top there is global options, which specified the directory options in /var/named directory. Now you need to create the example.com.zone file into /var/named directory.

But this is the changes from RHEL 3 to RHEL 4, in RHEL 3 DNS runs on / root directory but in RHEL 4 root directory of DNS is separated using the chroot means from now DNS has it's own root directory.

Which is defined in /etc/sysconfig/named file

```
ROOTDIR=/var/named/chroot
```

Let's go to create the zone database file:

Generally it store the information in following syntax:

```
[domain] [ttl] [class] [type] [rdata]
```

Where domain specify domain name, ttl time to live how much information should be cached, class record classification usually IN means Internet, type, Record Type either SOA, MX of A and rdata specify data for record.

```
#vi /var/named/chroot/var/named/example.com.zone
```

```
$TTL 3434
```

```
@ IN SOA example.com. admin.example.com. (
```

```
100; Serial Number

1H; Refresh Time

1M; Retry Time

1W; Expire Time

1D; Minimum Time to Live

)

@ IN NS 192.168.0.1

@ IN NS 192.168.0.2

www IN A 192.168.0.3

ftp IN A 192.168.0.4
```

In First Line defined the Time to Live on cache Name server, Cache name server stores the lookup information into the cached and gives reply to client rather than lookup times to times.

Here @ symbol is reversed for zone name example.com, every zone should start with SOA that means this is complete database for particular zone can reply to client. admin.example.com is the email address to which DNS should send the mail.

In DNS database file, there are five time parameters

- i. First is Serial Number Slave will try to refresh with master DNS server on defined refresh time interval but question is that when slave should copy the master's database file when changes occurred in master !! Remember that when you made any changes on master, you need to upgrade the Serial Number. When slave contact to master, it checks serial Number, if serial Number is updated then slave DNS copy the updated portion from Master.
- ii. Refresh Time : Time to Refresh with Master DNS server by Slave DNS server
- iii. Retry Time : Time to retry if first refresh failed
- iv. Expire Time: Domain when should expire
- v. Minimum Time to Live for Negative Answering

Now you need to specify the DNS Name server which specified by NS record.

I configured there are two DNS server for example.com one is master 192.168.0.1 and another is 192.168.0.2, which is slave DNS server.

Now you need to add host on zone by using A Record Type.

www IN A 192.168.0.3 Which specify that www.example.com is 192.168.0.3 Where A record specify Associate IP Address.

Now let's configure by specifying the Mail Exchanger of domain. Mail Exchanger is the host, which is responsible to delivery the mail to domain users.

```
#vi /var/named/chroot/var/named/example.com.zone
```

```
$TTL 3434

@ IN SOA example.com. admin.example.com. (

    100; Serial Number

    1H; Refresh Time

    1M; Retry Time

    1W; Expire Time

    1D; Minimum Time to Live

)

@ IN NS 192.168.0.1

@ IN NS 192.168.0.2

www IN A 192.168.0.3

ftp IN A 192.168.0.4

mail IN A 192.168.0.5

mail1 IN A 192.168.0.6

@ IN MX 5 mail.example.com.

@ IN MX 10 mail1.example.com.
```

See the configuration, mail.example.com is associated with 192.168.0.5 and mail1.example.com is associated with 192.168.0.6. We can specify the Mail Exchanger of domain

using MX record Type, Where mail.example.com is the primary Mail Server for example.com domain and maill.example.com is the secondary mail exchanger which specified by the numerical value. First Priority will give to host having lowest number.

```
#named-checkzone example.com
/var/named/chroot/var/named/example.com.zone : which
checks the configuration of
/var/named/chroot/var/named/example.com.zone
configuration.
```

```
# service named start | restart | status
```

Now configure the Client DNS server

```
#vi /etc/resolv.conf

nameserver 192.168.0.1

nameserver 192.168.0.2

#host www.example.com

#nslookup ftp.example.com

#dig mail.example.com
```

Now it's time to configure the DNS with load balancing. Yes, you access the www.hotmail.com site what one single host can provide service to millions of user at a time no, you need to configure more than one host for www.hotmail.com. BIND has mechanism to redirect the request to different hosts.

```
#vi /var/named/chroot/var/named/example.com.zone

$TTL 3434

@ IN SOA example.com. admin.example.com. (

    100; Serial Number

    1H; Refresh Time

    1M; Retry Time

    1W; Expire Time

    1D; Minimum Time to Live

)

@ IN NS 192.168.0.1

@ IN NS 192.168.0.2

www 0 IN A 192.168.0.3

www 0 IN A 192.168.0.4

www 0 IN A 192.168.0.5

www 0 IN A 192.168.0.6
```

RH302

Now four hosts are configured for www. You need to configure web server in these four hosts to provide service in equal load balancing.

Just check using host command on client.

Let's go with the Reverse Lookup

Reverse lookup maps Name into IP Address, when user query using IP your DNS server should reply to client by mapping into name.

```
# vi /etc/named.conf

zone "0.168.192.in-addr.arpa" IN {

    type master;

    file "0.168.192.in-addr-arpa.zone";

};
```

In Reverse Lookup you need to use the in-addr-arpa keyword because IP Addresses are managed by ARPA, similarly specified the type and file name.

```
# vi /var/named/chroot/var/named/0.168.192.in-addr.arpa.zone

$TTL 5454

@ IN SOA @ admin.testking.com. (

    100; Serial Number
```

```
1H; Refresh Time

1M; Retry Time

1W; Expire Time

1D; Minimum time to Live

)

@ IN NS 192.168.0.1

@ IN NS 192.168.0.2

3 IN PTR www.example.com.

4 IN PTR ftp.example.com.

5 IN PTR mail.example.com.

# service named start | restart

# host 192.168.0.3
```

Global Options in /etc/named.conf

directory : Path of directory use to configure the zone database file. By default /var/named directory.

allow-query : Clients list to allow query on DNS server

allow-transfer : Who can be slave name server ? Allowed host can transfer the DNS database of Zone into slave server.

Forwarders : Forward to whom it DNS server unable to resolve the host.

Example

```
acl "Internal" { 192.168.0.0/24;172.24.0.0/26; };

options {

    directory "/var/named";

allow-query { Internal; };

forwarders { 202.2.2.2; };

allow-transfer { 192.168.0.2; };
```

In example I created one ACL (Access Control List), which contains two different network. In directory options default directory is written so zone database file should create on this directory. host from either 0 or 24 network can query to DNS server, If DNS server unable to resolve client request it forwards request to next dns server 202.2.2.2 and 192.168.0.2 can be slave server by copying master DNS database.

Configuring Slave DNS server

I already mentioned that DNS can be either master or slave server. Slave provides the backup to Master server.

In my Configuration Example: 192.168.0.1 is the master and 192.168.0.2 is the slave server

```
# vi /etc/named.conf

zone "example.com" IN {

    type slave;

    masters { 192.168.0.1; };

    file "example.com.zone";

};
```

In Master you need to allow transfer.

```
# server named start | restart
```

May be You unable to transfer the database from master to slave if there is not write permission to named group in /var/named/chroot/var/named. When you examine the Log file (/var/log/messages) you will get the errors of permission denied error.

```
# chmod g+w /var/named/chroot/
```

Now again restart the named service, database file will transfer from master to slave server.

RNDC (Remote Name Daemon Control): Utility which controls the Named service, which uses the encrypted key to manage

secure communication. /etc/rndc.conf is the main configuration file for rndc service.

```
# rndc reload : which reload the rndc by using rndc configuration file.
```

If you feel the need to secure your DNS server, you'll want to change this key. The following command automatically sets up a new key in /etc/rndc.key, with a key size of 512 bits.

```
# rndc-confgen -a -b 512
```

By default in Redhat Enterprise Linux, root server comes with configuration, when user sends request to DNS server either DNS reply to client or forward the request to another DNS server or sends the request to root name server, where all DNS record maintained. Here is the default configuration of root name server.

```
zone "." {  
  
    type hint;  
  
    file "named.ca"  
  
};
```

FTP Server Configuration

FTP is the file transfer protocol use to transfer files between networks. FTP services runs on port 20 and 21, where 20 for data and 21 for user authentication.

In Redhat Enterprise Linux vsftpd (Very Secured FTP) is used as FTP server. You need to install vsftpd package.

```
#rpm -ivh vsftpd-*
```

By default Real User as well as Anonymous can Login in FTP server. Real user Login in user's home directory and anonymous login in /var/ftp/ directory.

/etc/vsftpd/vsftpd.conf is the main ftp configuration file.

I will go through the some configuration of vsftpd.conf

```
anonymous_enable=YES
```

If you want to deny anonymous you can write

```
anonymous_enable=no
```

Where # symbol is used comment

```
local_enable=YES
```

Whether login allow to real user or not ? I already wrote that anonymous as well real users are allow to login.

```
write_enable=yes
```

This options enable logged in users to access fully root filesystem as well as can created directory in ftp prompt.

Local_umask=022

What to set the default permission of uploaded files ? By default setting 022 means

666

022

644

So this mask set the permission of rw-r--r-on uploaded files.

You Know that by default Real users only can upload files into FTP server anonymous can download only. There are options either enable to upload to anonymous or not.

```
#anon_upload_enable=YES
```

```
#anon_mkdir_write_enable=YES
```

If you want to enable file upload by anonymous uncomment anon_upload_enable=yes line. But remember that you need to create a directory with ownership of ftp user as well as write permission to ftp user.

