STANSYS
SOFTWARE SOLUTIONS
Training | Consulting | Development

Linux Admin

Hi,

Greetings from **Stansys Software Solutions**,

Stansys Software Solutions is a premier **IT Training, Consulting and Development** Company located at Hyderabad, Mumbai & Bangalore – India. Providing quality Classroom Trainings, Corporate Trainings and Online trainings on **UNIX/LINUX ADMINISTRATION**, SAS & SAP modules with **live setup**.

STANSYS SOFTWARE SOLUTIONS is one of the best **Linux administration** training institutes in India.

STANSYS SOFTWARE SOLUTIONS

#7-1-621/113(67/3RT), Beside: Nagarjuna Jr.College, Near: S.R.Nagar Community Hall, S.R.Nagar, Hyd-38|Ph:8143408688|9542195422|www.stansys.co.in|stansys.linux@gmail.com

Linux syllabus

UNIX/LINUX Basics(EX200):

- **Overview of UNIX**
- **History of Linux**
- **Linux architecture:**
  - Kernel
  - Shell
- **Understanding Linux commands:**
  - Displaying system date and time : date
  - Displaying present and working users : who and whoami
  - Calculator : bc
  - Machine characteristics : uname
  - Displaying a message : echo and printf
- **Files system:**
  - Linux file Hierarchy Concepts
  - Listing files and directories : ls
  - More and less command
  - Creating and viewing the files : cat
  - Create, Modify, Change and Removing directories
  - Moving and renaming files : mv
  - Copying a files : cp command with attributes
  - Links – Hard Link and Soft Link
  - Absolute path name
  - Relative path name
- **Comparisons:**
  - Cmp
  - Diff
- **Compressions:**
  - zip
  - compress
  - gzip
  - bzip2
- **File attributes:**
  - chmod
  - chown
  - chgrp
- **Filter commands:**
  - which, whereis, locate
  - find commands with attributes

- **String Processing:**
  - head, tail
  - wc, sort, uniq
  - cut, paste
- **String Processing with regular expressions:**
  - sed
  - grep
- **System Monitoring:**
  - introduction Process concepts
  - process basics
  - process commands
- **System Automation:**
  - at, batch, cron
- **Shell:**
  - Configuring shell
  - Variables
    - Local variable
    - Environment Variable
- **Shell startup scripts:**
  - Login shell
  - Non – Login shell
- **Vi editor:**
  - Overview of vi editor
  - Three modes of vi editor
  - Saving and quitting
  - Navigation
  - Editing a text
  - Undoing changes
  - Yank and paste
  - Changing, Deleting
  - Searching for pattern
  - Search and Replace

System Administration:

- **RedHat installation(Text and Graphical Mode):**
  - Standalone Installation
  - Network installations(Kickstart)
- **User and Group Management:**
  - Creation of users and Groups
  - Understanding /etc/passed,/etc/group,/etc/shadow and /etc/gshadow
  - Switching accounts :su
  - Password aging policies
  - Creation of quotas for users,groups and files systems

- **Disks and Partitioning:**
  - Managing partitions
  - Understanding file systems
  - Creating file system ext2,ext3 and ext4
  - Reverting file systems
  - Making a swap partition
  - Making a File Swap
  - Understanding virtual file system
    - /proc
  - Managing a data with mount command
    - Mounting File system
    - Mounting CD/DVD's, USB, and Floppys.
  - Understanding and Configuring /etc/fstab and /etc/mtab
  - Using AutoFS Services
- **File systems and Such:**
  - File System Setup
  - Managing File System Quotas
  - File System Security with ACL's
- **System Initialization:**
  - Boot sequence overview
  - Bios initialization
  - Boot loader
    - Grub boot loader and grub.conf configuration file
    - Trouble shooting of grub boot loader
  - Kernel initialization
  - Init initialization
  - Run levels (0-6)
  - Virtual Consoles
  - Controlling services
  - System shutdown and reboot
- **Troubleshooting:**
  - Boot issues
  - Troubleshooting File System
- **Kernel Services:**
  - Kernel overview
  - Kernel hardware support
  - Configuring kernel parameters
  - Kernel upgradation
- **Network Configuration:**
  - Configuring Network Utilities
    - Netconfig, setup, neat and with configuration file
    - Ifdown,ifup, ifconfig,ping
    - Managing services
    - Binding multiple addresses

- **Xinetd services:**
  - overview of xinetd services and non xinted services
  - configuring xinetd services
- **Red Hat Package Manager(RPM):**
  - Overview of RPM
  - Installing, Removing a software with YUM
  - RPM queries
  - RPM verifications
- **Yellow Dog Update Manager(YUM):**
  - Overview of YUM
  - Installing, Removing a software with YUM
  - YUM queries
- **Printing and Administration Tools:**
  - Configuring a standalone printer
  - Configuring a Network printer
    - Cups
- **LVM'S (Logical Volume Manager):**
  - Overview of LVM'S
  - Creation of physical volume
  - Creation of logical partition
  - Extending the Vol group
  - Extending the logical partition
  - Removing Vol group and logical partition
- **Redundant Array of Independent Disks(RAID):**
  - Overview of RAID
  - Types of RAID
  - Configuring RAID 0,1 and 5
- **Backups:**
  - Understanding of different backups
  - Taking backups with dump,cpio,tar

Network administration and Security services(EX300):

- **Networking Basics:**
  - Setting up Networking
  - Troubleshooting Network Connections
  - Advanced Networking
  - Client DNS Troubleshooting
- **Remote Access:**
  - Telnet configuration
  - Secure Shell (SSH)
  - VNC Server configuration
- **Security Services:**
  - Security Through TCP Wrappers

- **Network File Systems(NFS) Services:**
  - NFS overview
  - NFS advantages and disadvantages
  - Configuring NFS server
  - Configuring NFS client
  - Configuring NFS client with /et/fstab file
  - Configuring NFS Client with Autmount services
- **File Transfer Protocol(FTP) services:**
  - FTP Overview
  - Configuring FTP server and FTP client
  - Configuring FTP server for anonymous users and real users
  - Securing FTP server
- **SAMBA services:**
  - Overview of SAMBA
  - Installing and configuring samba server
  - Configuring samba server with heterogeneous platform
  - Configuring samba shares between UNIX- windows vice –versa
  - Configuring SAMBA shares with different level of security
- **Domain Name Service(DNS):**
  - Understanding DNS Services
  - Configuring types of DNS
    - Primary DNS
    - Secondary DNS
    - Forwarder and cache DNS
- **Web Services with APACHE:**
  - Apache overview
  - Apache configuration
  - Apache Security
  - Virtual Hosts
  - Configuring IP- based , Name based and Port based.
  - Configuring member logins for web server
- **NIS (Network Information Service):**
  - Overview of NIS
  - Configuring NIS Master and Slave Server
  - Configuring NIS Client
  - Configuring NIS with NFS servers
  - Using AutoFS Service with NIS
- **Dynamic Host Configuration Protocol(DHCP):**
  - Overview of DHCP services
  - Configuring DHCP server
  - Configuring DHCP Client in heterogeneous platform
- **Proxy server with Squid service:**
  - Configuring SQUID services
  - Configuring ACL's in SQUID

- **Securing data:**
  - Digital certificates
    - Creating certificates for IMAPS
    - Creating certificates for users
- **E-Mail services:**
  - Overview of email
  - Configuring sendmail service
  - Configuring webmail access with squirremail services
  - Configuring a dovecot services
  - Configuring mail client with mutt.

TRAINER DETAILS

(1) Mr. R.N.RAJU

5+yrs of experience as a Linux Admin

Red Hat Certified Professional

SERVICES

- **Subject Training**
- **Resume Writing**
- **Providing Interview Tips & Questions**
- **Conducting Mock Interviews**
- **Placements & Outsourcing**

STANSYS SOFTWARE SOLUTIONS

#7-1-621/113(67/3RT), Beside: Nagarjuna Jr.College, Near: S.R.Nagar Community Hall, S.R.Nagar, Hyd-38|Ph:8143408688|9542195422|www.stansys.co.in|stansys.linux@gmail.com

Compiled By

Mr.R.N.Raju

UNIX and LINUX Faculty

Stansys Software Solutions

Supervised and Scrutinized By

Mr. Krishna

IT Architect

AND

Faculty for SAS

Stansys Software Solutions

UNIX/LINUX

→ UNIX is a CUI Operating System.

→ LINUX is not just for UNIX wizards. LINUX is a clone of O/S.

→ Linux is the most important achievement of free software, it has been developed for business, education & personal productivity.

→ Everyone has to start somewhere, and Linux administrators and engineers are no exception. If you have purchased this book, I imagine that your goal is to pass the Red Hat exams (RHCSA & RHCE) while acquiring or improving your current Linux skills.

→ These Linux skills and commands are all essential for knowing how to work with linux, not just Red Hat.

* Operating System: (O/S)

→ Operating System is a interface between User & computer (or) It is a System Software.

→ The operating System is the most important program that runs on a computer. Every general-purpose computer must have an operating System to run other programs.

→ Operating Systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

→ It is classified into two types.

① Single User Systems.

② Multi User Systems.

① **Single user Systems:** provides a platform for only one user at a time. They are popularly associated with Desk Top operating System which run on standalone Systems where no user accounts are required.

Example: DOS

② **Multi User Systems:** More than one user can access same System resources (cpu, applications, memory, printers.... etc) at the same time known as multiuser.

Example: UNIX, LINUX

* Features of UNIX/LINUX:

(a) **Multiuser:** A multi-user operating System allows more than one user to share the same computer system at the same time.

(b) **Multi Tasking:** More than one program can be run at a time. The main concept of multitasking is maximum utilizing cpu resources.

(c) **Open System:** The UNIX is open source code. i.e Any user can modified unix open source code according there ideas and requirements

→ Using UNIX open source code

Sun Micro Systems + adding additional features = SunSolaries

IBM + " = IBM-AIX

HP + " = HP-UX

Santa Cruz + " = Sco-unix

Silicon Graphics + " = IRIX

Micro Soft + " = Xenix

→ Any operating system developed based on UNIX open source code known as flavors of UNIX.

→ The Linux was given to GPL (General public Lience) Organized by GNU.

→ Linus Torvalds, who was then a student at the university of Helsinki in Finland, developed Linux in 1991. Linux is also open system

Distributors of Linux:

Red Hat	Suse	Ubuntu	Puppy	Slakware
Centos	OEL	Fedora	White box	Mandrake

(d) **Security:** one of the most valued advantages of Linux over the other platforms lies with the high security levels it ensures. Every linux user is happy to work in a virus-free environment and use the regular virus-prevention time needed when working with other operating systems for other more important tasks.

→ UNIX/LINUX has given two levels of securities.

(i) **System level Security:** Its controlled by System Administrator.

(ii) **File Level Security:** Its controlled by Owner of the file.

(e) **portability:** portability means Endependent of hardware & processor

(f) **Communication:** The main concept of communication facility Exchanging of information or files from one user account to another user account.

(g) **programming facility:** UNIX o/s provides shell. Shell works like a programming language. It provides commands and keywords.

Script language	programming language
1. It is an interpreter based language.	1. Compiler based language.
2. Enterpreter converts high level instructions into lowlevel instructions line by line.	2. The whole program in a single shot into machine language.
3. Doesn't create .exe files	3. Create .exe files.
4. No need to compile the program.	4. Need to compile the program.
5. It takes less lines of code	5. Takes numerous lines of code.
6. Reducess cost of maintainance	6. Increses cost of maintainance.

(h) **Help facility:** It is the beautiful feature of UNIX/LINUX operating systems. Dont know the information about given command just gothrough the help line.

Example: # man <command name> ↵

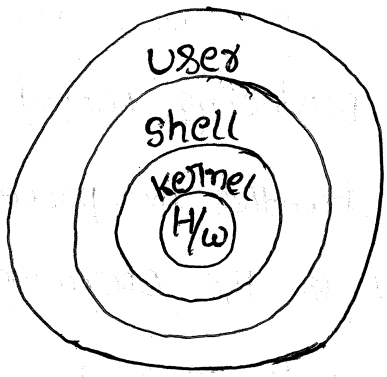
(or)

info <command name> ↵

(or)

<command name> --help ↵

* Architecture of O/S:



User:- User is nothing but an individual who uses the available hardware & software resources.

Shell: It is a command line interpreter. The shell access request from user and the checks command existence, if the command exist then it converts into kernel understandable language and it send the given request to kernel. The shell access interface between user and kernel.

Types of Shells:

Shell name	Developed by	prompt	Interpreter name
Bourne Shell	Stephen Bourne	$	Sh
Bash Shell	Stephen Bourne	$	bash
Korn Shell	David korn	$	ksh
Z Shell	paul	$	Zsh
C Shell	Bill Joy	%	csh

Note: The advanced version of Bourne shell is Bash shell. Bash means Bourne again Shell.

Default Shell name	Flavor name
Bash Shell	Linux
Bourne Shell	Sco-unix, Solaries, Hp-ux
Korn Shell	IBM-AIX
C Shell	IRIX

Kernel: The kernel is the heart of the operating System.

→ The kernel is responsible for interacting with the hardware and producing output to the screen.

→ It handles the process, memory, file, device and network management for the operating system.

→ Linux is tonly just the kernel.

* Difference between UNIX & WINDOWS:

UNIX	WINDOWS
1. It is GUI	1. It is GUI
2. It is Multiuser and Multitasking o/s	2. WINDOWS also Multiuser and Multitasking o/s.
3. To boot UNIX o/s, 2 MB RAM is Enough.	3. 12MB RAM is required.
4. UNIX is process based concept	4. It is Thread based concept.
5. On UNIX, Any user process is killed it will not effect to others.	5. It Effects to all.
6. Unlimited users working on the Server.	6. Limited users working on the server.
7. UNIX is open System	7. It is closed System.
8. It is portable o/s.	8. Not portable.
9. No down time	9. Down time is there.

* File System:

→ It is method of storing the data in an organized fashion on the disk. Every partition on the disk except MBR and Extended partition should be assigned with some file system in order to make them store the data. file system is applied on the partition by formatting it with a particular type of file system.

Types of file systems:

(a) Disk file systems:

→ A disk file system is a file system designed for the storage of files on a data storage device, most commonly a disk drive, which might be directly or indirectly connected to the computer.

Ex: FAT, FAT32, NTFS, CDFS, HFS, ext2, ext3, ISO 9660.

(b) Network file systems:

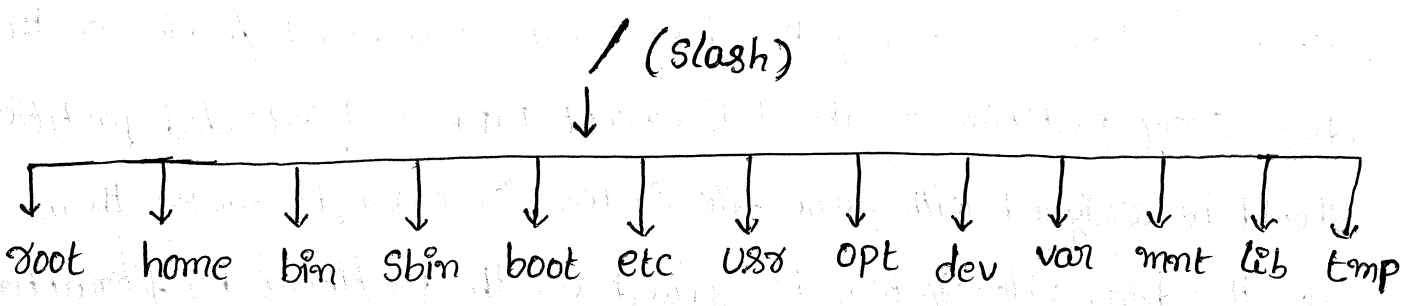
→ A Network file system is a file system that acts as a client for a remote file access protocol, providing access to files on a server.

Ex: DFS, NFS, SMB, FTP

(c) Virtual file system:

→ The purpose of VFS is to allow client applications to access different types of concrete file systems in a uniform way. It can be used to bridge the differences in windows, Mac OS and Unix file System, so that applications can access files on local file systems of those ~~file systems~~ types without having to know what type of file System they are accessing.

⇒ File System Hierarchy System:



/ : This is top level working directory. It is parent directory for all other directories. It is called as "ROOT" directory. It is represented by forward slash(/)

root: It is home directory for root user(super user). It provides working environment for root user.

home: It is home directory for other users. It provides working environment for other users (Except root).

bin: (Binary files): It contains commands used by all users.

Sbin: (Super user binary files): It contains commands used by only super user (root).

boot: It contains system bootable files, bootloader information, Kernel related information for Linux.

etc: It contains all system configuration files.