Anonymous user can create directory or can write from ftp prompt or not ? if you uncomment the line anon_mkdir_write_enable=yes, anonymous can create the directory in ftp prompt.

You want to display message on directory basis ? When user changes directory through FTP can display directory message. This option enable by default.

```
dirmessage_enable=YES
```

To display directory message, you need to create file .message and write message what you want to display.

FTP server maintains the log of uploading and downloading files in /var/log/xferlog file. This option also by default enable.

```
xferlog_enable=YES
```

FTP service uses 20 and 21 Port, where 20 for ftp data and 21 for user authentication.

```
connect_from_port_20=YES
```

```
#chown_uploads=YES
```

```
#chown_username=whoever
```

Ownership change or not of uploaded file having no ownership, example uploaded by anonymous.

Example:

```
Chown_uploads=yes
```

```
Chow_username=user1
```

Now Uploaded files ownership will be user user1.

Denying Certain users logging through FTP

/etc/vsftpd.ftpusers file is used to deny the real users for ftp service.

Enter the user name one per line to whom you want to deny.

User1

User2

User3

/etc/vsftpd.user_list file some time used to deny, some to allow. IF you use userlist_enable=yes in vsftpd.conf file, this file is used to deny, if userlist_enable=no then only the user written in /etc/vsftpd.user_list are allowed to access the ftp service.

After changing the configuration restart the vsftpd service.

```
# service vsftpd restart
```

If you would like to start vsftpd service automatically at next reboot

```
#chkconfig vsftpd on
```

FTP Client

There are different ways of accessing the ftp service. One way is using ftp or lftp client tools.

```
#ftp server
```

or

```
#lftp -u username server
```

When you connect to ftp server will get like this prompt

```

230-welcome to Nike's FTP server
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:
!                cr                ndir                proxy             send
$                delete             nget               sendport         site
account          debug             mkdir              put              size
append           dir              nl                 pwd              status
ascii           disconnect        no                 quit             struct
bell            form             modtime           quote            system
binary          get              nput              rcv              sunique
bye             glob            newer             reget           tenex
case           hash            nmap             rstatus         trace
ccc           help            nlist            rhelp           type
cd             idle            ntrans           rename          user
cdup           image           open             reset           unmask
chmod          lcd             passive          restart         verbose
clear          ls              private          rmdir           ?
close         nacdef          prompt           runique
cprotect       ndelete        protect          safe
ftp> help rmdir
rmdir          remove directory on the remote machine
ftp> help open
open           connect to remote ftp
ftp>

```

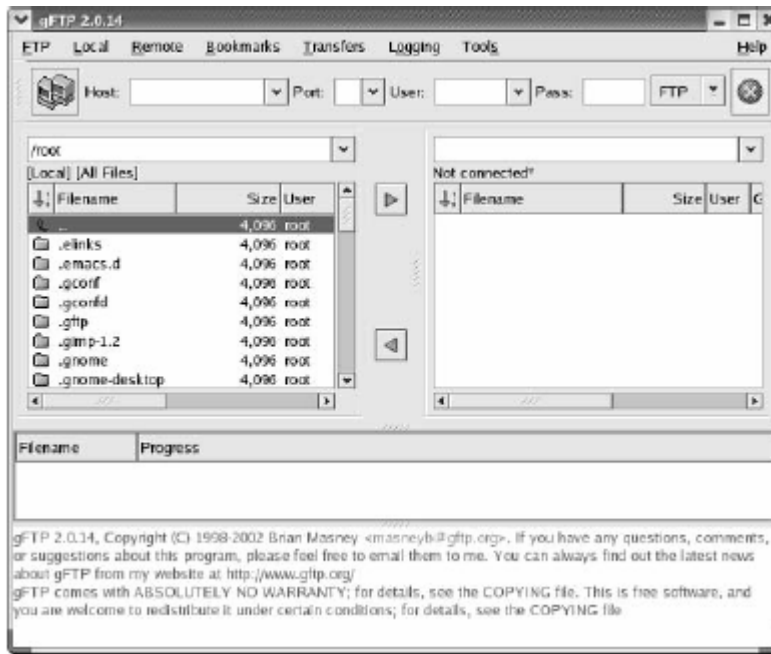
Some Commands runs in FTP prompt

Commands	Description
Put	Uploads single file at a time
Mput	Can upload multiple files using wildcard
Get	Download Single File
mget	Download Multiple Files
mkdir	Creates directory from ftp prompts
Ls	List Directory Contents
Pwd	Displays absolute Working path
cd	Change Directory
User	Allows enter username and passowrd

If you enjoy to work with Graphical User Interface version, there are lots of tools for ftp connections. In Redhat Enterprise Linux 5 gFTP and Kget etc applications.

Leading the way in IT testing and certification tools, www.testking.com

In Gnome Click on Applications→Internet→gFTP



NFS Server Configuration

NFS (Network File System) is the standard File sharing services in Linux and Unix. Through NFS, we can share the data in Linux Environment. Redhat Enterprise Linux uses NFS in both server and client side.

NFS is very easy to configure you need to just write in /etc/exports file.

Syntax:

Directory Client(Permission)

Example:

```
/pub            *.example.com(rw, sync)
/public        192.168.0.0/255.255.255.0(rw, sync)
192.168.1.0/255.255.255.0(ro, sync)
```

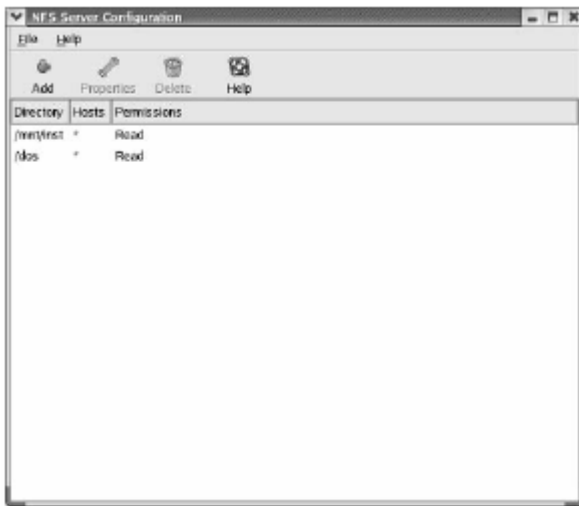
Client List can specify either using IP Address or host name. *.example.com represents all the members of example.com domain. Similarly client list can write using IP Address/subnet mask. In above example 0 network gets in read and write mode as well as 1 network gets in read only mode.

Options in NFS:

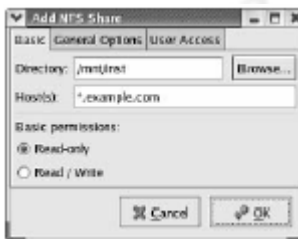
ro : Shared permission Read only
rw : Shared permission Read and Write
sync : Shared permission in sync mode
no_root_squash : Remote root user gets permission as local root user
all_squash : All remote user mapped as anonymous user

Once you've modified `/etc/exports`, you need to do more. First, this file is simply the default set of exported directories. You need to activate them with the `exportfs -a` command. `exportfs -r` refresh `/etc/exports` shares. As well as `exportfs -v` list all shared directories from local computer.

Using GUI tool, you can configure the NFS server using `system-config-nfs` command



Click on Add



Click on General Options



NFS is the RPC service so you need to start portmap with nfs.

```
# service nfs start
```

```
#service portmap restart
```

Similarly you can check what data are shared from the remote host using showmount command.

```
#showmount -e server
```

You can use the shared directory from the server using mount command as well as using Autofs feature.

Samba Server Configuration

Samba helps to share the data between Linux and Windows System. Microsoft developed NetBIOS protocol over TCP/IP to resolve Name similarly SMB works based on NetBIOS protocol.

SMB helps

- Sharing Data
- Sharing Printers
- Authentication and Authorization
- Name Resolution with WINS server

Samba Server Installation

```
#rpm -ivh samba-*
```

```
#rpm -ivh samba-client-*
```

samba package provides the server configuration interface and samba-client provides the samba client tool to connect to Microsoft shares.

Let's go to connect to Microsoft Share:

```
#smbclient -L //computer1 -U administrator%password
```

```
Domain=[ALLACCESS] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
-----
Sharename      Type      Comment
-----
RHHEL3        Disk     Mastering Red Hat Enterprise Linux Book
IPC$          IPC      Remote IPC
D$            Disk     Default share
print$        Disk     Printer Drivers
SharedDocs    Disk     Disk
mount2000    Disk     Linux Transfer for Windows
RHCE4        Disk     Disk
ftpboot       Disk     Disk
HP LaserJ     Printer  Comment Test
Downloads     Disk     Disk
RedHat        Disk     Disk
ADMIN$        Disk     Remote Admin
c$            Disk     Default share
Auctions     Disk     Disk
cfs           Disk     Disk
Isabel        Disk     Disk
Printer       Printer  hp par 1200 series
L$            Disk     Default share
Domain=[ALLACCESS] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
-----
Server         Comment
-----
Workgroup      Master
```

This command displays all shared data from computer computer1. Where computer1 is the Microsoft Windows netbios name. SMB authenticate to user so username is administrator and password is password.