/etc/hosts, /etc/resolv.conf

usr: By default Soft wares are installed in /usr directory.

(UNIX Sharable Resources).

opt: It is a optional directory for users. It contains third party softwares.

dev: It contains all device files information. similar to device manager of windows. In UNIX/LINUX Every device treated as a file.

var: It is containing variable files information like mails, spring, log files.

mnt: It is default removable media working directory. It is empty by default.

lib: It contains library files which are used by OS. It is similar to dll files of windows. Library files in linux are SO (Shared Object) files.

tmp: It contains temporary files information.

media: It contains all of removable media like CD-ROM, pendrive.

proc: It contain process files.
It's contents are not permanent, they keep changing
It's also called as Virtual Directory.
It's file contain useful information used by OS.
like /proc/meminfo ---
/proc/cpuinfo ---

—x—

* Basic commands:

→ root user prompt.

$ → User working prompt.

$logname → Displays current user name.

$pwd → present working directory.

$date → Display current date & time.

$cal → Displays current month calender.

$cal 2020 → particular year total months.

$cal 04 2020 → 2020 year 04th month calender.

$who → To display the information about all the users who have logged into the system.

$whoami → It displays current user name.

$finger → It displays complete information about all the users who are logged in.

$uptime → How long server up & running, how many users connected and load avg time.

$which (or) $whereis → Given command location

Ex: which date↵

$tty → Terminal position.

$df → Displays disk free size

$du → Disk usage information

$clear → To clear the screen.

* Creating files:

⇒ **cat (concatenate):** It is used to create a file and display, appending the contents of a file.

→ **To create a file:**

```
$cat > filename ↵
Hello World
Ctrl+d (To save the file)
```

→ **To display the content of the file:**

```
$cat < filename ↵
(or)
$cat filename ↵
```

→ **To append the data in the existing file:**

```
$cat >> filename ↵
-------
Ctrl+d (To save)
```

⇒ **Touch:** To create multible files but all are Empty.

Syn: $touch file1 file2 file3 ----filen

Ex: $touch file1 file2 file3 ↵

⇒ **ls:** Displays the contents of a directory.

Syn: $ls [options]

Options:
- -r → Reverse
- -a → hidden
- -R → Recursively
- -i → inode
- -l → long list
- -h → human readable

⇒ **mkdir:** creates a directory.

Syn: mkdir <Dirname>

$mkdir Linux↵

→ **To create multible directories:**

$mkdir Dir1 Dir2 Dir3 --- Dirn↵

→ **To create a Nested directory:**

$mkdir -p world/asia/India/ap/Hyd↵

↳ parent

→ **To check:** $ tree world↵

(or)

$ ls -R↵

⇒ **Navigation commands:**

cd: changes the current location.

cd .. → To go one level back

cd ../.. → To go two levels back

cd → To change user's home directory.

Ex: $cd world↵

$ls↵

* **Note:** The trailing slash (/) is optional when you're using the cd command. It indicates that the name being specified is a directory.

Ex: $cd Documents/↵

⇒ **cp:** copies files or directories from one location to another.

Syn: cp [options] source Destination

-R → copies recursively
-f → copies forcefully
-v → provides verbose output.

Ex: $cp file1 file2 ↵ one file to another.

$cp file1 file2 Documents ↵ Multible files into Directory.

$cp -R Documents unix ↵ one directory to another.

$cp -rvf Documents unix world/asia/india/ap/Hyd ↵

$cp /var/log/messages . ↵ (.) represents current location.

⇒ **MV:** Moves or renames files and directories.

Syn: mv [options] SOURCE DEST

-v → verbose

→ Rename the file by specifying the file name & new name of the file:

$mv messages messages.bak ↵

→ move it to the test directory for safekeeping:

$mv messages.bak test/ ↵

$ls test ↵

⇒ **rm:** Deletes files or directories

Syn: rm [options] FILE

-i → interactive
-r → Recursively
-f → forcefully

→ Delete the messages.bak file:

$cd test ↵

$rm -i messages.bak ↵

→ Delete the test directory:

$cd .. ↵

$rm -rf test/ ↵

⇒ file: Displays the type of a file

Syn: file <filename>

Ex: $file test1 ↵

test1: Empty

$ file /etc/passwd ↵

passwd: ASCII test.

* Meta characters (or) Wild card characters:

(a) * : It matches zero (or) more characters in the given file.

Ex: $ls a* ↵ Displaying files start with 'a'.

$ls i*g ↵ Start with 'i' End with 'g'

$ls *g ↵ Listout End with 'g' only

$rm i* ↵ removes Start with i

$rm *g ↵ removes End with g only

$ cp a* Documents/ ↵ copies start with a

$ cp -rf i*g Documents/ ↵

$cp -rvf * /backup ↵ copies current directory all files

(b) ? : It matches any single character in the given file.

Ex: $ ls ? ↵ Display single character files.

$ ls ?? ↵ Two character files

$ ls a??? ↵ List four character files but first one is 'a'.

$rm ?? ↵ Removes two character files.

$cp ??? Documents/ ↵ Copies three character files.

(c) [ ] : It matches any single characters in the given list.

Ex: $ ls [aeiou] ↵ Displays given matching character files.

$ls [aeiou]* ↵ Displays start with a, e, i, o, u files.

$rm [aeiou]* ↵ Removing start with a, e, i, o, u

$cp [aeiou]* unix/ ↵ copying start with a, e, i, o, u

(d) [-] : It matches any single characters in the given range.

Ex: $ ls [a-f]* ↵ Displays start with a, b, c, d, e, f

$ ls [a-f, o-v]* ↵ Display start with a-e & o-v.

$rm [a-f]* ↵ Removes a-f

$cp [a-f, 1-9]* unix/ ↵ copying files a-f & 1-9

* Using a Text Editor:

Being able to use a text Editor is probably one of the most critical skills to have as a System administrator. you constantly need to Edit config files, write scripts or make changes to system files.... all of which require you to use a text Editor.

→ The three most popular editors available today include

vi (or) vim : Text editor with great flexibility.

emacs : Similar to vi, an advanced text Editor with many features.

nano : A basic text Editor for quick editing

⇒ Vi (or) Vim Editor:

→ Using this Editor to create new files, open the files and modifying the data into a Existing files.

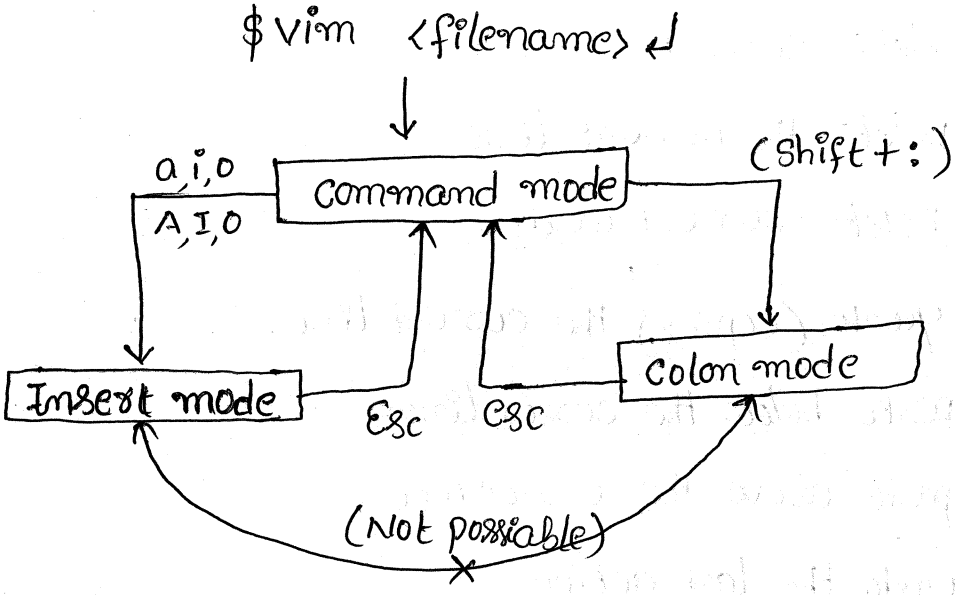
→ The vi Editor is most popular.

→ It has three modes : (a) Command mode
(b) Insert mode
(c) Execution (or) colon mode.

→ By default mode is command mode.

Syn: Vim [arguments] [File]

Arguments: -R → opens a file in read-only mode
-o → open two files at a time
+ → Starts at the end of the file
+<num> → Starts at line <num>



Insert mode options:

i → To begin insert mode at the current cursor position.

I → To insert at the beginning of the current line.

a → To append to the next word's letter.

A → To append at the end of the line.

o → To insert a new line below the cursor position.

O → To insert a new line above the cursor position.

commands for command mode:

e → Moves to the end of a word.

b → Moves to the beginning of a word.

$ → Moves to the end of a line.

^ → Moves to the begining of a line.

H → Moves to the first line onscreen.

M → Moves to the Middle line onscreen.

L → Moves to the ~~end~~ last line onscreen.

x (nx) → Deletes current character.

dd (ndd) → Deletes the current line.

dw (ndw) → Deletes current word.

yy (nyy) → Yanks (copies) the current line.

p → paste below the cursor line.

P → paste above the cursor line.

u → Undo the last action.

gg (ngg) → go to begginning of the file.

G → End of the file.

w (n) → To move the cursor forward, word by word.

b (n) → To move the cursor backword, word by word.

ctrl + f → To forward one page.

ctrl + b → To backword one page.

/ → To search a word in the file.

n → find next occurence of search word.

N → find previous occurence of search word.

. → Repeat last command action.

Commands for last line mode:

:q → To quit without saving

:w → To save the changes

:wq → To save & quit

:wq!
(or)
:x → To save & quit with forcefully.

: set nu
(or) } → To setting line numbers.
: se nu

: set nonu
(or) } → To remove line numbers.
: se nonu

: n → Jumps to line n

: $d → To delete last line

: ! <unixCmd> → To execute unix cmds.

: x → To give password to the file and remove password.

: /string/ → To search a word in the file.

→ **To find & Replace:**

: % s/root/dog/ ↵ To replace string "dog" for the first instance on a line.

: % s/root/dog/g ↵ for each instance of a line.

: % s/root/dog/gi ↵ To ignore casesensitive

: % s/root/dog/gc ↵ ask for confirmation.

→ **Executing unix commands in vi:**

Any unix command can be executed from the vi command line by typing an "!" before the unix command.

Ex: : ! pwd ↵

: r ! date ↵ Reads the results from the date command into a new line following the cursor.

: r ! cat file1 ↵

→ I want to copy 1,4 lines to paste after 10th line:

:1,4 co 10 ↵

→ I want to move 3,7 lines after 8th line:

:3,7 mo 8 ↵

→ I want to copy 1,30 lines create a new file:

:1,30 w test1 ↵

→ I want to append the data into a existing file:

:8,20w >> test1 ↵

→ I want to insert end of the line (or) we require line

:r /etc/passwd ↵

Managing two files at time:

$vim -o file1 file2 ↵

(or)

$vim file1 file2 ↵

Options:

:n → Edit next file (file2)

:rew → Rewind to the file (file1)

(or)

→ To move one file to another file (ctrl + w)

↳ press two times

—x—

* I/O Redirection :-

→ Sometimes you need to use the output from a command more than once. To accomplish this, you can redirect the output of commands using some neat command-line tricks.

→ There are also a few characters you can use to direct or redirect output of commands. These characters are

>	Directs output to a file or device (override if the file exists)
<	Directs input from the file or device.
>>	Appends output or text to a file (creates if the file doesn't Exist).
|	pipes the output of one command to another.
&&	combines commands.

(or)

STDIN – file Description (FD) – 0

STDOUT – file Description (FD) – 1

STDERR – file Description (FD) – 2

Examples : ① $cat file > backup ↵

$cat backup ↵ To verify

② $cat > test2 < test1 ↵ Input from the test1

$cat test2 ↵ To verify

③ $cat test1 test2 test3 2> Error1 ↵
↳ file not Exist
$cat Error1 ↵ To verify

④ $cat Sample test test3 > out-file 2>> Error1 ↵
↳ file not Exist
$cat out-file ↵
$cat Error1 ↵ } → To verify

⇒ **echo:** outputs or displays a string.

Ex: $echo "this is some sample text" ↵

→ To output some text to a file:

$echo "this is some sample text" > file_example ↵

$cat file_example ↵ To verify.

⇒ **cut:** Divides a string or output.

Syn: cut [option] file

-d Specifies a delimiter
-f Displays a particular field.
-c Displays a character.

→ Displays the third field of the text using space as a delimiter:

$cut -d " " -f3 file_Example ↵

→ Displays third & fourth fields:

$cut f3,4 file_Example ↵

→ Displays 1st to 5th characters:

$cut -c 1-5 file_example↵

⇒ paste: To join two or more files horizontally by using delimiters.

→ To join two files horizontally:

$paste states capitals↵

AP Hyd
MP Bopal
KN Banglore

→ To join two files using delimiter:

$paste -d ":" states capitals↵

AP : Hyd
MP : Bopal
KN : Banglore

$paste -d ":" states capitals > Example↵

⇒ WC: provides a word or line count.

Syn: wc [options] file

-l Lines
-w words
-c characters

$wc Example↵ Displays lines, words and characters.

$wc -l Example↵ only lines

$wc -w Example↵ only words.

⇒ **Diff:** Displays different lines between two files.

```
$diff file1 file2 ↵
```

⇒ **Cmp:** It compares two files character by character.

```
$cmp file1 file2 ↵
```

Note: If files are same it doesn't return any output otherwise it displays line numbers and character position.

⇒ **tr:** It translate character by character.

```
$tr "aeiou" "AEIOU" < sample ↵
$tr "a-z" "A-Z" < sample ↵ Translate lower to upper.
$tr "A-Z" "a-z" < sample ↵ Upper to lower
$tr -s " " < sample ↵
    ↳ squeeze
$tr -d "aeiou" < sample ↵ To delete aeiou
$tr "," "\t" < sample ↵ Replaced with tab space.
```

⇒ **aspellcheck:** To check the spelling mistakes but not gramitical mistakes.

```
$aspellcheck sample ↵
$aspellcheck test ↵
```

⇒ **Head:** Displays top 10 lines of the file

$head Sample ↵

$head -5 Sample ↵ Top 5 lines.

⇒ **Tail:** Displays last 10 lines of the file.

$tail Sample ↵

$tail -5 sample ↵ last 5 lines

$tail -f sample ↵ file is open continously.

⇒ **piping (|):** Combine the two or more commands in to a single line.

→ Here the first command output is taken as the next command input.

$ls -l | wc -l ↵

$cat Example | cut -d " " -f3 file_Example ↵

$cat Example | head -20 ↵

⇒ **&&:** combines commands.

$echo "This is text file" > file_Example && cut -f3 Example ↵

$cat file_Example ↵ To verify

$echo "My original text" >> file_Example && cat file_Example ↵

⇒ **More:** To see the contents of a file in the form of pagewise.

```
$more example↵
```

⇒ **less:** To display file contents in pagewise. But we can go to all directions.

```
$less example↵
```

options: f → forward direction
b → Backward direction
v → vi editor mode
q → to quit.

⇒ **Tee:** It is used to write the data into the files as well as on the screen.

```
$cat sample | tee file1 file2 file3↵
$cat file1↵ to verify
$cat file2↵
```

⇒ **Sort:** Sorts the output of a command or file.

Syn: Sort [options] FILE

-r → sorts in reverse order
-b → Ignores leading blanks
-n → compares according to numarical storing value.

$ sort Example ↵

$ sort -r Example ↵ Reverse order

$ sort -n Example ↵ Display numaric

$ sort -u Example ↵ uniquee lines

$ sort -f Example ↵ Ignores case

ASCII Values
0-9 ⇒ 48-57
A-Z ⇒ 65-90
a-z ⇒ 97-122

⇒ **uniq:** Lists all the unique lines in a file or command output.

$ uniq Example ↵

$ uniq -u Example ↵ Displays non duplicated lines

$ uniq -d Example ↵ Displays only duplicated lines

$ uniq file_example > uniq_file && cat uniq_file ↵

→ On above command to view uniq lines in the sample file, create a new file based on the output, and view the contents of this new file.

⇒ **Sed (Stream Editor):** To search and replace strings or patterns in the given file.

→ Sed is a multipurpose filter command.

Syn: Sed "s/oldstring name/new string name/g" <filename>

s → Substitution

g → Global occurence in Every line.

$ sed "s/unix/linux/g" sample↵

$ sed "s/unix/linux/gi" sample↵ Ignore case.