Suppose test directory is shared from computer1 and you want to connect to shred directory

```
#smbclient //computer1/test -U administrator%password
```

After Connecting you will get smb prompt.

```
Smb:<> ls
```

```
Smb:<> get filename
```

```
Smb:<>put filename
```

Another way of connecting to windows share using mount or smbmount command.

```
#mount -t smbfs //computer1/test /mnt/smb -o  
username=administrator,password=password
```

It will mount the shared test directory into /mnt/smb directory. It brings the external windows shared directory into the Linux Filesystem Hirerchy. When mounting the samba shared data, you need to specify the smbfs filesystem.

```
#umount /mnt/smb unmounts the mounted filesystem
```

```
#smbmount //computer1/test /mnt/smb -o  
username=administrator%password
```

smbmount also same as mount command but only use to mount samba shared data.

Samba Server Configuration

/etc/samba/smb.conf is the main configuration file for samba server in linux as well as other files located in /etc/samba directory. smb is the samba service.

When you install samba rpm package it install the package with default configuration file /etc/samba/smb.conf. It is better way to go with basic example.

1. Sharing Data

```
#vi /etc/samba/smb.conf
[global]
netbios name=linuxserver
workgroup=mygroup
server string=sharing from linux server
security=share

[data]
path=/data
browsable=yes
writable=yes
public=yes
```

I recommend you rename the default smb.conf file and create new.

There are some tags are predefined example, global, printers, homes etc.

Global section is used to define the global option to other share data.

```
netbios name=linuxserver
```

I already mentioned that Microsoft Windows uses netbios protocol to resolve computer name same thing what name should resolve or what name should display in network places. Your share will display with linuxserver name.

Your samba share belong which group that defines using workgroup directives. This share belongs to mygroup.

Server string directives is used to write the description of share. And security defines the level of security of samba share. Value of Security can be:

Security=Server : Server Security mode is left over from the time when samba was not capable of acting as a domain member server. It is highly recommended not to use this feature.

Security=User : User level security first because it's simpler. In user-level security, the client sends a session setup request directly following protocol negotiation. This request provides a username and password. The server can either accept or reject the username and password combination.

security=share : In share level security, the client authenticates itself separately for each share. It sends a password along with each tree connection request, but it does not explicitly send a username with this operation.

Now it's time to define share name. [data] is the share name of shared directory.

```
[data]
path=/data
browsable=yes
writable=yes
public=yes
```

path is the directory to share, **browsable=yes** means shared directory appear in network places, if you would like to share as hidden share use no option.

writable=yes, this is share level permission. Directory is sharing in read and write mode.

public=yes, guest user of windows can access or not.

Now you have to start the smb service

```
#service smb start | restart
```

2. Sharing Data with user Authentication

```
#vi /etc/samba/smb.conf
[global]
netbios name=linuxserver
workgroup=mygroup
server string=sharing from linux server
security=user
smb passwd file=/etc/samba/smbpasswd
encrypt passwords=yes

[data]
path=/data
browsable=yes
writable=yes
public=yes
```

When you would like to share data with user based authentication, means before accessing the data should ask for samba user and password. You should use the user in security type.

smb passwd file represents where to store the username and password of samba user. Passwords should sent on encrypt format or not define by encrypt passwords options.

Now you need to create the samba user

```
#smbpasswd -a user1 : It will create the user1 as a samba user and stores the username and password into the file as defined in smb passwd file directives.
```

Just restart the smb service.

```
#service smb start | restart
```

Go to windows system and access the shared from linux using linuxserver netbios name. When you try to access it ask for username and password of linux server.



Some other important options

- i. `hosts allow = 172.24. 192.168.0` : Define which hosts can access the share.
- ii. `valid users= user1 user2` : Define Which user can access this share
- iii. `read only` : Whether share the data read only mode or not
- iv. `write list` : Which user or group can access in read and write mode even data shared in read only mode.

Example:

```
#vi /etc/samba/smb.conf
[global]
netbios name=linuxserver
workgroup=mygroup
server string=sharing from linux server
security=user
smb passwd file=/etc/samba/smbpasswd
encrypt passwords=yes
hosts allow= 172.24. 192.168.0.
[data]
path=/data
browsable=yes
writable=yes
public=yes
valid users=user1

[data1]
path=/data1
browsable=yes
writable=no
write list=user2 @training

[data2]
path=/data2
browsable=yes
writable=no
hosts allow=172.24
```

RH302

```
# service smb restart
```

Login in Windows system and access from Network Places or go to the run and type [\\linuxserver](http://linuxserver)

www.testking.com

Sharing User's Home Directory

SMB can use for user authentication also, if you are using samba domain user's home directory should access from the client machine.

Example

```
#vi /etc/samba/smb.conf
[global]
netbios name=linuxserver
workgroup=mygroup
server string=sharing from linux server
security=user
smb passwd file=/etc/samba/smbpasswd
encrypt passwords=yes

[homes]
public=no
browsable=yes
writable=yes

#useradd user1
#useradd user2
#useradd user3
#smbpasswd -a user1
#smbpasswd -a user2
#smbpasswd -a user3

#service smb restart | start
```

Sharing Printer through Samba

Samba also helps to share the printer connected in linux server.

```
#vi /etc/samba/smb.conf
[global]
netbios name=linuxserver
workgroup=mygroup
security=share
printing=cups
printcap name=/etc/printcap
load printers=yes
```

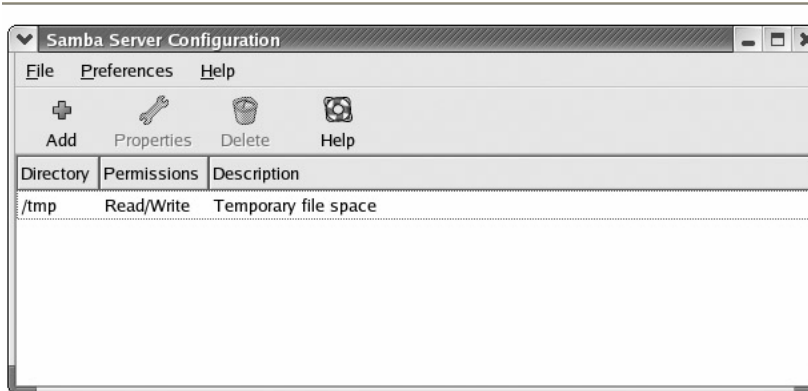
```
[printes]
path=/var/spool/samba
public=yes
browsable=yes
writable=no
printable=yes
```

printing define the software used to print the document.
/etc/printcap file maintains all printer named installed on local system.

Printers is the predefined tag which represents all installed printer. /var/spool/samba is the spooling directory.

There is tool name **testparm**, which checks the syntax of /etc/samba/smb.conf.

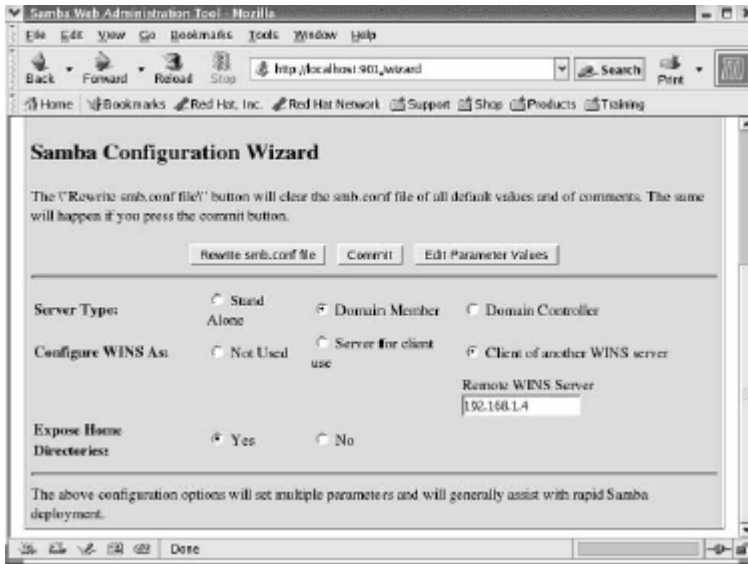
If you would to like to configure the SAMBA server using Redhat GUI Version tool
 #system-config-samba



Similarly you can configure samba server through browser called samba swat. Open browser and type <http://localhost:901>



Samba Swat Configuration window

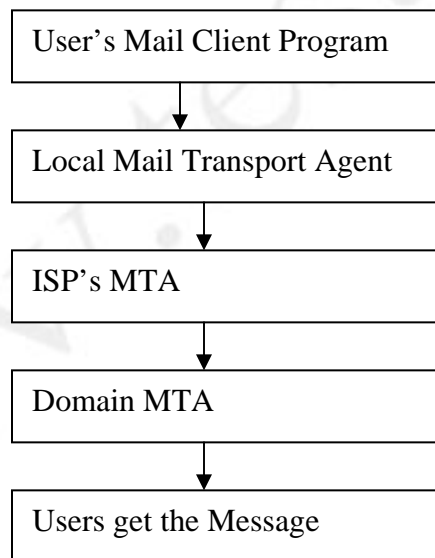


Sendmail Server

Sendmail is the default mail server in Redhat Enterprise Linux 5 having lots of features.

- It routes mail in different types addresses
- Supports for virtualdomain as well as virtual users
- Can Masquerade Email Addresses
- Automatically retry for failed email
- By Default allows connections only from localhost
- Rejects mail from unresolvable domain
- Anti-Spam Features added

Here is the overview of Email transfer



When user sends the message using Mail Client program like kmail, Evolution Mail. Mail will send to Local Mail Transport Agent. Local Mail Transport Agent uses the Multiple MTA in between the source MTA and Destination MTA. ISP's MTA search the domain mail exchanger of destination domain. Then ISP's MTA and Destination MTA start the negotiation to establish the connection. After Completing the Negotiation connection will established and according to the Administrator's policy mail will accept or reject by the destination MTA.

For Sendmail you need to install

- i. sendmail
- ii. sendmail-cf
- iii. dovecot

In RHCE exam you need to configure the basic mail server.

Some Important Files needs to remember

- i. **/etc/mail/sendmail.cf** : It is the main sendmail configuration file, which is read by sendmail service. This file is the Micro 4 Language's output generated using sendmail.mc file.
- ii. **/etc/mail/sendmail.mc** : It is the file used to configure the mail sendmail configuration file. It

is in readable format. Whatever you made changes you need to generate sendmail.cf file.

- iii. **/etc/mail/access** :It is the file to allow or deny mail coming from host, network, domain or mail address.
- iv. **/etc/mail/virtusertable** : This file helps to map the virtual address into the real address.
- v. **/etc/mail/local-host-names** : It contains the list of domains to accept the mail coming for.
- vi. **/etc/aliases** : This file is used to alias the email address.
- vii. **/etc/dovecot.conf** : It is the dovecot configuration file used to enable imap, imaps, pop3, pop3s protocols.

Let's go to configure the mail server

Suppose I'm going to configure the mail server for example.com domain. I specified that mail exchanger of example.com domain is mail.example.com associated IP 192.168.0.5. Yes I'm doing on mail.example.com host.

- i. vi /etc/mail/local-host-names
example.com
- ii. vi /etc/mail/sendmail.mc
dn1 DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
- iii. m4 /etc/mail/sendmail.mc >/etc/mail/sendmail.cf
- iv. vi /etc/mail/access

```
192.168.0 ACCEPT
v.    vi /etc/dovecot.conf
      protocols = imap imaps pop3 pop3s
v.    service sendmail start
vi.   service dovecot start
```

I'm here going to configure the mail server for example.com domain so I should specify the domain name to which mail coming accept by this host.

I already wrote that by default sendmail server accept the connection only from localhost. Now need to allow the smtp or pop connection from other hosts also so I comment the line containing to allow only to localhost using dnl word. sendmail.mc is the main user configuration file written in Micro 4 Language where dnl comment the line. After changing the configuration of sendmail.mc file needs to create sendmail.cf using m4 because sendmail server reads the sendmail.cf file.

Access file define to accept or reject mails coming from;

```
192.168.0      ACCEPT
192.168.1      REJECT
@cracker.org   REJECT
nobody@       REJECT
user1@yahoo.com ERROR:550 Invalid Email Address
```

Here you can define which mail accept or reject coming. In Above example mail coming from 192.168.0 network accepts, coming from 192.168.1 network rejects, mail from cracker.org domain rejects, any mail coming having nobody

RH302

in email address rejects . Using ERROR:550 error Code you can display user define error message.

By default dovecot start the imap protocol if you want to start pop protocol you should write in dovecot configuration file /etc/dovecot.conf.

```
# vi /etc/dovecot.conf
protocols = imap imaps pop3 pop3s
#service dovecot start | restart
```

Let's go to map the virtual address into real address.
/etc/mail/virtusertable file is used to map the virtual address into the real address.

```
@abc.com          user1
info@xyz.com     user2
admin@testking.com user3
```

In above example, mail coming for any user of abc.com domain will send to user user1, mail coming to info@xyz.com will send to user2 and mail coming to admin@testking.com to user3.

Aliasing Real Address to Read Address

Suppose you are working as a Administrator in abc.com and there are two employee having user1 and user2 username. When user user1 absent user2 will handle all user1's responsibilities, now you should forward all mails coming to user1 to user2.

Yes for this there is a file /etc/aliases, from this file we can alias the user.

User1: user2 : All mail coming to user user1 will send to user user2. But remember that after changing the configuration of aliases file needs to generate the database file aliases.db using **newaliases** command.

After Configuring mail server, you can directly send or check the mail by login into the mail server in 25 and 110 ports. 25 port is used by SMTP (Simple Transfer Protocol) and 110 is used by POP3 (Post Office Protocol).

Example of login into mail server in SMTP port.

```
#telnet mail.example.com 25
helo mail.example.com
mail from: user1@example.com
rcpt to: user2@example.com
data
Hello user2
.
quit
```

Yes SMTP protocol is used to send the message so I shown you the example of sending mail from SMTP port. Let's go to check the mail via pop port.

```
# telnet mail.example.com 110
user user1
pass mypassword
stat
top 1 123 (Give the value of stat output)
quit
```

Let's Go with sendmail.mc more options

This is the main configuration file for sendmail server program. Here `dnl` is comment and parentheses starts with back quote and end with single quote.

The following include command adds the `cf.m4` command as a macro processing prototype; by default, it requires installation of the `sendmail-cf-*` RPM.

So every time when you make changes into `sendmail.mc` file needs to generate `sendmail.cf` file using `m4` command.

```
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
```

Local Version associated with installed sendmail server

```
VERSIONID(`setup for Red Hat Linux ')dnl
```

```
CONFIGURING SENDMAIL 597
```

```
Defined the OS type.
```

```
OSTYPE(`linux')dnl
```

Write the next mail server name to forward all outgoing mail. Generally this is the Mail server of your ISP.

```
dnl define(`SMART_HOST', `smtp.your.provider')
```

Defined the database name containing the list of black listing.

```
FEATURE(`access_db',`hash -T<TMPF> -  
o/etc/mail/access.db')dnl  
FEATURE(`blacklist_recipients')dnl
```

If the root user tries to log in, the EXPOSED_USER command requires the full e-mail address.

```
EXPOSED_USER(`root')dnl
```

The LOCAL_DOMAIN command specifies an alias for the local computer; localhost.localdomain is a default alias in /etc/hosts.

```
LOCAL_DOMAIN(`localhost.localdomain')dnl
```

MASQUERADE_AS changes the domain to all outgoing mails.

```
MASQUERADE_AS(`testking.com')dnl
```

```
dnl # masquerade not just the headers, but the envelope  
as well
```

```
dnl #
```

```
dnl FEATURE(masquerade_envelope)dnl
```

```
dnl #
```

```
dnl # masquerade not just @mydomainalias.com, but  
@*.mydomainalias.com as well
```

```
dnl #
```

```
dnl FEATURE(masquerade_entire_domain)dnl
```

```
dnl #
```

RH302

using MASQUERADE_DOMAIN you can masquerade to multiple domains with same.

```
dn1 MASQUERADE_DOMAIN(localhost)dn1
dn1 MASQUERADE_DOMAIN(localhost.localdomain)dn1
dn1 MASQUERADE_DOMAIN(abc.com)dn1
dn1 MASQUERADE_DOMAIN(example.com)dn1
```

Apache overview

Apache web server is the most widely used http daemon based web server. Which provides the secure as well as non-secure contents transfer between client and server using http or https protocols. Apache loads lots of modules dynamically to interpret the CGI, Perl, PHP etc scripts on browser.

```
LoadModule access_module modules/mod_access.so
LoadModule auth_module modules/mod_auth.so
LoadModule auth_anon_module modules/mod_auth_anon.so
LoadModule auth_dbm_module modules/mod_auth_dbm.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule ldap_module modules/mod_ldap.so
LoadModule auth_ldap_module modules/mod_auth_ldap.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule env_module modules/mod_env.so
LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule cern_meta_module modules/mod_cern_meta.so
LoadModule expires_module modules/mod_expires.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule headers_module modules/mod_headers.so
LoadModule usertrack_module modules/mod_usertrack.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule mime_module modules/mod_mime.so
LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule asis_module modules/mod_asis.so
```

```
LoadModule info_module modules/mod_info.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule dir_module modules/mod_dir.so
LoadModule imap_module modules/mod_imap.so
LoadModule actions_module modules/mod_actions.so
LoadModule speling_module modules/mod_speling.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module
modules/mod_proxy_connect.so
LoadModule cache_module modules/mod_cache.so
LoadModule suexec_module modules/mod_suexec.so
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule file_cache_module modules/mod_file_cache.so
LoadModule mem_cache_module modules/mod_mem_cache.so
```

/etc/httpd is the root directory of httpd service,
/etc/httpd/conf/httpd.conf is the main configuration file
for http service.

By default httpd service runs under the ownership of apache
user and apache group on port 80.