$ sed "s/unix/linux/" sample↵

$ sed "s/^unix/linux/gi" sample↵

$ sed "s/unix//gi" sample↵ Delete a word from a file.

$ sed -e "s/unix/sas/gi" -e "s/linux/dba/gi" sample↵

$ sed -n "2p" sample↵ To print 2nd row

$ sed -n "3,5p" sample↵ To print 3rd, 4th, 5th rows.

$ sed -n "1p↵
>$p" sample↵ print 1st and last rows.

$ sed '3d' sample↵ Delete 3rd row.

$ sed '2,5d' sample↵ Delete 2 to 5 lines.

$ sed '2,5w file' sample↵ It copies 2nd to 5th rows from sample file to file.

$ sed '=' sample↵ To get line numbers.

⇒ Regular Expressions (or) Regex (Grep):

→ Globally research a regular Expression & print

→ To search a string or regular expression in a file(s).

Syn: grep [options] PATTERN FILE(S)

$ grep root sample ↵

$ grep root sample Example backup ↵

$ grep root * ↵ Search all files in a current directory.

$ grep -i root sample ↵ Ignore case

$ grep -c root sample ↵ counts no. of lines

$ grep -n root sample ↵ print the lines along with line no's.

$ grep -l root sample ↵ List file names only the given patte

$ grep -r root * ↵ Search the pattern Recursively

$ grep -v root sample ↵ prints nonmatching lines.

$ grep -o root sample ↵ prints only the given pattern.

$ grep root sample --color ↵ Displays output in color

$ grep "it technology" sample ↵

$ grep "Exam*" sample ↵ prints start with Exam pattern.

$ grep "b[aeiou]ll" sample ↵

o/p: ball
bell
bill
boll

$ grep "b..d" sample ↵

o/p: band
book
ba#d
ba-d

Note: "." & "*" are wild card characters, it matches any single character.

$grep c[on] Example↵

$grep [0-9] Example↵

word pattern: \< \> ⇒ word boundary

\< ⇒ Starting of the word

\> ⇒ Ending of the word

$ grep "\< root \>" sample↵

$grep "\<root" sample↵ o/p: root ✓ root123 ✗

$grep "root \>" sample↵ o/p: root ✓ root123 ✓ xroot123 ✗

$grep "\<[0-9][0-9][0-9][0-9]\>" Sample↵ 1025 ✓ 112 ✗ 1356 ✓

Line pattern:

Anchors: ^ ⇒ Start of the line.

$ ⇒ End of the line.

$grep "^d" Sample↵ line start with d

$grep "^me" sample↵ line start with me.

$ grep "me$" sample↵ line End with me.

$grep "^[^aei] Sample↵ Not start with a, e, i

$grep "[0-9]$" Sample↵ line Ending with digit.

$grep "^unix$" Sample↵ line should contain only unix.

$grep "^$" sample↵ Displays Empty lines.

$grep "^...$" sample↵ Line should contain three characters.

fgrep: To search the string more faster than the grep command

```
$ fgrep "unix ↵
        >sas ↵
        >dba" sample ↵
```

egrep (Extended grep): It is a combination of grep & fgrep plus some additional regular Expressions.

```
$egrep "(unix|oracle|sas)" sample ↵
$egrep ab{3}c sample ↵   Exact occurence of preceding character
$egrep "|<[0-9]{4,7}|>" sample ↵
$egrep ab{3}c => abc  abbbc  abbbbbc
                  ×          ×
```

⇒ **Find:** This filter is used to search the results by depending on requirments may be on name, inode, permissions, user----etc.

Syn: find <search path> <criteria> <action>

(a) **Based on name:**

```
$ find / -name passwd ↵
$ find /home -name passwd ↵
$ find /etc -name 'pass*' ↵
$ find . -name linux ↵
```

(b) Based on Size:

+n ⇒ for greater than n.
-n ⇒ for less than n.
n ⇒ for Exactly n.

$ find / -size 4c ↵ 4 character files

$ find / -size +4c ↵ More than 4 character files

$ find / -size -4c ↵ less than 4 characters.

$ find . -size +50m ↵ More than 50M.

$ find /etc/Backup -size -50m ↵ Less than 50M

$ find / -size +30M -size -50M ↵ Between 30 to 50m.

c) Based on permissions:

$ find / -perm 644 ↵

$ find / -perm 665 ↵

$ find / -perm 777 ↵

(d) Based on Type: $ find / -type f ↵ To find files

$ find / -type d ↵ To find directories

(e) Based on inode:

$ find / -inum 15253 ↵

$ find /root -inum 32512 ↵

$ find /home -inum 130123 ↵

(f) Based on time:

mtime → Modification time.
ctime → Change time.
atime → Access time.

$ find / -mtime +10 ↵
$ find / -mtime -10 ↵
$ find / -mtime 10 ↵

⟹ To find the file with access time:

$ find /root -atime +5 ↵ 5 days ago.
$ find /root -atime -5 ↵
$ find /root -atime 5 ↵

⟹ To find the file with change time:

$ find / -ctime +5 ↵
" " -5 ↵
" " 5 ↵

$ find / -amin +5 ↵ file was last accessed 5 minutes ago
$ find /root -cmin +5 ↵ file's status was last changed 5 minutes ago.

$ find /home -mmin +5 ↵
$ find /root -amin -5 ↵
$ find . -amin 5 ↵

(g) Based on user:

$ find / -user <username>

$ find / -user raju↵ particular user files.

(h) Based on group:

$ find / group <groupname>

$ find / group sales↵ particular group files.

* path: It is the way of representing files & directories in the system.

→ There are two types of paths.

(i) Absolute path: It is the way of representing files and directories form the top of hierarchy.

Ex: $ ls /root/world/asia/india/ap/hyd/↵

$ cp /home/raju/linux /root/world/asia↵

(ii) Relative path: It is the way of representing files and directories which are related to current directory.

Ex: $ cd /home/raju/Desktop↵

$ cp linux unix/sas↵

$ cd unix/sas↵

$ ls↵

* Monitoring System performance: (or) process Management:

→ A process is a program under Execution. (or)

→ A process is a instance of a running program.

→ process have their own address space in memory, thread of Execution, and characteristics such as security context, Environment and current priority.

→ The linux kernel tracks every aspect of a process by its process ID number information about Each process is advertised by the kernel to user program through the /process/PID directories.

→ When a process starts another program, the new process is called child process. This original process is the parent process of its child process. Child process inherit characteristics from its parent, such as its Environment and the user and groups its as which its run.

→ There are two types of process: (a) foreground process.
(b) Background process.

(a) Foreground process:

→ In foreground user can execute only one process (or) job.

Ex: $ firefox ↵

→ To kill the foreground job:

Ctrl + c

Ex: ② $ cp file1 file2 ↵

(b) Background process:

→ In Background user can execute many jobs at a time.

Ex: $ firefox &↵

$ cp file1 file2 &↵

→ To check the Jobs list: $ jobs ↵

ps: Displays information about running process.

$ ps ↵

→ To view process with more detailed information:

$ps u ↵

→ To can detailed about a particular process:

$ps aux | grep ssh ↵

(or)

$ps aux ↵

kill: Terminates a process.

Syn: $ kill PID

$kill 4286↵

Sometimes if the kill command doesn't work the way you intended it to, you can also call it with the -9 option to give it priority on the System.

$kill -9 4286 ↵
↳ signal.

Signal: The operating system communicates to process through signals. These signals reports events or Error situations to processes. In many cases signals will result in the process Existing

→ one typical signal is SIGTERM, which terminates the process; it asks it to Exit cleanly.

→ Another is SIGKILL, which kills the process; the process is required to Exit immediately.

→ To find the PID(s) belonging to the SSH service:

$pidof sshd ↵

(or)

$pgrep sshd ↵

top: Monitors system resources (Similar to Task Manager in Windows)

$top ↵

options:

s → To change the time interval for updating top results (sec's)

R → To sort by PID number

u → username to get only that user process details.

P → To sort by cpu utilization.

M → To sort by RAM utilization.

C → To display or hide command full path.

r → To renice a process

k → To kill a process

w → To save the modified configuration

'q' → To quit.

→ When you're comfortable working with processes, you can then make some more advanced adjustments, such as changing the priority of a particular process.

renice: Adjusts the priority of a particular process.

Syn: renice <priority> [options]

-p changes process priority for a particular PID.

-u changes process priority for a particular user(s).

→ The priority value range from -20 (first priority) to 20 (dead last priority). only the root user may set processes to use a priority under 0.

#renice -2 3874 ↵

* **Note:** If all ready processes have the same priority, they will share the processor equally. priority only has an Effect when two process at different priority levels are computing for cpu time, in which case the lower priority process will get less time & apper to run more slowly.

nohup: The nohup jobs will create in server account so nohup jobs will execute even the user disconnects from his account.

Ex: $nohup cp file1 file2 & ↵

$nohup firefox & ↵

—×—

* Communication commands :

→ The main concept of communication facility exchanging of information or files from one user to another user.

write : It is used for to write message to another user account, but he should be logged into the user.

```
$ write username/terminalname ↵
  -----
  ctrl+d (save & quit)
```

→ To deny messages : $mesg n ↵

→ To allow messages : $mesg y ↵

wall : It is used for to send broadcast message to all users, who are connected to server

```
$ wall ↵
  Welcome to Linux.....
  ctrl+d (save & quit)
```

Mail : Using mail command you can quickly and efficiently circulate memos and other written information to your co-workers. you can even send and receive mails from people outside your organization.

```
$ mail user1@server1254.example.com ↵   Single user
$ mail user1 user2 user3 ↵              Multible users at a time
$ mail user1 < stud ↵
$ mail user2 < backup_file ↵            } It translates files to user.
```

→ Mails are stored in mailbox : (/var/spool/mail/username)

→ To open the mail box : $mail ↵

Note: By default all mails will store in primary mail box (/var/spool/mail). It will opened mails in primary mail box transfered to secondary mail box (i.e mbox).

→ TO open secondary mail box : $mail -f ↵

→ The primary mailbox only maintains unread mails.

Mail box options:

q → quit	d → delete
r → reply	d 2 → delete 2nd mail
P → print	w filename → It writes to new file.

* One Bit Equals to how many bytes :

→ Bit is the smallest component of data and byte is larger than bit size. The size 1000 can be replaced with 1024 and still be correct using the other acceptable standards. Both of these standards are correct depending on what type of storage you are refferring.

processor (or) Virtual Storage		Disk Storage	
1 bit	= Binary digit	1 bit	= Binary digit
8 bits	= 1 Byte	8 bits	= 1 Byte
1024 bytes	= 1 Kilobyte	1000 bytes	= 1 Kilo
1024 Kilo	= 1 Mega	1000 Kilo	= 1 Mega
1024 Mega	= 1 Giga	1000 Mega	= 1 Giga
1024 Giga	= 1 Tera	1000 Giga	= 1 Tera
1024 Tera	= 1 peta	1000 Tera	= 1 peta
1024 peta	= 1 Exa	1000 peta	= 1 Exa
1024 Exa	= 1 Zetta	1000 Exa	= 1 Zetta
1024 Zetta	= 1 Yotta	1000 Zetta	= 1 Yotta
1024 Yotta	= 1 Bronto	1000 Yotta	= 1 Bronto

* **Links:** To give a pointer to the source file called as a link.

→ In unix/Linux two types of Links.

(a) Soft Links
(b) Hard Links.

(a) Soft links: → The inode number of the source file, Link file are different.

→ It can be created across the file system.
→ Editing of original file will be replicate in the Link files.
→ Size of soft link file Equals to number of characters in original file path.
→ If source file is deleted the link file will not be accessible.
→ It is also be called as shortcut link.

Syn: $ ln -s <source file> <link file>

Ex: $ ln -s /Backup/linux /root/Desktop/linux ↵

(b) Hard links: → Source file, link file has same inode numbers.

→ It can't be created across file system.
→ Editing of original file will replicate in the link files.
→ Size of hard link file is same as original file.
→ The source file is deleted the link file we can access.
→ It is a backup link.

Syn: $ ln <source file> <link file>

Ex: $ ln /root/backup /root/Desktop/backup ↵

* **Shell concept:** Shell is a command line interpreter. The Shell access request from user and the checks command existence if the command exist then it converts into kernel understandble language (machine language) and it send the given request to kernel.

→ The shell access interface b/w user and kernel.

⇒ **Types of shells:**

Shell name	Developed By	prompt	Interpretername
Bourne shell	Stephen Bourne	$	Sh
Korn shell	David korn	$	ksh
C shell	Bill Joy	%	csh
Bash shell	Stephen Bourne	$	bash
Z shell	paul	$	zsh

Note: The advanced version of Bourneshell is bash shell.

→ Bash means "Bourne again shell".

→ Bash shell is default in Linux.

Default Shell name	Flavour name
Bash shell	Linux
Bourne shell	SCO_unix, Solaries, HP-UX
Korn shell	IBM-AIX
CShell	IRIX (Silicon Graphics)

Features of shells:

- Word completion.
- Command History.
- Command alias.

→ To check the shells:

$cat /etc/shells ↵

→ To check parent shell of current user:

#echo $SHELL ↵

→ To view the available shells:

#cd /bin ↵

#ls *sh ↵

→ To shift from bash shell to sh shell:

#sh ↵

→ To shift from sh shell to k shell:

#ksh ↵

→ To check current working shell:

#echo $0 ↵

→ To Exist the shell:

#Exist ↵

Command completion: Linux automatic command completion is a tool or program that can identify what you are typing in the linux command line terminal and can complete that command, words or sentence for you. this is really cool feature in Linux.

→ When <TAB> key is pressed, any command starting with the given string will be completed by the system automatically.

→ For multible commands that starting with the given string, pressing <TAB> key twice will list down all those matched files or commands.

→ If there are no matched of any command, files or folders. Then, the automatic word completion will not shown, a 'ting' sound will buzzed.

Ex: $ cd /var/l<tab>
lib/ lock/ log/

Command History: The history command performs one of several operations related to recently-executed commands recorded in a history list. Each of these recorded commands is refferred to as an 'event' when specifying an event to the history command.

$history ↵
$history 10 ↵
$history -c ↵ Lock the history.
$history -r ↵ Unlock the history.
$ rm .bash_history ↵ Removes the history.

Command alias:

→ Alias is a built in shell command in Linux/unix operating systems.
→ It can save you a lot of typing by assiging a name to long commands.
→ The alias command can be useful if you want to create a 'shortcut' to a command.

Syn: aliasname='command'

Ex: $ alias u=useradd ↵
$ alias c=clear ↵
$alias ↵ Display alias list
$unalias u ↵ Disable alias
$vim .bashrc ↵ permanent alias names

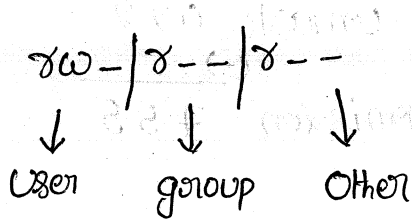
File permissions

→ Just like every operating system, Linux comes with a set of permissions that it uses to protect files, directories, and devices on the system.

→ These permissions can be manipulated to allow (or) disallow access to files and directories on different parts of the system.

Basic file permissions:

→ Let's look at how permissions work first. Linux permissions are implemented through the properties of files and defined by three separate categories.



User: person who owns the file.

Group: Group that owns the file.

Other: All other users on the system.

→ permissions in Linux can be assigned one of two ways. you can use the mnemonic or a single digit to represent the permission level.

Operation	Digit	Mnemonic	Description
Read	r	4	View file contents.
Write	w	2	Write to or change.
Execute	x	1	Run the file.

Default file permissions:

umask: Universal mask is a default value that always gets dedicated from maximum file permission allocated for every file & Directory.

→ For super user umask value is #022.

→ For Normal user umask value is $002.

For super user:

→ Maximum permission of a file 666

umask 022

(-)

→ Default file permission → 644

→ Maximum permission of a directory 777.

umask 022

(-)

→ Default directory permission 755

For Normal user:

→ Maximum permission of a file – 666

umask – 002

(-)

664

→ Maximum permission of a directory - 777

umask - 002

(-)

775

→ To see the umask #umask↵

→ To change the umask #umask 222↵

→ To view umask value from the file

#vim /etc/bashrc↵

Operators:

+ ⇒ To add a permission.

− ⇒ To remove a permission.

= ⇒ To override the permission.

→ Here are some of the commands you can use to work with permissions:

(a) chmod:- It is used to change the permission of a file and directory. It can be used by the owner of the file (or) by root.

Syn: chmod [options] [permission] [File]

-R → Acts recursively.

-v → provides verbose output.