User apache

Group apache

```
# Change this to Listen on specific IP addresses as shown  
below to
```

```
# prevent Apache from glomming onto all bound IP addresses  
(0.0.0.0)
```

```
#
```

```
#Listen 12.34.56.78:80
```

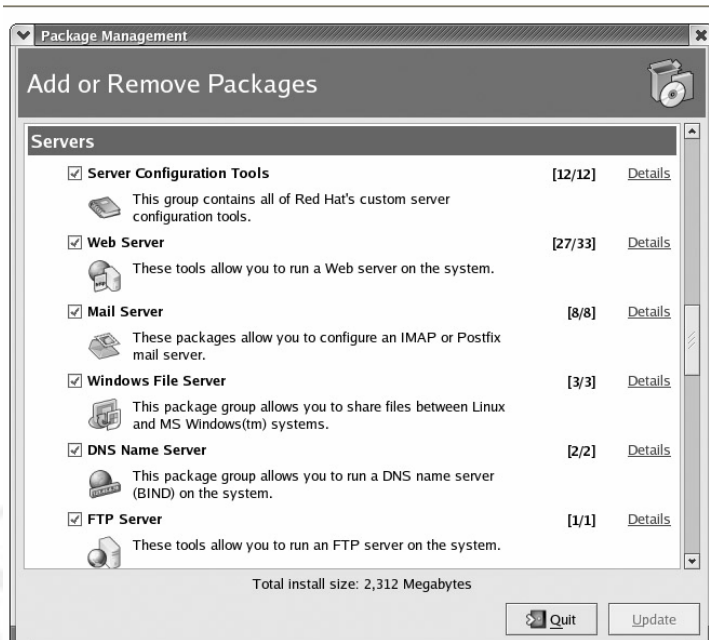
```
Listen 80
```

Installing http service

```
# rpm -ivh httpd-*
```

Or

```
#system-config-packages -tree=/var/ftp/pub
```



/var/www/html is the default directory if you would like to change the default change

```
<Directory "/var/www/html">  
in /etc/httpd/conf/httpd.conf file.
```

By default DirectoryIndex is index.html or index.html.rar

```
DirectoryIndex index.html index.html.var
```

Similarly AccessFileName is .htaccess

```
AccessFileName .htaccess
```

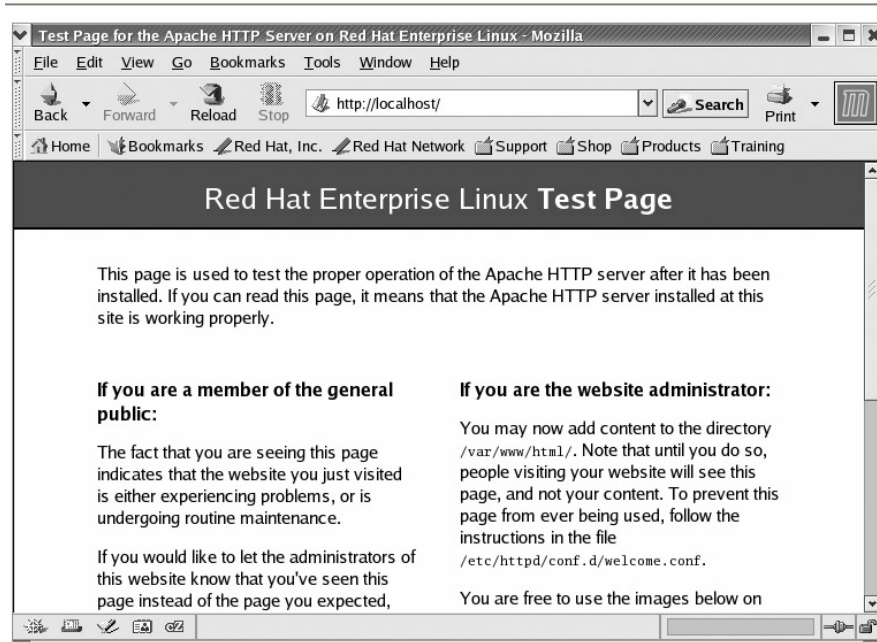
Starting httpd service

```
#service httpd start
```

```
#chkconfig --level 35 httpd on
```

1. Setting Default Page for http service

When you test the http service through browser by typing <http://localhost>, it will display message page.



To change the default page

```
#cd /var/www/html
#cat >index.html
<html>
<head>
<title>:::test page for localhost:::</title>
</head>
<body>Test page</body>
</html>
```

Now Open the browser and type <http://localhost> you will get you index.html page.

We can Configure the apache web server for web site either one site one ip or by sharing the IP Address means multiple web site on single IP Address.

2. Apache configuration for IP based web site
Before starting this First fully configured the DNS.

```
# vi /etc/httpd/conf/httpd.conf
<VirtualHost 192.168.0.3>
ServerName www.example.com
DocumentRoot /var/www/example
ServerAdmin admin@example.com
DirectoryIndex index.html index.php
</VirtualHost>
#service httpd restart | start
#links http://www.example.com
```

Virtualhost maps the virtual directory into the real path. Servername define the service name for virtualhost. DocumentRoot directives defines the path of document for web site. ServerAdmin is the email address to mail when error occurred on server. DirectoryIndex directives defines the default page for the web site.

You can Access the web site either using GUI browser or console browser.

Links is the console based browser.

3. Example of Configuring Apache webserver for Name based web site

If you want to host multiple web site on single IP Address. Example www.example.com as well as www.abc.com are associated in 192.168.0.3.

```
#vi /etc/httpd/conf/httpd.conf
NameVirtualHost 192.168.0.3
<VirtualHost www.example.com>
ServerName www.example.com
ServerAdmin admin@example.com
DocumentRoot /var/www/example
DirectoryIndex index.html index.htm index.php
</VirtualHost>

<VirtualHost www.abc.com>
ServerName www.abc.com
ServerAdmin admin@abc.com
DocumentRoot /var/www/abc
DirectoryIndex index.html index.htm index.php
</VirtualHost>

#service httpd restart
#links www.example.com
#links www.abc.com
```

4. virtual Hosting with User based Authentication

Apache server supports the virtualhost configuration with user based authentication.

I'm going to show you the example that www.example.com should be able to access by the http users created in web server.

```
# vi /etc/httpd/conf/httpd.conf
<VirtualHost 192.168.0.3>
  ServerName www.example.com
  DocumentRoot /var/www/example
  <Directory /var/www/example>
    AllowOverride Authconfig
  </Directory>
  ServerAdmin admin@example.com
  DirectoryIndex index.html index.htm index.php
</VirtualHost>
```

You should use the Directory directives to define the path of directory.

Now Create the Access File in directory defined in directory directives in Virtualhost.

```
#cd /var/www/example
```

```
#vi .htaccess
AuthName "Only to Authorized Users"
AuthType      basic
AuthUserFile  /etc/httpd/conf/mypasswd
Require       valid-user

# htpasswd -c /etc/httpd/conf/mypasswd user1
# htpasswd -m /etc/httpd/conf/mypasswd user2
#chgrp apache /etc/httpd/conf/mypasswd
#chmod g+r /etc/httpd/conf/mypasswd
#service httpd restart
```

For User based Authentication you need to create the .htaccess file by defining Authentication dialog message, authentication type, file stores the http user name and password and required to authenticate.

htpasswd command creates the http user and ask for password. I already told you that httpd server runs under the ownership apache user and group so need to change the ownership and set the read only permission to group.

When you access the www.example.com website, it asks for the username and password.



5. Virtual Hosting with Host based Authentication

I shown you the example of user based authentication, now going to configure which host or network can access the web site or deny to which site.

```
# vi /etc/httpd/conf/httpd.conf
<VirtualHost 192.168.0.3>
ServerName www.example.com
DocumentRoot /var/www/example
ServerAdmin admin@example.com
<Directory /var/www/example>
Order Allow, Deny
Allow from .example.com
</Directory>
DirectoryIndex index.html index.htm index.php
</VirtualHost>

#service httpd restart
```

To allow or deny to host you can use order allow, deny or deny, allow.

Order allow, deny : Explicit Allowed to clients specified in allow from and deny everyone else.

Order deny, allow : Explicit denied to clients specified in deny from and allow everyone else.

In Above example allowed to all member of example.com domain and deny to everyone.

6. Configuring Apache Web server to execute CGI Scripts

You should create your own scriptAlias directory for CGI Scripts and needs to place all CGI scripts on aliases directory.

```
# vi /etc/httpd/conf/httpd.conf
```

```
<VirtualHost 192.168.0.3>
```

```
ServerName www.example.com
```

```
DocumentRoot /var/www/example
```

```
ServerAdmin admin@example.com
```

```
DirectoryIndex index.html index.htm index.php
```

```
ScriptAlias /cgi-bin/ /var/www/example/cgi-bin/
```

```
</VirtualHost>
```

```
# mkdir /var/www/example/cgi-bin
```

```
#cd /var/www/example/cgi-bin
```

```
#vi test.sh
#!/bin/bash
echo Content-Type: text/html
echo "Hello RHCE Guys"
#chmod a+x test.sh
#service httpd restart
```

Now your CGI scripts is ready to execute

```
#links www.example.com/cgi-bin/test.sh
```

7. Configuring Secure HTTP

Apache web server provides feature of secure http by loading the mod_ssl.so module. By default communication using the http protocol is plain text format so there is solution of make encrypted communication using apache web server by configuring https. https protocol uses 443 tcp port.

Encryption is based on either RSA or DSa algorithm. Private kets, self-signed certificates or certificate signature requests can be generated using the openssl utility.

/etc/httpd/conf/ssl.key/server.key is the private key file and **/etc/httpd/conf/ssl.crt/server.crt** is the self singed certificate.