Ex: ① # chmod u+rw,g+r,o+x linux ↵

(or)

chmod 641 Linux ↵

② # chmod ugo =rw backup ↵

(or)

chmod 666 backup ↵

③ # chmod u-w,g-r,o-x linux ↵

④ # chmod -R u+w,g+r,o+x Linux ↵

⑤ # chmod -R 777 unix ↵

⑥ # chmod 755 unix ↵

(b) Chgrp:

→ By using this command we can change group of the file.

Syn: Chgrp [options] [groupname] [file]

-R → Recursively
-V → Verbose

Ex: #ls -l linux ↵

#Chgrp sales linux ↵

(c) Chown:- This command is used to we can change the owner of the file, as well as owner & group at a time.

Syn: chown [options] [user:group] [file]

-R → Recursively
-V → Verbose.

Ex: #Chown raju linux ↵ To change only owner.

#chown raju:sales linux ↵ To change owner & group.

#chown -R ramu:color unix ↵ Recursivly to change.

→ To view the symbolic as well as numaric mode of permission

#stat linux ↵

→ To change the permissions in GUI mode

#nautilus & ↵

→ Assign the permissions in GUI mode:

Right click on file → properties → permissions.

—x—

Automation Jobs

→ In any operating system, it is possible to create jobs that you want to reoccur. This process known as job scheduling, is usually done based on user-defined jobs.

→ As an administrator, however, you can define your own jobs and allow your users to create them as well.

→ The importance of the job scheduling is that the critical tasks like taking backups, which the clients usually wants to be taken in nights, can easily be performed without the intervention of the administrator by scheduling a cron job. If the cronjob is scheduled carefully than the backup will be taken at any given time of the client and there will be no need for the administrator to remain back at nights to take the backup.

→ For Red Hat or any other linux, this process is handled by the cron service or a daemon called crond, which can be used to schedule tasks (also called jobs).

→ By default, Red Hat comes with a set of predefined jobs that occur on the system (hourly, daily, weekly, monthly, and ~~the~~ with arbitrary periodicity).

→ There are two tools to scheduling jobs.

(a) at

(b) crontab

⇒ **AT Jobs:** "at" is used to schedule the job for a particular time or interval, in other words it is used only for one time or only for one interval.

Syn: at [options]

-l	Lists all jobs in the queue
-d	Removes a job from the queue.
-f	Reads input from the file
-m	Sends mail to the user when the job is complete.

Examples:

① $at 9am↵

at> date

ctrl+d (Save & quit)

② $at now + 3 days ↵

at> /bin/echo "Hello world"

ctrl+d (Save & quit)

③ $at 03222013 ↵

at> ls

ctrl+d (Save & quit)

④ $at 1:30 3/22/2013 ↵

at> cp file1 file2

ctrl+d (Save & quit)

→ View the currently queued jobs:

$at -l ↵

(or)

$atq ↵

⑤ $at -f filename.npm ↵

at> /bin/echo "Hello world"

Ctrl+d (save & quit)

→ Delete the job from the queue:

$at -d 1 ↵

(or)

$atrm 1 ↵

→ Verify that the job is truly gone:

$atq ↵

→ To view the job details:

$at -c 2 ↵

⇒ Restricting a user from using at jobs:

→ The atd service uses two files to control access to the services.

/etc/at.allow

/etc/at.deny

The /etc/at.allow file:

- If it exists, only these users are allowed (at.deny is ignored).
- If it doesn't exist, all users except at.deny are permitted.

The /etc/at.deny file:

- If it exists and is empty, all users are allowed (Red Hat default)

for both files:

- If neither file exists, root only.

⇒ cron jobs:

→ The default setting for Red Hat allows any user to create a cron job. As the root user, you also have the ability to edit and remove any cron job you want.

→ Let's jump into creating a cron job for the system. you can use the crontab command to create, edit, and delete jobs.

Syn: crontab [-u user] [option]

options: -e Edits the user's crontab.

-l Lists the user's crontab.

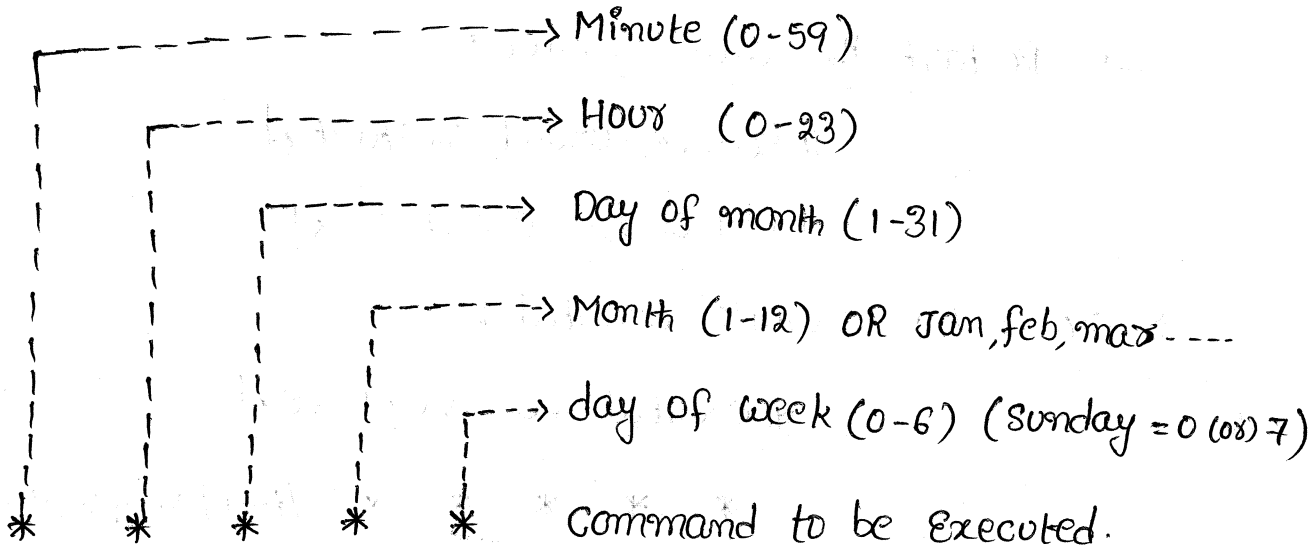
-r Deletes the user's crontab

-i prompts before deleting the user's crontab.

→ Before you start using the crontab command, however, you should look over the format it uses so you understand how to create and edit cron jobs. Each user has her own crontab file in /var/spool/cron, based on the username of each user. Any "allow" actions taken by the cron service are logged to /var/log/cron.

→ To view the /etc/crontab file to understand its Syntax:

$grep ^# /etc/crontab↵



Examples:

crontab -e↵

*/01	*	*	*	*	date
*/30	11	*	*	*	cp file1 file2
45	10,22	03	*	*	/bin/echo "Hello world"
50	22	01, 11	10	*	logname
59	23	31	12	*	/bin/echo "Happy New year"
*/01	*	*	*	0,6	/bin/echo "Today is weekend"

:wq!↵

→ To check assigned cronjobs:

crontab -l↵

→ To check the crond job service:

```
#service crond status ↵
```

→ Restart the cron service:

```
#service crond restart ↵
#chkconfig crond on ↵
```

→ To setup user01's crontab:

```
#crontab -u user01 -e ↵
* * * * * /tmp/sample_script
:wq!
```

→ To remove a user's crontab jobs:

```
#crontab -u user01 -r ↵
```

→ You can verify the log file:

```
#tail /var/log/cron ↵
```

*

Note:

→ What do you think happens if you set up cron jobs to run during the night (say, to run some reports) and you shut down the system right before you go home? well, it turns out that there is another great feature of cron. the /etc/~~cron~~anacrontab file defines jobs that should be run every time the system is started. If your system is turned off during the time that a cron job should have run, when the system boots again, the cron service will call /etc/anacrontab to make sure that all missed cron jobs are run.

→ Let's look at the /etc/anacrontab file:

#cat /etc/anacrontab ↵

Control access to the cron service:

→ To start working with cron, first need to know at the two config files that control access to the cron service:

→ These two files are

/etc/cron.allow.

/etc/cron.deny.

The /etc/cron.allow file:

- If it exists, only these users are allowed (cron.deny is ignored)
- If it doesn't exist, all users except cron.deny are permitted.

The /etc/cron.deny file:

- If it exists and is empty, all users are allowed (Red Hat default)

For both files:

- If neither file exists, root only.

— X —

User Administration

→ User is nothing but an individual who uses the available H/w & S/w resources

→ In Red Hat, there are three different types of users.

(a) Super user (or) root user:

→ The root user account is the equivalent of the Administrator (or) Enterprise Admin account in the Windows world.

→ It is the most powerful account on the system and has access to everything.

(b) System users:

→ A System account is similar to a normal user account. The main difference is that System users normally don't have a home directory and can't login the way normal users do.

→ Many system users are created or associated with applications or service to help run them more securely.

→ For example if we install 'Apache it will create a user apache. these kinds of users are known as System users.

(c) Normal user's:

→ Normal users are the users created by the root user. They are normal users like Rahul, Sara, Raju ---- etc.

→ Normal user accounts have no write access to anything on the system except their home directory (they can read and explore much of the system, however), which is created when the user account is added.

→ As an Administrator, you can assign access rights to different files & directories, allowing your users to gain access to different areas of the system (outside their home directory).

Some important points related to users:

→ Users & Groups are used to control access to files and resources.
→ Users login to the system by supplying their username & password.
→ Every file on the system is owned by a user and associated with a group.
→ Every process has an owner and group affiliation, and can only access the resources owner or group can access.
→ Every user of the system is assigned a unique user ID number.
→ Users name and UID are stored in /etc/passwd.
→ Users password is stored in /etc/shadow in encrypted form.
→ Users are assigned a home directory and a program that is run when they login (usually a shell).
→ Users can't read, write or Execute each other's files without permissions.

Types of users in Linux & their attributes:-

Type	Example	UID	GID	Home Directory
Super user	root	0	0	/root
System user	ftp, ssh, nobody	1-499	1-499	/var/ftp
Normal user	visitor, sara	500-60,000	500-60,000	/home/user

→ Whenever a user is created in Linux things created by default:

→ A home directory is created (/home/username)
→ A mail box is created (/var/spool/mail)
→ Unique UID & GID are given to user.

User private Group (UPG) :-

On Red Hat Linux uses user private Group (UPG) schema. According to UPG scheme, you create the any user account, the user consists the primary group with same name and same ID.

→ For Example if a user is created with the name Raju, then a primary group of that user will be Raju only.

→ The user information maintained by the two database files:

(a) /etc/passwd :→ This file maintains user related information.

Syn: <username>:<password>:<UID>:<GID>:<comments>:<Homedir>:<shell>

(b) /etc/shadow: → This file maintains user related password information.

Syn: <username>:<encrypted password>:<Last passwd change>:<min>:<max>:<warn>:<inactive>:<expires>:<not used>

complexity Requirements of password :-

→ A root user can change password of self and any user in the System, there are no rules for root to assign a password. Root can assign any length of password either long or short, it can be alphabet or numeric or both. on the whole there is no limitation for root for assiging a password.

→ A normal user can change only its password. Valid password for a normal user should add here to the following Rules.

→ It should be at least 7 characters but not more than 255 character
→ At least one character should be upper case.
→ At least one character should be lower case.
→ At least one character should be a symbol and number.
→ It should not match the previous password
→ The login name and the password can't be same.

→ To manage user accounts, you can use the following commands:

Useradd:- Create user (or) System accounts.

Syn: useradd [options] LOGIN

options:

-u	userid
-c	comment
-e	Expire_Date
-s	SHELL
-r	creates a system account
-d	Home directory
-g	primary group id
-G	secondary group id.

Ex: → Create a user

```
#useradd raju↵
```

→ To check the user you just created

```
# cat /etc/passwd | grep raju↵
```

→ Let's create a user with our own attributes

```
#useradd -u 555 -c "Linux user" -d /opt/india -s /bin/sh india↵
```

→ To check the user:

```
# cat /etc/passwd | grep india↵
```

Tip:- As a good practice, you should provide a label or some description for each account; otherwise, after time, you will forget what it is for.

Usermod:- Modifies user accounts.

Syn: usermod [options] LOGIN

Note:- All the options which are used with useradd command can be used and,

-l TO change login name

-L TO Lock account

-U TO Unlock account.

Ex: → Changing the name of the user

#usermod -l newname oldname ↵

→ TO lock the user account

#usermod -L username ↵

→ To unlock the user account

#usermod -U username ↵

Note: When an account is locked it will show ! (Exclamation mark) in /etc/shadow file.

Userdel: Removes a user or System account.

Syn: userdel [options] LOGIN

-f forces deletion of the user even if he's still loged in.

-r Removes the user's home directory and mail spool.

Ex: #userdel username ↵

passwd: Sets a password or resets a password for a user account.

Syn: passwd [options] [LOGIN]

-l → Locks a user's account

-u → Unlocks a user's account

Ex: #passwd raju↵

→ Let's look at how the password files work.

#cat /etc/shadow | grep raju↵

Chage: Enables you to modify the parameters surrounding passwords (complexity, age, expiration)

Syn: chage [options] user

-d Indicates the day the password was last changed.

-E Sets the account expiration date

-I Change the password in an inactive state after the account expires.

-l Shows account aging information.

-m Sets the minimum number of days between password changes.

-M Sets the maximum number of days a password is valid.

-W Sets the number of days to warn befor the password expires.

Ex: → Find the user's password information.

#chage -l user↵

→ Sets user account to expire in one week

#chage -E 2013-03-28 raju↵

pwck: Verifies the consistency of passwords across database files.

→ When you create or delete users, sometimes things don't always work out properly. This can cause the password file to become inconsistent you can use the pwck command to verify the consistency between the /etc/passwd & /etc/shadow file.

#pwck ↵

Group Administration

→ Group is nothing but collection of users using which one can reduce the administration task in the o/s environment.

→ Groups are divided into two types.

(a) primary group:- It is a group in which a user initially belongs in this group the user can access the resource with default permissions.

(b) Secondary group:- A part from primary, if a user have an account in the other group i.e then it is called as secondary group to the user.

group → The group information maintained by the two database files.

(i) /etc/group: This file maintains group related information.

Syn: <group name>:<password placeholder>:<GID>:<members>

(ii) /etc/gshadow: This file maintains group password related information.

Syn: <group name>:<password placeholder>:<group admin>:<members>

groupadd: Creates a group.

Syn: groupadd [options] groupname

-r creates a system group

-g groupid

Ex: → Let's create a group called sales.

#groupadd sales ↵

→ To verify the group:

cat /etc/group | grep sales ↵

→ To add the user:

#usermod -G sales user1 ↵

#cat /etc/group | grep sales ↵

→ To add another user to the sales group

#usermod -G sales user2 ↵

→ Now if you verify, you should see two user accounts in the last field:

#cat /etc/group | grep sales ↵

→ Another way you can verify what groups a user belongs to is to use

Syn: id [options] [username]

-G Shows the GID

-n Shows the name instead of the ID

-u Shows the UID.

Ex: #id -Gn user1 ↵

→ If the ID command is called without any options, you can also see what UID & GID the user has: #id user1 ↵

groupmod: Modifies the properties of a group.

Syn: groupmod [options] groupname

-g groupid

-n newgroupname

→ To change the groupid:

groupmod -g 888 sales ↵

→ To change groupname:

#groupmod -n <new-name> <Existing name>

gpasswd:

→ Assign the password to the group:

#gpasswd <groupname>

→ Adding and Removing Members to a Group:

Syn: gpasswd [options] <arguments> <groupname>

-a Add single user

-M Add Multible users

-A Group Administrator

-d Removing a user from group

Ex: #gpasswd -a user1 Sales ↵

#gpasswd -M user2, user3, user4 color ↵

#gpasswd -d user2 color ↵

#gpasswd -A user3 color ↵

groupdel: Deletes a group.

→ To removes a group:

```
#groupdel <groupname>
```

Note: If the group has Empty (or) Secondary users you can delete the group. In case the group maintains single primary user, then you can't delete the group account.

Switching Accounts:

su: Enables you to run a command as another user or switch user accounts.

→ To switch accounts, use this command:

```
#su user1↵
```

→ you can also login as the root user using the su command:

```
#su - root↵
```

*__Tip:-__ you can log in to the root user account using the su command with no parameters. So what is the difference between using su and su- the su command moves you into the root user's account without initializing any of root's path or shell variables. When you use su -, everything is initialized as if you were logging in from the console.

User Account Initialization: When a user is created, everything from the /etc/skel directory is copied to the user's newly created home directory (usually /home/<username>).

→ you can modify these "skeleton" files or can add your own custom files. The benefit here is that user creation becomes standardized, ensuring that policies are adhered to. The customizable files are broken down into two different sections:

(a) User-Specific files:

→ After a user is created and his home directory is populated, that user can now customize those files to fit his own personal needs.

• bashrc	Defines functions and aliases
• bash_profile	Sets environment variables
• bash_logout	Defines any commands that should be executed before the users log out.

(b) Global User Configuration:

/etc/bashrc	Defines functions and aliases
/etc/profile	Sets environment variables
/etc/profile.d	Specifies a directory that contains scripts that are called by the /etc/profile file.

→ one last file to look at is /etc/login.defs. This file controls specifies relating to System wide user logins and passwords.

```
# grep -v ^# /etc/login.defs ↵
```

(or)

```
# cat /etc/login.defs ↵
```

Group Collaboration:

Group collaboration is an essential part of any business and for any system administrator who deals with users. Here we look at three key features about file and directory permissions;

(a) Setuid : This flag is used to allow multiuser access.

→ for example, if you have a script that generates reports for your company, but the script must be run as user1 to succeed, you can set the setuid bit to enable other users to run this command as through they were user1.

→ create a file to hold the report script:

```
# touch reporting_script
```

→ Set the setuid bit:

```
# chmod 4755 reporting_script
```

(or)

```
#chmod u+s reporting_script
```

→ Now view the permissions of the file:

```
# ls -l reporting_script
```

→ On the file's owner permissions, notice that there is an 's' in in place of the x. This shows that this file has the setuid flag set.

*Tip: → To find all setuid files:

```
# find / -perm 4000↵
```

(b) Setgid: This flag is used to allow multigroup access.

→ which is similar to setuid but set at the group level instead. With this bit set, all users of the group are able to execute the file instead of just the user who owns it. The setgid bit allows users to collaborate on files.

Step ①: As root, create the directory:

#mkdir /tmp/oracle ↵

Step ②: create the group and add users to it.

#groupadd Sales ↵

#usermod -G Sales user1 ↵

#usermod -G Sales user2 ↵

Step ③: Assign the permissions for collaboration:

#chown root:sales /tmp/oracle

#chmod 2770 /tmp/oracle

Step ④: verify #ls -ld /tmp/oracle ↵

→ Now all members of the Sales group are able to read/write to files within this folder. Also, notice that access to this folder is denied for anyone who isn't a members of the sales group.

(c) Sticky bit: This flag prevents accidental delete by users & groups

Step ①: Set the sticky bit on the /tmp directory:

#chmod 1777 /tmp ↵

Step ②: verify #ls -ld /tmp ↵

→ for the sticky bit, there is a 't' on the end of the permissions listed.

Now Otherusers are not able to delete your files; only you can.

→ This feature might be helpful when you're sharing files and there are particular files you don't want other users to delete.

—x—

Networking

→ One of the key elements of connecting to different systems in the network configuration involved.

→ A Network is a set of hardware devices connected together, either physically or logically to allow them to Exchange information.

→ Network management is fairly easy when it comes to Red Hat.

→ Most of the network configuration is kept in files; therefore, adjusting these settings is simple.

→ In the network system maintains the fully Qualified Domain name

∴ F.Q.D.N = Hostname + Domain name

→ Let's start by looking at the information about hostname & Networking

→ To check the hostname: # hostname ↵

→ To Managing hostname temporarily:

hostname Server1254 ↵

→ To Managing permanently: #vim /etc/Sysconfig/network ↵

NETWORKING=yes

HOSTNAME=Server1254

NETWORKING_IPV6=yes

→ for avoiding gorephical problems:

#vi /etc/hosts ↵

192.168.0.254 Server1254.Example.com Server1254

:wq! ↵

→ **TO Managing IP-Address:**

→ TO Check the ipaddress:

Syn: ifconfig [options] [interface]

options: netmask
up
down

Ex: #ifconfig eth0↵

→ TO display all interfaces on the System

#ifconfig↵

→ TO change ip address temporarily:

Syn: #ifconfig eth0 <ip-address> netmask <Subnetmask> <up/down>

#ifconfig eth0 192.168.0.254 netmask 255.255.255.0 up↵

#ifconfig eth0↵ To verify:

→ TO Change permanently:

(a) #setup↵ (b) #System-config-network-tui↵

→ you could also check the output of the interface config file

#vim /etc/sysconfig/network-scripts/ifcfg-eth0↵

DEVICE=eth0
BOOTPROTO=None
ONBOOT=yes
IPADDR=192.168.0.254
NETMASK=255.255.255.0

:wq↵

→ To check the interface detected (or) not:

Syn: #ethtool <interface>

#ethtool eth0↵

→ To bring the single interface down:

#ifdown eth0↵

→ To restore the interface that you just brought down:

#ifup eth0↵

* Note:

→ Any time you make a change to an interface's settings, you need to bring down that interface and then bring it back up again.

WARNING: Restarting the network service interrupts all network connections and any client that is currently connected.

→ Restart the network service as follows:

Syn: # service <service name> <stop/start/restart/status>

service network restart↵

→ To check the all services status:

#Service --status-all↵

→ To Manage peramently:

Syn: #chkconfig --level <runlevels> <servicename> <on/off>

chkconfig network on↵

→ To check the status of the service:

#chkconfig --List network↵

→ To disable the service at boot time: #chkconfig network off↵

Routing: When you have a system that has two or more network interfaces, they are called dual-homed (or) multihomed systems. You need to make sure that each interface has a gateway that it can route through.

Syn: route [options]

add	Add a net route
del	Deletes an existing route
flush	Flushes any temporary routes

→ Let's look at the current routes on the system:

#route ↵

→ To set default gateway:

#route add default gw 192.168.0.1 eth0 ↵

→ To verify: #route ↵

Networking utilities:

ping: Tests the connectivity between two hosts

#ping 192.168.0.254 ↵

→ When you ping something on a linux host, unlike in windows, the ping continues until you cancel it. You can limit the number of ping requests sent by prefixing -c number_count in front of the destination host.

#ping -c 3 192.168.0.254 ↵

netstat: Shows information about connections (open, closed and listening).

→ Using netstat command to obtain information on routing tables, listening sockets, and established connections.

Syn: netstat [options]

Options:

-r	Displays the routing table.
-I	Displays interface statistics
-t	Shows tcp connections
-u	Shows UDP connections
-a	Displays all sockets (tcp, udp, or local)
-p	Displays process ID's
-e	Displays Extended information.

→ To check that the connection is available for your clients:

```
#netstat -tuape | grep ssh ↵
```

Client DNS Troubleshooting:

/etc/sysconfig/network	: contains the hostname of the system.
/etc/hosts	: contains the local IP to hostname mappings
/etc/resolv.conf	: contains the Ip address of the DNS servers
nslookup	: Queries (or) looks up a domain name or system
ping	: Test connectivity between two hosts.

Ethernet Bonding :

Ethernet bonding is used to combine multiple interfaces into one, creating an increase in available bandwidth and redundancy. This is done by creating a special network interface file called as a channel bonding interface.

package Management

→ Software is the basic of any operating System, allowing you to install and use different utilities.

→ In Linux, Software is distributed through the use of packages, which contain the actual software files.

→ Each distribution of Linux has its own package management System.

→ For RedHat, there are two package management systems : RPM & YUM.

Working with RPM:

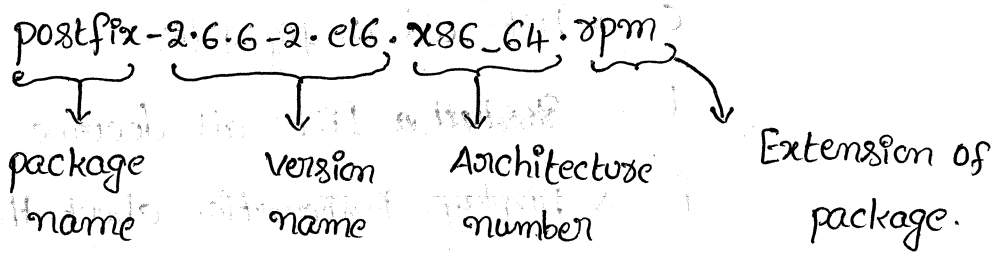
→ RPM stands for (Red Hat package Manager)

→ RPM is default package installation tool in Linux operating System.

→ By using Rpm we can install, upgrade, query, verify and Remove the packages.

→ Before diving into package management, let's look at the naming convention used by the system to describe packages.

package parameters :



Methods of Installation:

→ Two ways of Installations.

- Standalone
- Network.

Standalone: In this type, we can install the packages through any removable media (or) through dump.

Installing and Removing packages:

Syn: #rpm <options> <pkg-name> --force --aid

options: i → Installs a given package

v → verbose output.

h → Shows hash progress when installing

U → Upgrades a given package

e → Removes a given package.

--force → Install the package with forcefully.

--aid → Install the package along with Dependencies

--nodeps → To Erase an package without dependencies.

Quary Options (with -q):

Syn: #rpm <options> <pkg-name>

c → Lists all config files.

d → Lists all documentation files.

i → Displays information about the package.

l → Lists the files in a package.

s → status of the package.

verify options (with -v):

-a → Queries all packages

f → Displays information about the specified file.

→ for installing an application.

```
#rpm -ivh nano-2.2.6-1.x86_64.rpm ↵
```

→ for installing an application with forcefully.

```
#rpm -ivh nano-2.2.6-1.x86_64.rpm --force ↵
```

→ If you want to upgrade this package (because you know that it is already installed), you can substitute the -i option for -U.

```
#rpm -Uvh nano-2.2.6-1.x86_64.rpm ↵
```

→ for uninstalling a package

```
#rpm -e nano ↵
```

→ you can always reinstall the package at a later date if you keep the .rpm file on your system

```
#rpm -ivh -replacepkgs nano-2.2.6_1.x86_64.rpm ↵
```

Tip: A common situation to run into on the job is having to install a package that is already installed. you don't have to go through the trouble of uninstalling the package first only to reinstall it. you can use the -replacepkg option alongside the regular install options to override an Existing installation.

→ Query the instal'ed System package for nano:

```
#rpm -qa | grep nano ↵
```

→ Query the information from the nano package:

```
#rpm -qi nano ↵
```

→ Suppose you are looking around on your new Red Hat installation and a file but aren't sure what it does. you can use the -f option to query the package that the file belongs to, possibly giving you a better idea of what that file might be used for.

→ find out where the /etc/Syslog.conf file came from by doing the following

#rpm -qf /etc/Syslog.conf↵

→ Use the -c option to find all config files

#rpm -qc rsyslog ↵

→ To find the documentation files for a given package.

#rpm -qd rsyslog ↵

→ To listing of all files that come with the package.

#rpm -ql rsyslog↵

→ To find out whether a package has any dependencies:

#rpm -qR rsyslog↵

Network installation: In this level we can install the package from Server through NFS (or) FTP services.

NFS service: → first check the communication.

#ping 192.168.0.254↵

→ for accessing the data shared from Server

#mount 192.168.0.254:/var/ftp/pub/Server /mnt↵

#cd /mnt↵

#rpm -ivh vsftpd* --force --aid↵

FTP Service: In this method to install the package the ftp server should have the dump of o/s under the ftp default shareable location.

→ first check the communication

#ping 192.168.0.254 ↵

→ for accessing the data shared from the server.

#rpm -ivh ftp://192.168.0.254/pub/Server/<pkg-name> --force --aid

Working With YUM:

→ yum stands for yellowdog update Modifier.

→ In this section, we look at the exact same tasks, except this time we use the more flexible yum utility.

→ The yum command has access to repositories where tons of packages are kept and can install, upgrade, or remove them for you automati -cally.

→ yum also takes care of resolving and installing any dependencies for you, which the rpm command can't do.

→ yum is an interactive tool which waits for the confirmation of a user.

→ yum is a default package management tool in RedHat o/s.

→ Using this tool we can install the required packages with dependencies.

Syn: yum <options> <Commands> <package name>

Options:

c → Specifies the location of the config file.

q → Specifies quit, no output.

y → To always answer yes to prompts.

v → provides verbose output.

Commands:

clean → Removes cached data.

erase → Removes a package from the System.

List → Displays available packages

Install → Install a package on the System.

Search → Enables you to search for a package.

Update → Updates a package.

grouplist → Displays available packages groups.

groupinstall → Install a packages with in a group.

groupremove → Removes a packages with in a group

YUM Server configuration:

→ Mount the dvd

#mount /dev/dvd /mnt↵

→ Install RPM package (vsftpd)

#rpm -ivh vsftpd* --force --aid↵

→ Copy the Dump of o/s into the default sharable location ftp.

#cp -rvf /mnt/* /var/ftp/pub ↵

* → means all the data under the mount point /mnt.

→ Install the createrepo package:

#rpm -ivh createrepo* --force --aid ↵

→ Create the new Repository:

#createrepo -g /~~mnt~~var/ftp/pub/Server/repodata/comps-rhel5-server-core.xml /var/ftp/pub ↵

Note: If any errors are showing then remove

#rm -rf /var/ftp/pub/repodata ↵

→ Open the yum configuration file:

#vim /etc/yum.repos.d/linux.repo ↵

1. [linux]
2. name=yum Server
3. baseurl=ftp://192.168.0.254/pub
4. Enabled=1
5. gpgcheck=0

:wq! ↵

→ Restart the ftp service

service vsftpd restart ↵

yum clean all ↵

→ To list out packages

```
#yum list ↵
```

→ To install the package

```
#yum install postfix -y ↵
```

→ you could also update the postfix package

```
#yum update postfix -y ↵
```

→ To remove the package

```
#yum remove postfix ↵
```

Note: one great feature about yum is that instead of updating a single package, you can list all updates that need to be installed for the system.

```
#yum list updates ↵
```

→ from this list, you can choose to update packages individually or as a whole. If you want to install all the updates

```
#yum update ↵
```

→ To get a listing of all available "groups":

```
#yum grouplist ↵
```

→ you can then install that "groups":

```
#yum groupinstall "Development Tools" ↵
```

Note: Don't forget that Linux doesn't handle whitespace the way that Windows does. If you specify a group name, you need to enclose it in quotation marks (" ").

Searching for packages:

→ find the postfix package to install:

```
#yum search postfix↵
```

→ To find out more information about the postfix package:

```
#yum info postfix↵
```

→ To flush the cache, do the following

```
#yum clean all↵
```

Configuring Additional Repositories:

→ Some times you might want to install a package that isn't in the repositories that come preconfigured with Red Hat. If the package is available in someone else's repository, you can add that person's repository to your yum config file.

→ you can either add your own custom repositories to the main config file /etc/yum.conf (or) create a .repo file in the /etc/yum.repos.d directory which will be added automatically. Here is what a sample entry for a custom repository looks like:

```
[unique title]
name=My custom yum Repository.
baseurl=ftp://192.168.0.250/opt/yum/myrepos
enabled=1
gpgcheck=0
```

•1.03 1 ↵

→ One neat trick that you can do is to create a repository based on an ISO.

→ This trick can be useful in an environment whether there is no Internet access and you'd like to install packages from the Red Hat DVD.

Step ①: Create a folder for the temporary mount:

```
#mkdir /mnt/cd ↵
```

Step ②: Mount the ISO image (or) cd:

```
#mount -o loop /dev/cdrom /mnt/cd ↵
```

Note: → To create a ISO image.

```
#dd if=/dev/scd0  of=/OS/Rhel5.iso ↵
```

↳ To check it which device is mount

→ Read the image file

```
#mount -o loop /OS/Rhel5.iso /DVD ↵
```

Step ③: Create a repository in the temporary directory:

```
#cd /mnt ↵
#createrepo . ↵
```

This creates an XML file of all the packages from the mounted CD.

Step ④: You also need to clean the current repository cache:

```
#yum clean all ↵
```

Step ⑤: Create a .repo file for your temporary repository:

```
#vim /etc/yum.repos.d/iso.repo↵

[ISO Repo]

name=My Repository.

Baseurl=file:///mnt/cd

enabled=1

gpgcheck=0

:wq! ↵
```

Adding your custom packages:

→ Just as you have already created two different types of custom repositories, you can add packages you have created to them as well.

Step ①: copy the file over to your private directory.

```
#cp /usr/src/redhat/RPMS/X86_64/mysample-1.0-0.X86_64.rpm
   /opt/yum/myrepos↵
```

Step ②: Update the repository to recognize your new package:

```
#createrepo -update↵
```

→ Now you should be able to search for your package in your private repository along with other software.

Registering your System:

To register your system to the Red Hat Network, you must have an active subscription with Red Hat. you can register during the installation of your system or manually after the system has already been installed. Use the 'rhn_register' command to begin the registration process. After you finish, you can visit http://rhn.redhat.com to start managing your system(s) through the web. you need to make sure that the rhnsd daemon is running in order for it to be managed.