/etc/httpd/conf.d/ssl.conf is the main SSL configuration file.

```
# vi /etc/httpd/conf.d/ssl.conf
<VirtualHost 192.168.0.3>
ServerName www.example.com
DocumentRoot /var/www/example
DirectoryIndex index.html
serverAdmin admin@example.com
SSLEngine on
SSLcertificateFile
/etc/httpd/conf/ssl.crt/server.crt
SSLcertificateKeyFile
/etc/httpd/conf/ssl.key/server.key
</VirtualHost>
```

Now you need to create the certificate file and key file. In Redhat Enterprise Linux already pre-configured MakeFile is stored in /etc/httpd/conf or /usr/share/ssl/certs directory. Now you need to just use the make command.

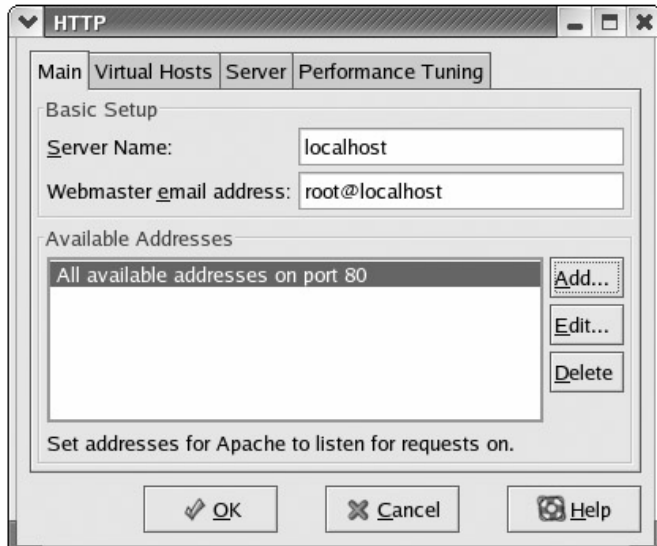
```
#cd /etc/httpd/conf
#make testcert
#service httpd restart
```

Open the Browser and type <https://www.example.com> now you will get the signed certificate.

There is GUI version of Redhat's http configuration tool:

Leading the way in IT testing and certification tools, www.testking.com

#system-config-httpd



Squid Server

Squid is the internet cache proxy server for FTP, HTTP and other clients request. Squid supports FTP, HTTP as well as SSL and other protocols.

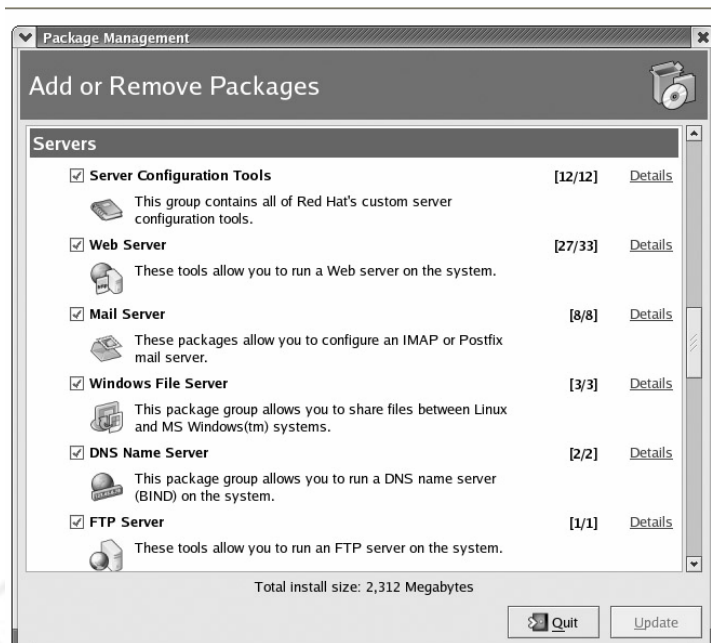
Installing Squid

/etc/squid/squid.conf is the main squid configuration file provides by squid rpm package.

```
#rpm -ivh squid-*
```

or

```
#system-config-packages -tree=/var/ftp/pub
```



In Redhat Enterprise Linux you need to know the basic configuration to run squid proxy server.

Leading the way in IT testing and certification tools, www.testking.com

1. Port : by default squid runs on port 3128, you can change that port using http_port directives
http_port 8080 : It runs the squid on 8080 port
2. ACL You Need to create the Access Control List to make allow or deny the Internet Access.

```
acl mynet src 192.168.0.0/255.255.255.0  
acl denynt src 192.168.1.0/255.255.255.0  
acl blocksite dstdomain .yahoo.com
```

These ACL define certain Network or domain name. src acl type defines source from , dstdomain define the destination domain.

After Creating ACL, you need to either allow or deny.

```
http_deny deny blocksite  
http_access allow mynet  
http_access deny denynt  
  
#service squid start | restart  
#chkconfig squid on
```

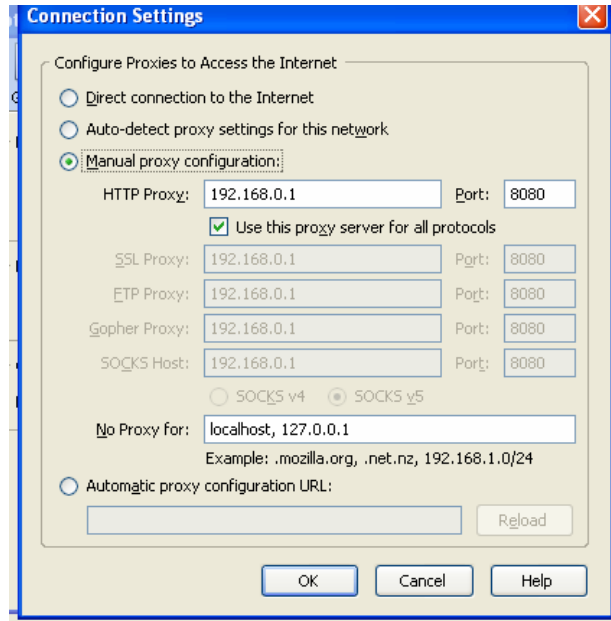
Proxy Configuration in Client

After Configuring the squid proxy server you need to set the proxy information in client browser.

- Open the Firefox browser

Leading the way in IT testing and certification tools, www.testking.com

- Click on Edit→Preferences
- Click on General
- Click Connection Settings
- Select Manual Proxy Configuration
 - Type Proxy address and port number running on.



NIS (Network Information Services)

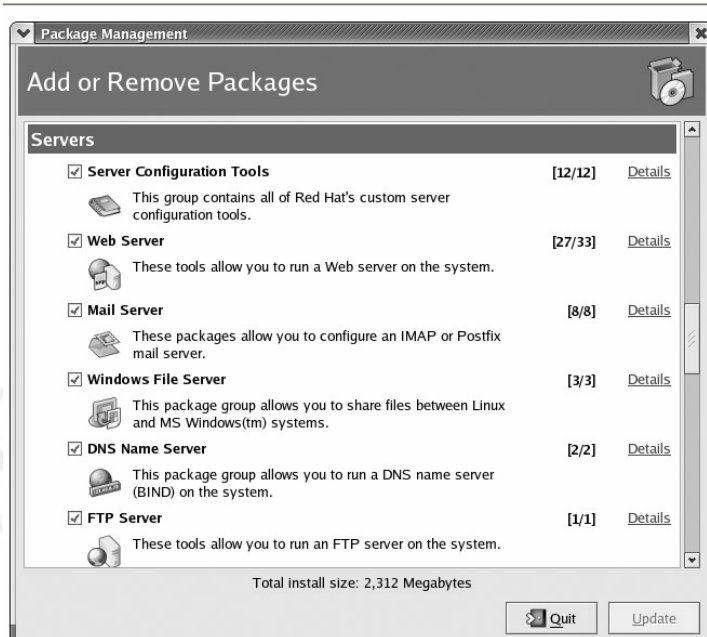
NIS is the traditional directory services for centralized authentication developed by Sun Micro Systems. Still it is used as a standard authentication method in Linux.

In Network environment one server can be Master NIS and more than one can be slave NIS servers. Master NIS is the server having all original configuration and information but slaves are called the backup of master.

You need to Install `ypserv`, `ypbind` and `yp-tools` rpm packages for NIS server.

Another way install using Redhat's GUI package management tool `system-config-packages`.

```
#system-config-packages --tree=/var/ftp/pub
```



- Click on Network Servers group and select ypserv.

Here I'm going to configure nis1.example.com as a master NIS server and nis2.example.com as a slave NIS server.

Configuring NIS Master Server

1. You need to set the domain name

```
#domainname example.com  
#vi /etc/sysconfig/network  
NISDOMAIN=example.com
```

You know domainname command displays or sets the domain for current session. If you would like to set permanently use the NISDOMAIN directives in /etc/sysconfig/network file.

2. vi /var/yp/MakeFile

Here I'm Going to Configure Master as well as Slave NIS Servers so if you have only master server you can set NOPUSH=true but if you have Master as well as slave server, you need to set NOPUSH=false.

```
NOPUSH=false
```

Now set the parameters to map with client.

```
all: passwd group hosts # rpc services ..
```

I set comment after hosts because I would like to map only passwd , group and hosts information.

Now you need to publish the maps information into directory. MakeFile is the preconfigured file, just make simple changes you need to publish on directory using make command.