Step ①: Set the daemon to boot on System start

```
# chkconfig rhnsd on ↵
```

Step ②: you should verify whether the service is currently running.

```
# service rhnsd status ↵
```

Step ③: If it is, you are all set; otherwise, start the service manually:

```
# service rhnsd start ↵
```

—— x ——

The Kernel

→ The heart of Red Hat is the Linux kernel. The kernel is responsible for interacting with the hardware and producing output to the screen. There is also a virtual file system that gets created in the /proc directory to hold information and parameters for the kernel.

→ Linux is truly just the kernel. Red Hat and the other distributions in existence today are software and configuration files packaged with the Linux kernel to bring you an entire operating system. Because the kernel is really what runs everything, understanding how it works is essential.

→ The kernel can be used to load new drivers, support new hardware, or even offer a custom kernel for individual needs.

→ The Linux kernel is modular, and because of this, you can load and unload kernel modules even after the system has booted.

→ Let's start with the uname command to find out some info, about the kernel.

uname: Displays information about the kernel.

Syn: uname [option]

-a	prints all information relating to the kernel
-s	Show the kernel name
-r	Requests kernel release information
-v	Requests the kernel version.

→ Let's check & see which version of the kernel is currently running:

```
#uname -a ↵
Linux root 2.6.32-71.el6.x86_64 .....
```

*Note: The kernel version numbering is important here. The first number is the major version of the kernel. The second number is the major release of the first number. If the release number is even, which it is (6), it means that this is a stable release of the kernel. Odd numbers are development kernels and should not be used for production systems. The third number is the patch version of the kernel. The last number (71) is added by Red Hat to represent its release version of the kernel. Also note the el6, which tells you that you are running Red Hat Enterprice Linux 6. If you couldn't tell, this is an x64-bit version of the operating system.

→ To get the version of the currently installed kernel:

```
#rpm -qa | grep kernel ↵
```

→ you could also use the following:

```
#rpm -q kernel ↵
```

When it comes to working with kernels, you should be familiar with different locations. Let's look at four of these locations:

/boot : place where the kernel and boot files are kept.

/proc : current hardware configuration & status.

/usr/src : Source code of the kernel.

/lib/modules : kernel modules.

lsmod : Lists currently loaded kernel modules

Syn: lsmod

→ To look at what is currently loaded by the kernel since you booted the system, you use the following command:

```
#lsmod ↵
```

Module	Size	Used by
autofs4	29253	3
hidp	23105	2
rfcomm	42457	0
l2cap	29505	10 hidp, rfcomm
ext4	353979	2

[output truncated]

→ The preceding output is truncated due to size.

→ Shows the details of the ext4 kernel module listed previously:

modinfo: Displays information about a kernel module

```
#modinfo ext4 ↵
#modinfo cdrom ↵
```

→ To find all the kernel Modules:

→ All the kernel modules will be residing in /etc/lib/modules directory

```
# cd /etc/lib/modules ↵
# ls ↵
```

→ To Search all the kernel modules in the system using find Cmd:

```
# find / -name *.ko ↵ (Modules in the System will be
                       ending with .ko extension)
```

→ To Remove

modprobe :→ To remove the loaded module

Syn: modprobe <modname>

#modprobe -r vfat ↵

→ Now to check

lsmod | grep -i vfat ↵

→ To install/re-install a module:

#modprobe vfat ↵

lsmod | grep -i vfat ↵

* Updating the kernel:

→ View the current version of the kernel:

#uname -r ↵

→ To view kernel package information

yum info kernel ↵

(or)

#rpm -qa | grep kernel ↵

→ Using the package manager, you can upgrade the kernel to the latest version:

#yum update kernel -y ↵

(or)

#rpm -ivh kernel-2.6.18-194.3.1el5 ↵

*
Note: When updating a kernel with the rpm command, never use the -U option to update. The reason behind this is that the update option erases the prior kernel when updating, whereas the -i option installs the newer kernel alongside the old kernel. If something doesn't work or goes wrong, you have an older kernel to revert to.

Tuning the kernel with /proc/sys:

→ The kernel has a virtual file system, /proc/sys, that allows you to tune the kernel while the system is running.

→ The kernel creates the /proc/sys virtual file system when the system boots up, which holds all the parameters of the kernel. This virtual file system is then used to manipulate kernel parameters for testing purposes (these changes are valid only until the system reboots).

→ When you have the kernel tuned the way you'd like, you can simply have your settings applied when the system boots (through a special config file), or you can compile your own kernel to have them built in permanently

→ As you are testing kernel changes, make sure you don't rely on any settings made within the /proc/sys file system because they are erased when the system reboots. During testing, you can use the echo cmd to change the values of the kernel while the system is running.

Step ①: View the current value in the kernel:

```
#cat /proc/sys/net/ipv4/ip_forward ↵
```

Step ②: change the kernel option that controls packet forwarding:

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

Step ③: verify the value has changed:

```
#cat /proc/sys/net/ipv4/ip_forward ↵
```

→ If you want the changes to be persistent across system reboots, you can put the parameters you'd like to remain during boot in the /etc/sysctl.conf file.

Sysctl: Enables you to tune kernel parameters.

→ Before you start tuning things, let's look at all the available options:

```
#Sysctl -a ↵
```

→ Now, let's make the same changes to the kernel as before.

Step ①: query the parameter responsible for forwarding packets within the kernel

```
#Sysctl -a | grep ip_forward ↵
```

Step ②: using Sysctl to change the option:

```
#Sysctl -w net.ipv4.ip_forward=1
```

↳ Enables you to change a settings in the sysctl config file.

Step ③: verify the value has been changed:

```
#Sysctl -a | grep ip_forward ↵
```

Step ④: Return the parameter to its original value:

```
#Sysctl -w net.ipv4.ip_forward=0 ↵
```

* Disks & partitioning *

→ Disk partitioning is one of the many steps you must take when preparing a system for use.

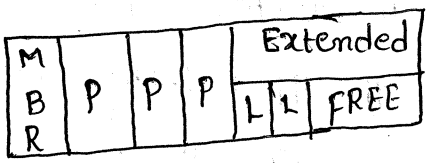
→ partitioning means to divide a single hard drive into many logicall drives.

→ In Each system the physical disk drivers are divided up logically into partitions that allow you to store data on them.

→ there are also special types of partitions such as RAID that allow for increased performance, redundancy, or both. LVM, like RAID, is an advanced form of partitioning that eases management of partitions and makes growing them for increased storage capacity simple.

→ one of the key points to remember when working with partitions is to always plan ahead

⇒ Disk partitioning Criteria:



MBR → Master Boot Record.

P → primary partition

Extended → Extended partition

L → Logical partition

Free → Force space.

→ Every disk can have only 3 primary partitions.

→ primary partition is a partition which usually holds the operating system

→ Extended partition is a special type of primary partition which can be subdivided into multiple logical partitions.

→ Logical partitions are the partitions which are created under Extended partitions

→ As in the real world, it is the results that matter. It doesn't matter whether you use Disk Druid, fdisk, or parted to create partitions. you can create new partitions at the command line or use GUI front ends to these tools such as the Disk utility.

→ Remember Disk Druid is available only during the installation process.

→ you can use two different utilities when partitioning disks:

fdisk → Disk partitioning utility

parted → Another Disk partitioning utility.

→ while fdisk is more common, it is slowly being replaced by parted, which is more flexible.

⇒ **Disk identification:**

→ Different types of disks will be having different initials in linux

IDE drive will be shown as /dev/hda

SCSI/SATA drive will be shown as /dev/sda

Virtual drive will be shown as /dev/vda

Note: The first two letters represent whether the disk is a SCSI (Sd) (or) IDE (hd) disk. The third letter represents which disk it actually is. If there is a number after the three letters, it is the number of the partition.

→ To view information about the current partition layout,

#cat /proc/partitions | grep hd ↵ for IDE

#cat /proc/partitions | grep sd ↵ for SCSI/SATA

→ you need to view their current partitions to see if any exist.

Syn: fdisk [options] [Device]

-options: -b Specifies the sector size of the disk
-h number of heads on the disk
-l Lists current partition table.

Note: There are some limitations when it comes to working with partitions. you can have only four partitions to a physical disk with one exception. If you want to make more than the four, you need to create three primary partitions and one Extended partition, although the primary partitions aren't required for extended partition creation. the Extended partition can then hold 11 logical partitions (5-16) on it.

⇒ **Creating a partition:**

Step①: #fdisk /dev/sda ↵

Step②: view all the options available to you

Command (m for help): m ↵

p	print the partition table
n	add a new partition
d	Delete a partition
m	print this menu
q	quit without saving changes
t	change a partition's System id
w	write table to disk and Exit

→ Create a new partition

#fdisk /dev/sda ↵

: n ↵

First cylinder (1-1044, default 1): ↵

Using default value 1

Last cylinder or +size ..... (1-1044, ...): +500M ↵

→ Create a second partition

: n ↵

.....

→ Verify newly created partitions

:p ↵

→ Write the changes to disk

:w ↵

→ Now that two new partitions have been created and written to disk, you should verify their existence. Before doing that, however, you want the kernel to reread the partition table to make sure that it recognizes all disks and partitions correctly. To do this, you use the partprobe cmd.

Syn: partprobe [options] [Device]

-d Does not actually inform the operating system

-s prints a summary of contents.

→ Now call the partprobe command

#partprobe /dev/sda ↵

→ Now that you have created partitions with the fdisk utility, do it again using the parted command

→ Create a partition:

#parted /dev/sda ↵

→ Menu (parted) help ↵

→ Create your first partition in a similar manner to fdisk:

(parted) mkpart ↵

partition type? primary/Extended/logical?

File System type? [Ext2] ?

Start ?

End ?

→ Make your second partition again

→ Before writing changes to disk, you should verify that they have been created the way you want them:

(parted) print

→ Exit the program to save your changes

(parted) quit↵

→ There are a few things you should notice here. First, you need to specify exactly where you want the start and end of the partition to be. If you don't plan this out ahead of time, you will end up with incorrect partition sizes. You should also take note of the fact that you don't have to write the changes to disk manually; this is done for you when you quit the parted program.

→ Again, you need to force the kernel to reread the partition table

#partprobe

→ Once again, verify that your partitions have been created successfully:

#parted -l↵

⇒ <u>Deleting a partition:</u> Deleting a partition is much easier than creating one because you need to specify only the partition number that you want to delete.

→ Start the fdisk utility: #fdisk /dev/sda↵

:p↵ printout the current partition

:d↵ Delete a partition

:6↵ & want to delete 6th partition

:w↵ write changes to disk

→ Don't forget to reread the partition table

#partprobe /dev/sda↵

→ Start the parted utility: # parted /dev/sda↵

(parted) print↵

(parted) rm 5↵

* File System *

→ It is method of storing the data in an organized fashion on the disk. Every partition on the disk except MBR and Extended partition should be assigned with some file system in order to make them store the data.

→ File System is applied on the partition by formatting it with a particular type of a file system.

→ The number of file system types may exceed the number of operating systems. while RHEL can work with many of these formats, the default is Ext4. while many users enable other other file systems such as ReiserFS, Redhat may not support them.

→ Before the partitions can be used, however you need to create a file system for each one.

→ The default file system for RHEL5 is Ext3 and has been changed to Ext4 for RHEL6. Both of these file systems offer a journaling option, which has two main advantages.

(i) It can help speed up recovery if there is a disk failure because journaling file systems keep a "journal" of the file system's metadata.

(ii) It can check drivers faster during the system boot process.

→ The journaling feature isn't available on older file systems such as Ext2.

→ The first Linux operating systems used the Extended File System (ext) until the last few years, Red Hat linux operating systems formatted their partitions by default to the seconded Extended file system (Ext2). For RHEL 5, the default was the third Extended file system (Ext3). The new default for RHEL6 is the Fourth Extend file System (Ext4).

→ Ext file system is the widely used file system in Linux, whereas vfat is the file system to maintain a common storage between Linux and windows (in case of multiple o/s)

Ext2	Ext3	Ext4
① Stands for second Extend file System.	→ Third Extend File System	→ Third Extended file System.
② Introduced in 1993	→ Introduced in 2001	→ Introduced in 2008.
③ Does not have journaling	→ Support journaling	→ Support journaling
④ Maximum file size can be from 16GB to 2TB	→ 16GB to 2TB	→ 16GB to 16TB
⑤ Maximum Ext2 file System size can be from 2TB to 32TB.	→ 2 TB to 32 TB	→ Maximum Ext4 file System size is 1 EB (Exabyte). 1 EB = 1024 PB (peta byte) 1 PB = 1024 TB (Tera byte)

→ There are many types of file Systems

Swap: the Linux swap filesystem is associated with dedicated swap partitions. you've probably created at least one swap partition when you installed RHEL.

MS-DOS & VFAT: these file systems allow you to read MS-DOS ~~command~~ formatted file Systems. MS-DOS lets you read pre-windows 95 partitions, or regular Windo partitions within the limits of short filenames. VFAT lets you read windows 9x/NT/2000/vista/7 partitions formatted to the FAT16 or FAT32 file systems.

ISO 9660: the standard file System for CD-ROMs. It is also known as the High sierra file System, or HSFS, on the unix systems.

/proc: A Linux virtual filesystem. Virtual means that it doesn't occupy real disk space. Instead, files are created as needed. Used to provide information on kernel configuration and device status.

/dev/pts: the Linux implementation of the Open Group's Unix98 PTY support.

JFS: IBM's journaled filesystem, commonly used on IBM Enterprice Servers.

ReiserFS: The ReiserFS File System is resizable and supports fast journaling. It's more efficient when most of the files are very small and very large. It's based on the concept of "balanced trees". It is no longer supported by RHEL, or even by its former main proponent, SUSE.

xfs: Developed by Silicon Graphics as a journaling filesystem, it supports very large files; as of this writing, xfs files are limited to 9×10^{18} bytes. Do not confuse this file system with the X font server, both use the same acronym.

NTFS: The current Microsoft Windows file system.

⇒ Creating a file system:

→ When you're creating a file system, there are many different ways to complete the same task.

→ They're all based on the mkfs command, which works as a front end to filesystem-specific commands such as mkfs.ext2, mkfs.ext3, and mkfs.ext4.

Syn: mkfs [options] [Device]

-j creates a journal option

-m specifies a reserved percentage of blocks on a file system.

→ There are two ways to apply formatting on a volume. For Example, If you've just created a partition on /dev/sda5

#mkfs -t ext4 /dev/sda5

#mke2fs -t ext4 /dev/sda5

#mkfs.ext4 /dev/sda5.

→ If you want to reformat an existing partition, Logical volume, or RAID array, take the following precautions.

- Backup any existing data on the partition
- Unmount the partition.

→ you can format partitions, Logical volumes, and RAID arrays to other filesystems. The options available in RHEL 6 include:

- mkfs.cramfs	creates a compressed ROM filesystem.
- mkfs.Ext2	formats a volume to the Ext2 filesystem.
- mkfs.Ext3	formats a volume to the Ext3 filesystem.
- mkfs.Ext4	formats a volume to the Ext4 filesystem.
- mkfs.msdos (or) - mkfs.vfat (or) - mkdosfs	formats a partition to the microsoft compatible VFAT filesystem; it does not create bootable filesystems.
- mkfs.xfs	formats a volume to the xfs filesystem developed by the former Silicon Graphics.
- mkswap	formats a volume to the Linux swap file system.

→ one advantage of some rebuild distributions is the availability of useful packages not supported by or available from Red Hat. For Example, CentOS 6 includes the ntfsprogs package, which supports the mounting of NTFS partitions.

⇒ Creating a Swap :-

→ In Linux, a swap space is used as a "scratch space" for the system. When the system runs low on memory, it uses the swap as a virtual memory area to swap items in and out of physical memory. Although it should not be used in place of physical memory because it is much slower, it's critical piece of any system.

→ There are two different types of swaps that you can have:

① File swap

② partition swap

partition swap:

Step ①: → Create a partition

```
#fdisk /dev/sda ↵
```

Step ②: → update to kernel

```
#partprobe /dev/sda ↵
```

Step ③: → use the mkswap command to create a swap space

Syn: mkswap [options] [Device]

-c checks the device for bad blocks before creating the swap area.

```
#mkswap /dev/sda8 ↵
```

Step ④: → Enable the swap partition

```
#swapon /dev/sda8 ↵
```

Step ⑥: → Verify the swap is running correctly

```
#swapon -s ↵
```

Syn: Swapon [options] [Device]

-a Enables all swap devices

-e Silently skips devices that don't Exist

-s verifies that the swap is running

Step ⑦: → If you want to turn off the swap, you can use the Swapoff command.

Syn: Swapoff [options] [Device]

-a Enables all swap devices

-e Silently skips devices that don't Exist

-s verifies that the swap is running

File swap: you can use the dd command to reserve space for another swap on the /dev/sda9 partition.

→ The dd command can be used for many different purposes and has a huge syntax

Step ①: → Reserve 1GB of space for the swap

```
#dd if=/dev/zero of=/mnt/file_swap bs=1024 count=1000000
```

Step ②: → Just as with partition swaps, you can now create a swap space specifying the device file just created

```
#mkswap /mnt/file_swap↵
```

Step ③: → Enable the swap

```
#swapon /mnt/file_swap
```

Step ④: → Again you can verify that the swap is enabled

```
#swapon -s↵
```

Note:

* → The big difference between the two swap types is that file swap is easier to manage because you can just move the swap file to another disk if you want. The swap partition would need to be removed, re-created, and so on. Although Red Hat recommends using a partition swap, file swaps are fast enough these days with less administrative overhead to not use them instead. One word of caution, though, is that you can use only one swap (of either type) per physical disk.

⇒ Mounting a file System:

→ After formatting a partition we cannot add the data into the partition. In order to add the data in the partition it is required to be mounted.

→ Mounting is a procedure where we attach a directory to the file system.

→ they can be mounted to any directory, which is refferred to as a mount point. Every mount point before is a directory.

→ If you mount a file System on a directory that is not Empty, Everything within that directory becomes inaccessible. Therefore, you should create a new directory as a mount point for each of your file Systems.

→ there are only two commands for mounting a file Systems:

mount	Mounts a file System.
umount	Unmounts a file System.

Step①:→ Start by going to the /opt directory, where you can make some directorys to serve as a mount points.

```
#cd /opt↵
#mkdir company_data ↵
#mkdir backup ↵
```

Syn: mount [options] [Device] [Mount_point]

-r	Mounts as read-only
-w	Mounts as read/write (the default)
-L LABEL	Mounts the file System with the name LABEL
-v	provides verbose output.

Step②: → Mount the two file systems

```
#mount /dev/sda6 /opt/company_data ↵
#mount /dev/sda7 /opt/backup ↵
```

* → Notice that you don't specify a file system type or any mount options. The reason is that the mount command automatically detects the file system type and mounts it for you. By default, the file system is also mounted with the defaults option (rw).

Step③: → To unmount a file systems:

Syn: umount [options] [Mount_point]

-f Force unmount.

-v provides verbose output.

Step④: → you can use the "fuser and lsof" commands to check for open files and users that are currently using files on a file system

Syn: fuser [options] [Mount_point / File System]

-c checks the mounted file system

-k kills processes using the file system

-m Shows all processes using the file system.

-u Displays user IDs

-v Verbose output.

→ Check to see what users are currently using the file system

```
#fuser -cu /dev/sda6 ↵
```

(or)

```
#lsof /dev/sda6 ↵
```

→ To kill the open connections, you can use the fuser cmd again:

```
#fuser -ck /opt/backup ↵
```

→ Now you should be able to unmount the file system:

```
#umount /opt/backup ↵
```

→ Now you know how to mount and unmount file systems, but there is something else you need to look at: If you reboot your system right now, all the file systems that you just mounted will no longer be available when the system comes back up. Why? The mount command is not persistent, so anything that is mounted with it will no longer be available across system reboots. & Suppose you want to know how to fix that, right? The system looks at two config files

/etc/mtab	contains a list of all currently mounted file systems
/etc/fstab	Mounts all listed file systems with given options at boot time.

→ View the /etc/mtab file:

```
#cat /etc/mtab ↵
```

Every time you mount or unmount a file system, this file is updated to always reflect what is currently mounted on the system

→ you can also query to check whether a particular file system is mounted

```
#cat /etc/mtab | grep backup ↵
```

→ you can use the mount command with no options to also view the currently mounted file systems:

#mount ↵

→ Go through the /etc/fstab file. The file follows this syntax:

<device> <Mountpoint> <file System type> <Mount options> < write data during shutdow>

<Check sequence>

→ View the /etc/fstab file:

#cat /etc/fstab ↵

*→ The first three fields should be fairly obvious because you have been working with them throughout the chapter. The fourth field defines the options that you can use to mount the file system. The fifth field defines whether data should be backup (also called dumping) before a system shutdo or reboot occurs. This field commonly use a value of 1. A value of 0 might be used if the file system is a temporary storage space for files, such as /tmp. The last field defines the order in which file system checking should take place. For the root file system, the value should be 1; everything else should be 2. If you have a removable file system (CD-ROM (or) External you can define a value of 0 and skip the checking altogether. Because you want the two file systems created earlier to be mounted when the system boots, you can add two definitions for them here.

→ open the /etc/fstab file for editing:

#Vim /etc/fstab ↵

/dev/Sda6 /opt/backup Ext3 defaults 0 0

:wq! ↵

→ you can use the mount command with -a options to remount all file systems defined in the /etc/fstab file

```
#mount -a ↵
```

⇒ Extra file System commands:

Label: Labels enable you to determine a specific file system more easily with a common name, instead of /dev/sda6. An added benfit is the system's being able to keep its label even if the underlying disk is switched with a new one.

Step①: → Take your file system offline

```
#umount /dev/sda6 ↵
```

Step②: → Let's label the file system ~~CDdata~~ ~~CD~~data to denote that it's the company_data file system.

```
#e2label /dev/sda6 CData ↵
```

Step③: → you can use the same command to also verify:

```
#e2label /dev/sda6 ↵
```

Step④: → Find the file system you just labelled:

Syn: findfs LABEL=<label> | UUID=<uuid>

```
#findfs LABEL=CData ↵
```

→ you can also query more information about the device using the blkid command.

Syn: blkid [options]

-s Shows specified tag(s)

dev Specifies the device to probe.

Step⑤ :→ Combine the blkid cmd with grep for specific results

```
#blkid | grep cData↵
```

Step⑥ :→ When you finish your maintenance, you can remount the file system with the new label instead of the device path:

```
#mount LABEL=CData /opt/company_data↵
```

→ you could even update the /etc/fstab file to use the label information instead of the device path.

```
#vim /etc/fstab↵
```

```
LABEL=CData    /opt/company_data    Ext3    defaults    0 0
```

```
:wq!↵
```

→ you can use the mount command to verify the label names

```
#mount -l↵
```

→ you also can use the df command to view the usage information for your file systems:

Syn: df [options]

-h specifies human-readable format

-l Local file systems only

-T print the file system type

```
#df -h↵
```

```
#df -Th↵
```

⇒ Managing file System quotas :-

→ Quotas are used to restrict the amount of disk space occupied by users or groups.

→ Quotas regulates disk consumption of users. It improves System performance.

→ Quotas are two types

① User level

② Group level

→ If we apply quotas on a group level it will effected to only the primary users of that group.

→ Quotas can be applied only quotas enabled partitions.

→ you need to install the required packages before you can use quotas on your System.

Step ①: → To install the quota package

#yum install -y quota ↵

Step ②: → Verify that the package was installed successfully

#rpm -qa | grep quota

Step ③: → you can query quota support from the kernel with the following command

#grep -i config_quota /boot/config-`uname -r`

→ Now that you have a listing of the commands you can use, you first need to edit the /etc/fstab file to specify which file systems you want to utilize quotas.

Step ①: → open the /etc/fstab file, Edit the following line

/dev/sda6 /opt/company_data Ext3 defaults, usrquota, grpquota

1 ↵

→ Now you need to remount the /opt/company_data file System before the changes take effect.

Step ②: → you can accomplish this by using the mount command:

#mount -o remount /opt/company_data ↵

Step ③: → you can verify that the mount and quota options took correctly

#mount | grep company_data ↵

→ there are two files that maintain quotas for users and groups.

aquota.users	users quota file.
aquota.group	Group quota file.

→ these two files are automatically created in the top-level directory of the file system where you are turning on quotas - in this case, the /opt/company_data file System.

Step ④: → To start the quota System, you use the quotacheck Cmd.

Syn: quotacheck [options] [partition]

-c	Don't read Existing quota files
-u	Checks only user quotas
-g	Checks only group quotas
-m	Doesn't remount the file System as read-only.
-v	provides verbose output.

#quotacheck -ugm /opt/company_data ↵

→ To verify that the quota files were created successfully

#ls /opt/company_data ↵

→ Enabling quotas: Normally, you would have to call the quotaon and quotaoff cmds to have the quota system enforced, but they are automatically called when the system boots up and shuts down.

Step ⑤: → Run the cmd manually the first time just to make sure that quotas turned on:

```
#quotaon -v /opt/company_data↵
```

→ Let's briefly discuss the two different limits you can have when dealing with quotas:

Soft Limit: Has a grace period that acts as an alarm, signaling when you are reaching your limit. If your grace period expires, you are required to delete files until you are once again under your limit. If you don't specify a grace period, the soft limit is the maximum number of files you can have.

Hard Limit: Required only when a grace period exists for soft limits. If the hard limit does exist, it is the maximum limit that you can hit before your grace period expires on the soft limit.

→ To work with quotas for users and groups, you need to do some conversions in your head here. Each block is equal to 1KB.

If you aren't good at the conversions, remember that 1,000KB = 1MB.

Step ⑥: → Set the limits for user1 by using the edquota cmd.

Syn: edquota [-u/-g] [username/groupname]

```
#edquota -u user1↵
```

filesystem	blocks	soft	hard	inodes	soft	hard
/dev/sda6	0	20000	25000	0	0	0

Step ⑦: Again, you use the edquota cmd, but with a different option:

#edquota -t ↵

→ Here, the current value is seven days for the block grace period. you should not give your users that much time to get their act together, so drop that limit to two days.

Tip: The Edquota cmd offers a pretty cool feature. After you configure a quota and your limits for a single user, you can actually copy this over to other users as if it were a template. To do this, specify the user you want to use as a template first and call the edquota cmd with the -p option.

#edquota -up user1 user2 user3 ↵

Step ⑧: Quota usage Reports:

Syn: repquota [options] [partitions]

-a Reports on all non-NFS file systems with quotas turned on

-u Reports on user quotas.

-g Reports on group quotas.

-v verbose output.

#repquota -uv /opt/company_data ↵

—X—

⇒ File System Security: Linux, like most operating systems, has a standard set of file permissions. Aside from these, it also has a more refined set of permissions implemented through access control lists.

→ this section covers both of these topics and how they are used to implement file system security for files, directories, and more.

Step①: Installing the required package

```
#yum install -y acl↵
```

Step②: verify the package installation:

```
#rpm -qa | grep acl
```

Step③: Before you can even use ACL's however, you need to make sure that the file system has been mounted with ACL parameter:

```
#mount | grep acl↵
```

Step④: you can accomplish this using the following

```
#mount -t ext3 -o acl,remount /dev/sda7 /opt/backup↵
```

Step⑤: If your file system isn't already mounted, you could also use the following:

```
#mount -t Ext3 -o acl /dev/sda7 /opt/backup↵
```

Step⑥: To verify, you can use the previous cmd:

```
#mount | grep acl
```

Step⑦: Adjust the following line in your /etc/fstab file.

```
/dev/sda7   /opt/backup   Ext3   defaults,acl   1 2

:wq! ↵
```

Step ⑧: → To make the changes take effect, you need to remount the filesyst

#mount -o remount /opt/backup ↵

→ Now verify that your file system has the ACL options:

#mount | grep -i acl ↵

→ The file system is now mounted properly with the ACL option, so can start to look at the management cmds that pertain to ACL's:

getfacl Obtains the ACL from a file or directory

setfacl Sets or modifies an ACL.

Step ①: Create a sample file on which you can test an ACL in the /opt/backu

#cd /opt/backup ↵

#touch file1 ↵

→ Now you can use the getfacl cmd to view the ACL currently associate with the file.

Syn: getfacl [options] file

-d Displays the default ACL

-R Recurses into subdirectories.

#getfacl file1 ↵

Syn: setfacl [options] file

-m Modifies an ACL

-x Removes an ACL

-n Doesn't recalculate the mask

-R Recurses into subdirectories.

Step ②: → Set the test file so that user1 also has access to this file

```
#setfacl -m u:user1:rwx /opt/backup/file1↵
```

→ To check the ACL permissions again:

```
#getfacl file1 ↵
```

Step ③: To remove the ACL for user1:

```
#setfacl -x u:user1 /opt/backup/file1
```

→ Verify the ACL has been removed:

```
#getfacl file1↵
```

Step ④: → If you have multiple ACL set up on a single file, you can remove them all with the -b option instead of removing them one by one:

```
#setfacl -b testfile ↵
```

File permissions and ACLs can get really complex if they aren't thought out ahead of time.

—x—

⇒ Logical volume Manager (LVM):

→ LVM is a form of advanced partition management. The benfit to using LVM is ease of management due to the way disks are setup.

→ LVM is a method of allocating hard drive space in to Logical volumes that can be easily resized of partition with LVM, the hard drive (or) set of hard drives are allocated to one (or) more physical volumes.

→ The physical volumes are combined into volume groups such volume group is divided into logical volumes which are assigned mount points as "/home', '/' etc. These logical volumes are formatted to Ext3 file System.

→ The LVM must follow the bellow sequence:

① physical volume.

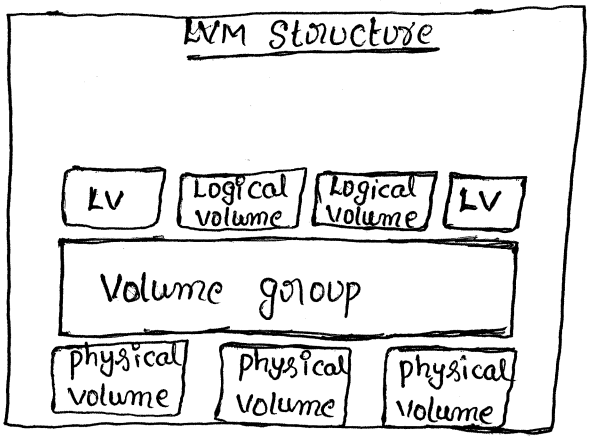
② Volume group.

③ Logical volume.

physical volume: The collection of individual physical drives are called as physical volumes.

Volume group: It is a collection of physical volumes and assign a name through which we can create logical volumes.

Logical volume: → The logical volumes are specified from the volume group. These are logical partitions which can resize, format, mount etc.



Implementation of LVM:

Step①: → Install the required packages:

```
#yum install -y lvm*↵
```

Step②: Verify that it is installed

```
#rpm -qa | grep lvm
```

Step③: creating an Lvm partitions: (four partitions)

```
#fdisk /dev/sda↵
```

→ To update to kernel for rereading

```
#partprobe /dev/sda↵
```

creating an LVM partition:

Step④: To create physical volumes:

```
#pvcreate /dev/sda{10,11,12,13}
```

→ verify that the physical volume was created successfully:

```
#pvdisplay /dev/sda10↵
```

Step⑤: → To create volume group:

```
#vgcreate India /dev/sda{10,11,12}
```

→ verify that the volume group was created successfully:

```
#vgdisplay -v India↵
```

→ When volume groups are created and initialized, the physical volumes are broken down into physical Extends (the unit of measurement for LVM). This is significant because you can adjust the size of how data is stored based on the size of each physical extend, defined when the volume group is created (the default is 4MB).

Step ⑥ : Create logical volumes :

→ To create a logical volumes, use the lvcreate cmd and specify the size of the partition that you'd like to create. The size can be specified in kilobytes, megabytes, gigabytes, or logical extents (LE). Like physical extents, logical extents are a unit of measure when dealing with logical volumes.

→ create a partition 2GB in size

#lvcreate -L 2000 &ndia -n (new) ap

→ To verify logical volume info,,

#lvdisplay ↵ (or) #lvs

→ To create one more logical volume

#lvcreate -L 3000 -n &ndia mp↵

→ using the Lvrename cmd you can change the name of a logical partition

#lvrename /dev/india/mp /dev/india/up↵

→ verify with the following cmd

#lvdisplay↵&ndia

Adjusting the size of Lvm partitions :

→ The single best feature of Lvm is that you can reduce or Expand your logical volumes and volume groups. If you are running out of room on a particular logical volume (or) volume group, you can add another physical volume to the volume group and then expand a logical volume to give you more room.

Step ⑦ : Add 2GB more to the ap logical volume

#lvextend -L +2000 /dev/india/ap↵

#lvExtend -L (or) 2000 /dev/india/ap↵

→ verify the change with the following cmd:

#lvdisplay /india↵

Step②: → To decrease a logical volume

#lvresize -L 2000 /dev/india/ap↵

(or)

#lvreduce -L-2000 /dev/india/ap↵

Step③: → Suppose, through, that you want to add a new physical volume so that you can extend your volume group.