3. cd /var/yp

```
# make
```

After successfully running make command check in /var/yp/ there you will get the directory same name as domain.

4. Start the ypserv and yppasswdd service

```
# service ypserv start  
#service yppasswdd start  
# service portmap restart
```

NIS also RPC services so it required portmap service.

5. Now define all NIS servers in Master Server

```
# /usr/lib/yp/ypinit -m
```

It will ask for the NIS server

Next host to add: nis1.example.com

Next host to add: nis2.example.com

Just Type all your slave NIS server name and press ctrl-D

6. Start the services

```
# service ypserv restart
```

```
# service yppasswdd restart
#service portmap restart
```

Now your NIS Master Server is ready. Let's go to configure NIS slave in nis2.example.com.

1. You need to set the domainname

```
domainname example.com
```

```
# vi /etc/sysconfig/network
    NISDOMAIN=example.com
```

2. /usr/lib/yp/ypinit -s nis1.example.com

I already told to you that Slave server is backup of master nis server, when you run this command, it will copy all information published in directory from master server.

3. Start the services

```
#service ypserv start
#service yppasswdd start
#service portmap restart
```

Sharing User's Home Directory

NIS only authenticate to users but when user login into client machine, user require user's home directory. So First you need to share user's home directory from server.

```
#vi /etc/exports
/rhome *.example.com(rw, sync)
```

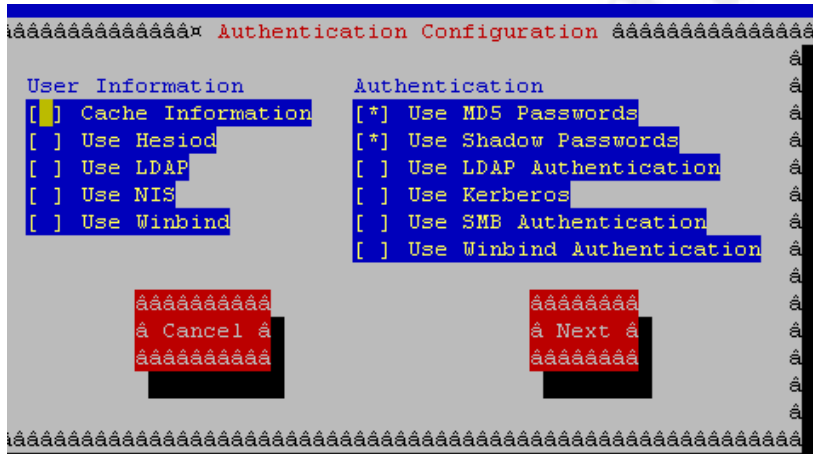
Here all remote users home directory are created into /rhome so I shared this directory.

```
#service nfs start
#service portmap restart
```

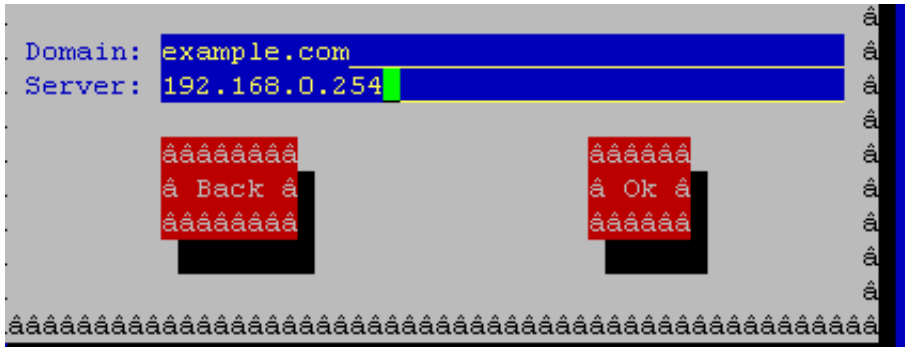
NIS Client

In client machine :

a. Type `authconfig` or `system-config-authentication` command



- f. Select on use NIS then click on Next
- g. Type Domain : example.com
- h. Server : 192.168.0.254



i. Click on ok

It means users are authenticated from the NIS server 192.168.0.254. When user login on your Client machine, home directory should present in logged on system.

I already written about the Automount feature. We can mount the user's home directory in client machine to make present user's home directory.

a. **mkdir /rhome**

b. **vi /etc/auto.master**

```
/rhome /etc/auto.home --timeout=60
```

This line specify the mount point by reading /etc/auto.home as well as unmount the /nisusers if user doesn't use within 60 seconds.

c. **vi /etc/auto.home**

```
* -rw,soft,intr 192.168.0.254:/rhome/&
```

Which line specify to mount all the contents of /rhome directory from server.

- f. service autofs restart : autofs service controls the auto mount feature of linux system. After changing configuration, need to restart the autofs service.
- g. Now login as server's users.

System Security

Pluggable Authentication Modules

Redhat Enterprise Linux uses PAM (Pluggable Authentication Modules) to authenticate to users by loading modules from /lib/security.

I would like to go by example of authentication,
#touch /etc/nologin

When you create this blank file, when users try to login locally on this machine, it denies.

Similarly I commented the tty2 in /etc/securetty file, when root try to login in terminal 2 it denies to login.

What will checks this ?? PAM yes PAM's modules checks this all things you can modify the configuration as per you needs.

Pam_nologin.so modules check whether /etc/nologin file is created or not, pam_securetty.so module checks which terminal are available to login to root user.

/lib/security: This directory contains list of pam modules

/etc/pam.d/ : This directory contains list of pam applications

/etc/security/ : This directory contains list of security configuration files, which reads by pam modules.

When you read the file /etc/pam.d/login

<i>Tests</i>	<i>Control Values</i>	<i>Modules and parameters</i>
Auth	required	pam_securetty.so
Auth	required	pam_nologin.so
Etc.		

PAM uses different types of methods to authenticate to users.

Tests:

Auth: Authentication Management , whether to prompt for a username and or a password.

Account: Account Management , it may deny access according to time, password expiration, or a specific list of restricted users.

Password : password management , It may ask for password to allow or deny the access.

Sessions : Checks whether user's session is running to not.

Control Values

Required : If the module works, the command proceeds. If it fails, go to the next command in the configuration file but result is already determined that should fail.

Requisite: Same as Required but It stops of checking other modules when one return fail result.

Sufficient: If the module works, the login or other authentication proceeds.

Optional: Ignore to PAM result either pass or faile.

PAM configuration for Time based login

PAM has the capabilities to control the users to login at any time. Using PAM can define the time for user to allow login.

For this you need to configure `/etc/security/time.conf` file, this file is checks by `pam_times.so` module.

`/etc/security/time.conf` the main configuration file for time based authentication using PAM.

This file has the syntax of:

Services:terminals:users:times

Generally services represent the pam services, terminals represents the name of terminal, users means name of user and times allowed time to run program.

Time can write Su, Mo, Tu, We, Th, Fr, Sa, Wk, Wd, Al

`login;*;user1;Al0900-1730`

This example allow login to user user1 between 9 am to 17:30pm

`Login;*;user2;SuMo1200-1400`

This example allow log to user user2 between 12pm to 14 pm.

Time.conf file is reads by `pam_time.so` but you need to call either in `login` or `system-auth` pam file.

`#vi /etc/pam.d/login`

account required /lib/security/pam_time.so

PAM configuration for Origin based login

Another way of controlling to users is allowing or deny login on certain hosts. PAM can do this.

/etc/security/access.conf is the main configuration file for origin based authentication. It has following syntax:

permission:users:origins

In Permissions either + or - can use where + allow to access and - deny to access. Second field contains the list of users either to allow or to deny and origins represents which terminal or host. Here you can user ALL and EXCEPT operator.

-:ALL EXCEPT root: LOCAL

This example deny to all users login locally except root user.

-:user1 : ALL EXCEPT tty5

This example deny to login in all terminals except tty5.

-:nisuser1:ALL EXCEPT station1.example.com

This example deny to login in all hosts except station1.example.com

Access.conf file is read by pam_access.so module. So you need to call this module.

```
#vi /etc/pam.d/login  
account required /lib/security/pam_access.so
```

Limiting Number of Processes and Logins

PAM also can control the number of logins to user, group members as well as can control number of processes can run by users.

```
# vi /etc/security/limits.conf  
user1 hard nproc 5  
@training - maxlogins 10  
user2 - maxlogins 1
```

Here user user1 can run maximum process 5, training group members maximum can login 10, user user2 can login one at a time.

This configuration file is read by pam_limits file.

```
# vi /etc/pam.d/system-auth  
session required /lib/security/pam_limits.so
```

www.testking.com

Securing Services: Using TCP Wrappers

TCP wrappers can control some services which is compiled with libwrap.so modules. Some services has their own mechanism to control the hosts like http, samba etc services.

But some services mail, ftp, sshd etc doesn't have it's own security mechanism to control hosts. So These services can control by TCP Wrappers.

TCP Wrappers can control these services:

Sendmail

Sshd

Vsftpd

Stunnel,

Gdm

Nfs

Portmap

Sladp

Dovecot

All xinetd based services

TCP wrappers uses main two files /etc/hosts.allow and /etc/hosts.deny.

Client Validating process by TCP wrappers

When client request for certain services it checks first in /etc/hosts.allow whether client is listed or not if listed explicitly allowed to access the service. If not listed then checks the /etc/hosts.deny file if client list in matched in hosts.deny file then deny to access, if not matched then allow to access the service.

Syntax: services:clients:options

Example:

/etc/hosts.deny

```
Vsftpd: ALL EXCEPT .example.com  
nfs,portmap      :      ALL      EXCEPT      .example.com,  
trusted.craker.org  
sshd:ALL  
dovecot:      ALL      EXCEPT      .example.com      EXCEPT  
station10.example.com
```

You can use the ALL, EXCEPT operator to allow or deny the services. First Example vsftpd allowed to access only from example.com domain, second example allowed to access nfs and portmap from example.com domain and trusted.cracker.org host. Third example deny to login using ssh from any host.

If multiple interface are connected into you machine and wants to allow or deny on interface basis:

sshd@192.168.0.1: ALL EXCEPT .example.com

sshd@192.168.1.1 : ALL

In this example if ssh login to 192.168.0.1 allow from example.com domain but ssh login to 192.168.1.1 deny

Similarly you can set multiple options while allowing or denying.

Example:

```
Sshd: ALL :spawn echo "Someone trying to attack through ssh to %s from %c" | mail -s "Danger" admin
```

By this example, when anyone try to login using ssh into server it will sends the mail to admin user with server (%s) information as well as Client (%c) information.

Securing Xinetd Based services

TCP wrappers can control xinetd based services located in /etc/xinetd.d/ directory. To allow or deny to transient services, you need to know the server program of services.

Here is the output of /etc/xinetd.d/telnet file

```
Service telnet
{
  disable = no
  flags = REUSE
  socket_type = stream
  wait = no
  user = root
```

```
server = /usr/sbin/in.telnetd →server program
name
    log_on_failure +=USERID
    instances = 20
    per_source = 1
}
```

Controlling telnet connection

```
#vi /etc/hosts.deny
in.telnetd: ALL EXCEPT .example.com
```

Similarly xinetd itself has it's own mechanism to control the service.

/etc/xinetd.conf is the global configuration file, if you make any changes on this file, it affects all xinetd based services.

There are three directives to control xinetd based service

```
Access_from = 192.168.0.0/24
No_access = 192.168.0.100
Access_times = 09:39-17:30
```

Controlling Telnet

Here is the output of /etc/xinetd.d/telnet file

```
Service telnet
{
```

```
disable = no
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd →server program
name
log_on_failure +=USERID
instances = 20
per_source = 1
Access_from = 192.168.0.0/24
No_access = 192.168.0.100
Access_times = 09:39-17:30
}
```

It allows telnet connection from 192.168.0.0/24 network except 192.168.0.100 between 9:30 am to 17:30 pm.

Introduction to iptables

Iptables is the default packet filtering tool in Linux, which filter packets based on Layer 2, Layer 3 and Layer 4 of the OSI Model.

There are three table types in iptables

- Filter
- Nat
- Mangle

Filter table is used to filter the packets on the basis of rules and chains, nat is used to translate the Network Address, mangle is the combined features of nat and filter.

Similarly filter uses different chain: INPUT, OUTPUT, FORWARD, POSTROUTING and PREROUTING.

Chain	Tables support
INPUT	Filter, mangle
OUTPUT	Filter, mangle
FORWARD	Filter, mangle
POSTROUTING	Nat, mangle
PREROUTING	Nat, mangle

INPUT: This chain is used to filter the packets coming into the local system. It checks before entering into the system.

OUTPUT: This chain checks the outgoing locally generated packets.

FORWARD: This chain checks the forwarding packets from one network to another network.

POSTROUTING : This chain translate the address after leaving the system.

PREROUTING : This chain Translate the address before entering into the system.

#iptables -L : Default table is filter so it lists the chain as well as rules configured to filter.

#iptables -F : It flush all rules.

#iptables -t nat -L : It displays all Network address translation rules.

Let's go to apply the filter rules, before that you need to know the options used to filter.

-p protocol name (Layer 4)
-i Incoming Interface
-o Outgoing Interface
-s Source Address
-d Destination Address
--sport Source Port
--dport Destination Port

Example:

```
#iptables -t filter -A INPUT -s 192.168.0.100 -p tcp --dport 8080 -j DROP
```

Action can be DROP, ACCEPT, LOG. In above example connection to 8080 port is dropped.

```
#iptables -t filter -A INPUT -s ! 192.168.0.0/24 -p  
tcp -dport 20 -j DROP
```

It deny the ftp connection from outside the 192.168.0.0/24 network.

```
#iptables -t filter -A OUTPUT -d 192.168.1.1 -p  
tcp --dport 23 -j DROP
```

Which drops the telnet connection to 192.168.1.1 from local system

```
# iptables -t filter -A FORWARD -s 192.168.0.10 -d  
192.168.1.10 -p tcp --dport 25 -j DROP
```

Order of checking rules

iptables checks the rules from the top, when one rule match it apply. When rule doesn't match it apply the chain policy.

You can configure the chain using

```
#iptables -P INPUT DROP
```

It set the policy of INPUT chain drop.

After applying your own rules and chain policy you need to save into files to apply automatically at next reboot.

```
#service iptables save
```

it will save your rules and policy configuration into /etc/sysconfig/iptables file.

```
# iptables -F : It flush all rules
```

NAT (Network Address Translation)

Nat allows to translate from private ip to public, so it make possible to access the public network as well as it hides the internal IP Address.

Using NAT we can configure for SNAT (Source NAT) as well as Destination NAT (DNAT).

SNAT: Which allows to change the source address, suppose I my Linux server is connected to ISP using leased line so I got public IP 202.2.2.2, which is connected to eth0 and another eth1 device connected to my local LAN having IP 192.168.0.1. Now to share Internet either I should configure Proxy server or share through SNAT. When packets comes from private LAN SNAT changes the source Address to 202.2.2.2 and make possible to access the internet.

```
# iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j SNAT  
--to-source 202.2.2.2
```

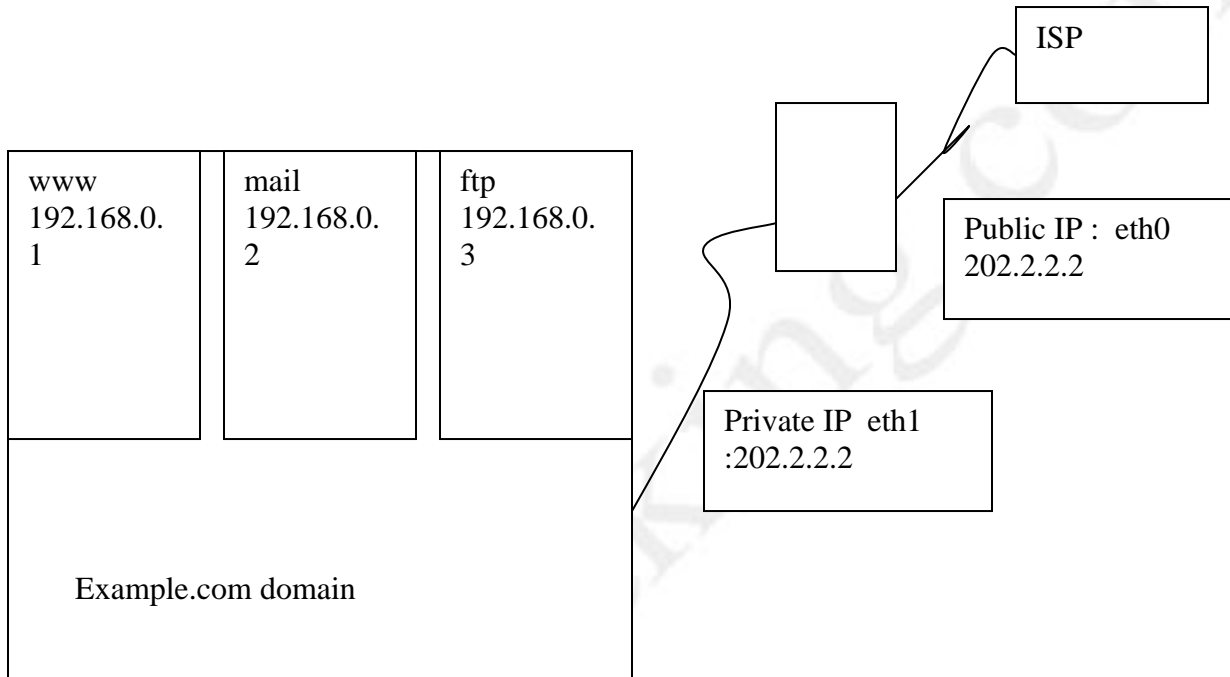
Similarly you can use MASQUERADE if you would like to translate the address into whatever assigned into device.

```
#iptables -t NAT -A POSTROUTING -o eth0 -j MASQUERADE
```

If ip dynamically changing into eth0 interface Masquerading is good.

DNAT

Destination NAT Allows to change the destination address.



When request for www.example.com comes in my Internet server I should redirect to 192.168.0.1. Yes this is DNAT, client request comes as a destination to 202.2.2.2 but I have to redirect into another host.

```
#iptables -t nat -p tcp --dport 80 -j DNAT --to-destination 192.168.0.1
```

```
#iptables -t nat -p tcp --dport 20 -j DNAT -to-destination 192.168.0.2
```

RH302

***Good Luck**

www.testking.com