→ Create a new physical volume somewhere

#pvcreate /dev/sda15↵

→ Now Extend your volume group to incorporate that new physical volu

#vgextend /india /dev/sda15↵

→ Now verify the details of the newly increased vg:

#vgdisplay -v /india↵

Step④: To reduce the volume group to no longer include the physical volume /dev/sda15, you can use the vgreduce cmd:

#vgreduce /india /dev/sda15↵

→ Now verify expansion or reduction of volume groups

#vgdisplay /india↵

Migrating Data: Suppose you have a drive that is old or dying and you'd like to remove it from the system. on a system with normal partitions, you would have to copy all the data from one disk to another while the disk is offline (because of files locks). Having LVM makes this easier because you can migrate your data from one disk to another, even while the disk is online! This capability is very useful when you need to replace a disk.

→ If you want to replace /dev/sda14 (/dev/sda) because it's failing, you can use the pvmove cmd to migrate the physical extents (which is really your data) to an other physical volume (/dev/sda15). (/dev/sdb)

Step①: → To create physical volume

#pvcreate /dev/sda15↵

Step②: → you need to add back /dev/sda15 to the vg:

~~less~~ vgextend Cndia /dev/sda15↵

Step③: → Also create a logical volume to hold the migrate data:

#lvcreate -L 3000 Cndia -n ban↵

Step④: → verify all logical volumes are in place

#lvdisplay Cndia↵

Step⑤: → Migrate the data from the "dying" drive

#pvmove /dev/sda14 /dev/sda15↵
(/dev/sda) (/dev/sdb)

Note: Make sure that you have more than one physical volume; otherwise there will be nowhere for the data to move.

Step⑥: verify that physical volume is Empty

#pvdisplay /dev/sda14↵
(/dev/sda)

Deleting an Lvm partition:

It just as important to understand how to delete Lvm partitions as it to create them. This is a common task when you are upgrading or redesigning a file system layout.

Step ①: → To remove a logical volume

```
#lvremove /dev/India/ap ↵
```

* → Although this advice should common sense, make sure you back up any data before deleting anything within the Lvm structure.

Step ②: → To remove the volume group:

```
#vgremove @ndia
```

→ you can also do both steps in one cmd by using the -f option

```
#vgremove -f @ndia ↵
```

Step ③: Wipe all the current physical volumes:

```
#pvremove /dev/sda10 ↵
#pvremove /dev/sda11 ↵
```

Note: use the resize2fs cmd to extend the file system. Before extending the file system, however, you should always ensure the integrity of the file system first with the e2fsck cmd.

Step ①: Syn: e2fsck [options] [Device]

-p	Automatically repairs (no questions)
-n	Makes no changes to the file system
-y	Assumes "yes" to all questions
-f	Force checking of the file system
-v	provides verbose output.

→ Check the file system

```
#e2fsck -f /dev/sndia/ap ↵
```

Step②:

Syn: resize2fs [options] [Device]

-p points percentage as task completes

-f force the cmd to proceed.

→ Extend the underlying logical volume:

```
#lvextend -L 3000 /dev/sndia/ap ↵
```

→ Now you can extend the file system

```
#resize2fs -p /dev/sndia/ap ↵
```

Step③:

→ Now that your maintenance is complete, remount the file system:

```
#mount /dev/sndia/ap /mnt ↵
```

→ you can use the mount cmd to verify it mounted successfully:

```
#mount ↵
```

→ Now you can use the df cmd to view the usage information for your file systems. this should also reflect the additional space that you just added to the /mnt file system.

Syn: df [options]

-h specifies human-readable format

-T points the file system type

```
#df -h ↵
```

RAID: Now let's move on to the final type of advanced partitioning: RAID

→ RAID means Redundant Array of Independent Disk

→ RAID partitions allow for more advanced features such as redundancy and better performance.

→ Mainly we implement the Raid inorder to increase the storage capacity along with data security.

→ There are two types of RAID's.

① Hardware raid.

② Software raid.

→ While RAID can be implemented at the hardware level, the Red Hat exams are not hardware based and therefore focus on the Software implementation of RAID through the MD driver.

→ Before we describe how to implement RAID, let's look at the different types of RAID:

RAID 0: (Striping) Disks are grouped together to form one large drive. This offers better performance at the cost of availability. Should any single disk in the RAID fail, the entire set of disks becomes unusable.

- Minimum 2, Max 32 Hard disks
- Data is written alternatively
- No fault tolerance.
- Read & write speed is fast.

RAID 1: (Mirroring) Disks are copied from one to another, allowing for redundancy. Should one disk fail, the other disk takes over, having an exact copy of data from the original disk.

- Min 2, Max 32 hard disks.
- Data is written simultaneously.
- fault tolerance available

RAID 5 : (Striping with parity) Disks are similar to RAID 0 and are join together to form one large drive. The difference here is that 25% of the disk is used for a parity bit, which allows the disks to be recovered should a single disk fail.

- Min 3, Max 32 hard disks
- Data is written alternatively
- parity is written on all disks
- Read & write speed is fast.
- fault tolerance is available.

Implementation of RAID 5:

Step ①: Install the following package

```
#yum install -y mdadm↵
```

Step ②: verify the install

```
#rpm -qa | grep mdadm↵
```

→ To start, you first need to create partitions on the disk you want to use. you start with a RAID 5 setup, so you need to make partitions on at least three different disks.

Creating a RAID Array:

→ create three partitions `#fdisk /dev/sda↵`

→ To verify when you're done `#fdisk -l↵`

→ Now you can begin to set up the RAID 5 array with the three partitions

Step ①: **Syn:** mdadm [options]

-a	Add a disk into a current array
-C	Create a new RAID array
-D	prints the details of array
-f	fails a disk in the array
-l	Specifies level of RAID array to create
-n	Specifies the devices in the RAID array.

-S Stops an array

-A Activate an array

-v provides verbose output.

#mdadm -Cv /dev/md0 -n3 /dev/sda1 /dev/sdb1 /dev/sdc1 -l5↵

Step ②: Again to verify that the RAID array has been created successfully

#mdadm -D /dev/md0↵

Step ③: view the status of the newly created RAID array:

#cat /proc/mdstat↵

This output shows that you have an active RAID 5 array with three disks in it. The last few lines here show the state of each disk and partition in the RAID array. You can also see that the RAID is in "Recovery" mode, or creating itself.

Step ④: If you wait the estimated 2.9 minutes and then query again, you see the following

#cat /proc/mdstat↵

You now see that the RAID is good to go as it has finished building itself.

What to DO When a Disk fails:

Suppose that a disk in the array fails. In that case, you need to remove that disk from the array and replace it with a working one.

Step ①: →Manually fail a disk in the array,

#mdadm /dev/md0 -f /dev/sdc1↵

Step ②: verify that the disk in the array has failed

#mdadm -D /dev/md0↵

Step ③: To remove a disk from the array

#mdadm /dev/md0 -r /dev/sdc1↵

Step ④: Look at the last few lines of the RAID details again

#mdadm -D /dev/md0 ↵

→ If you want, you could combine the previous two commands

#mdadm -v /dev/md0 -f /dev/sdc1 -r /dev/sdc1 ↵

Step ⑤: When the disk is partitioned, you can add it back to the array

#mdadm /dev/md0 -a /dev/sdd1 ↵

→ verify that it has been added properly

#mdadm -D /dev/md0 ↵

Step ⑥: Query the kernel

#cat /proc/mdstat ↵

Step ⑦: Should something go seriously wrong and you need to take RAID array offline completely

#mdadm -vS /dev/md0

Deleting a RAID Array:

Step ①: To delete an array, first stop it

#mdadm -vS /dev/md0

Step ②: Then remove the RAID array device

#mdadm -r /dev/md0 ↵

—x—

System Initialization

Boot process: Boot process consists the set of processes from power on the pc to login prompt comes.

→ when a computer boots up, the BIOS is the first program that is run. After it is loaded, the BIOS begins to test the system through the power on Self Test (POST) and then starts loading peripheral devices. The BIOS then looks for the boot device and passes control to it. The boot device contains the Master boot record (MBR), which starts to boot the system via the bootloader. From here, the Grand Unified Bootloader (GRUB) looks to boot into the kernel that is labeled as the default. Finally, the kernel calls the init process, which boots up the rest of the system.

→ The GRUB has become the default bootloader for Red Hat, Ubuntu, and many other versions of Linux as well.

→ When GRUB loads, you are given a list of kernels and additional operating systems from which you can choose to boot.

→ By default, there is a configurable 5-second timeout value that choose the default kernel if you don't make a selection and the timeout threshold is reached. After GRUB loads the kernel, it passes control over to the kernel, which it run begins to initialize and configure the computer's hardware.

*→ During the boot process, everything is logged to the /var/log/dmesg file. you can also use the dmesg cmd to query information about the boot process after the system has booted.

→ When the system's drivers are in place, the kernel executes the /sbin/init program.

*→ In RHEL6, the boot process has been replaced by a new utility called upstart instead of the traditional SysV init style scripts. This utility decreases the time that it takes the system to boot and is already currently being used on other versions of Linux such as Ubuntu.

* → The init program is the first process created by the kernel. It is responsible for the rest of the boot process and setting up the environment for the user.

→ First, it consults the /etc/inittab file, which defines how the rest of the boot process will go. The /etc/inittab file lists the default runlevel to boot into and the system initialization script (/etc/rc.d/rc.sysinit).

→ Let's look at the /etc/inittab file to see what the init process goes through

#cat /etc/inittab ↵

→ You can see that the default runlevel is set to 5, although six different runlevels are listed. The /etc/inittab file also defines how to handle power failures and virtual terminals. After the init process is done consulting the /etc/inittab file, the /etc/rc.d/rc.sysinit script is run, which handles setting the system clock, networking, setting up the user environment & more.

→ On Red Hat Linux, the default run level is 5. This default runlevel is passed to the /etc/rc.d/rc script, which calls all the programs in the /etc/rc.d/rc#.d directory.

→ The last thing that you should see is the login prompt. If you have a desktop manager installed such as Gnome, you should see a GUI login screen where you can login to the system; otherwise, you see a text mode login.

⇒ **Working with Grub:** The GRUB bootloader is broken down into different stages. The code contained on the MBR is considered GRUB stage 1. It loads GRUB stage 1.5, which tries to identify the file system type (optional), or it can call GRUB stage 2 directly. stage 2 is what calls the kernel and loads it into memory. On stage 1, GRUB needs to search the MBR looking for an active partitions from which to boot the kernel. GRUB has its own format for looking through hard disks.

→ The Syntax of this format is

(xdn[,m]) where xd is the drive
n is the number of the disk
m denotes the partition number.

→ The Syntax is very useful when troubleshooting issues with GRUB because you need to know how GRUB searches for disk drives when trying to find the primary partition. When the primary partition found, GRUB loads the kernel, which is where you move on to stage2. Stage2 is the place where you will tend to spend the most time troubleshooting boot issues with the system. As stage2 is starts, it presents you ~~which~~ with a list of kernel's that you can boot from, along with a listing of options that you can use to modify the parameters passed to the kernel during bootup.

Grub Boot options:

e	Edit the cmds before booting
a	Modify (or) append the kernel arguments before booting
c	Open the GRUB cmd line.

→ you can use 'a' option to modify any parameters you want to pass to the kernel. This includes changing the runlevel that the system will boot into.

→ After choosing the 'a' option, you can pass a mode as a parameter to enter into the mode. Here are the different modes that you can boot into:

Single-User Mode	perform maintenance tasks (or) forget the root password.
Runlevel 2 (or) 3	Load only partial services during the boot process
Emergency Mode	Used to perform tasks on an unbootable system.
Rescue Mode	Used to fix boot issues (or) reinstall GRUB.

The config file:

→ GRUB has only a single config file, /boot/grub/grub.conf. Two other files actually have soft links to this main config file as well: /boot/grub/menu.lst and /etc/grub.conf. When GRUB starts, it reads its configuration from the main config file

```
#cat /boot/grub/grub.conf
```

→ Using the c option to enter the GRUB cmd line, you can make changes to the config file, reinstall GRUB, or repair a broken config file.

The GRUB Command Line:

→ How to repair a broken MBR.

You need to make use of the rescue environment, which can be found by booting from the RHEL installation DVD. When you are in the rescue environment, you can repair your broken MBR.

Step ①: Load up the GRUB cmd line to find the disk and partition that contain the grub.conf file using the find cmd:

```
grub> find /grub/grub.conf ↵
      (hd0,0)
```

→ you could also run:

```
grub> root ↵
      (hd0,0)
```

Step ②: Install GRUB on the drive is returned:

```
grub> setup (hd0)
```

→ Now that your MBR is fixed, you should be able to boot the system once again.

⇒ Runlevels:

→ When the system boots up, it queries for the default runlevel, which is defined in the /etc/inittab file. When the default runlevel is located, the system boots into that particular runlevel.

→ There are six runlevels in total, which are shown in the /etc/inittab file. Each runlevel also has a directory called /etc/rc.d/rc#.d, where # is the runlevel (from 0 to 6).

→ Let's look at the different runlevels:

0	Halt
1	Single user mode
2	Multiuser with partial services
3	Full multiuser with networking (text mode)
4	Not used
5	Full multiuser graphical mode (GUI desktop login)
6	Reboot

→ The easiest runlevels to understand are 0 and 6. These two runlevels are called by the same cmd with different input. On runlevel 0, essentially the system is off. On runlevel 6, the system is restarting. Runlevel 1 is used to enter single-user mode, which you would enter if there are issues with the system and you'd like to perform maintenance. You can also reset the root user's password in this runlevel. The remaining runlevels provide various states for different services to run in.

→ Don't forget the the upstart is the program that actually starts & stops services at each runlevel now. The /etc/init/rc.conf file shows how each set of scripts is called:

```
#cat /etc/init/rc.conf↵
```

Runlevel Utilities:

→ let's now look at the many system utilities that help you manage the system in different runlevels. These management cmds are

Syn: shutdown [options] time

- -k Doesn't shutdown; just warns
- -h Halts the system after shutdown
- -r Reboots instead of turning off the system.
- -F forces a file system check on reboot.
- -n Kills all processes quickly (not recommended)
- -t SECs Sends a shutdown message but delays shutdown by x seconds.

Ex: #shutdown -h now ↵

#shutdown -r now ↵

#reboot ↵

#shutdown -h 120 ↵ delay the shutdown by 2 Minutes.

Halt: powers down the system.

→ To turn of the system #shutdown now (or) #halt ↵

poweroff: works the same as the halt cmd.

→ To check the current runlevel #runlevel ↵

(or)

#who -r ↵

→ To change runlevel 3 #init 3 ↵

Troubleshooting

I lost My Root user password:

Step ①: Boot into single-user mode by appending the command line during boot with the following

single

Step ②: When you are presented with a command prompt, change the root user password:

passwd root ↵

Step ③: Reboot the system and validate that the new root password works correctly:

#reboot ↵

password change Not Available in Single-user Mode:

When you enter single-user mode, you may encounter an issue where the root user's password can't be changed.

Step ①: verify the existence of the /etc/shadow file:

#ls /etc/ | grep shadow ↵

Step ②: If the /etc/shadow file doesn't exist, use the pwconv cmd to re-create the /etc/shadow file:

#pwconv ↵

Step ③: Now execute the passwd command to reset or change the root user's password:

#passwd root ↵

Step ⑭: Reboot the system and validate that the new root password works correctly:

#reboot ↵

The MBR is corrupt:

If you are having trouble booting the system and you have determined that the master boot record (MBR) is corrupt, you need to boot into rescue mode. Use the Red Hat DVD, boot from it, and choose the option to enter rescue mode.

Step ①: After you boot, enter the GRUB shell:

#grub ↵

Step ②: Locate the root drive:

grub> root ↵

Step ③: Reinstall the MBR from the GRUB shell:

grub> setup (hd0)

Step ⑭: Reboot the system to validate that the system boots properly:

#reboot ↵

Repair the file System :

When we have a inconsistency to the file /etc/fstab and the file systems listed by blkid utility.

Then the system will go to rescue mode

→ To troubleshoot this problem provide the root password for the maintainence

→ When we provide the root password correctly then a shell prompt will be opened

→ At this movement the file system is mounted in read only mode, hence we can't change the file system table (fstab file)

→ So mount the file system in rw mode

```
#mount -o remount,rw / ↵
```

→ Now open the file /etc/fstab

```
#vim /etc/fstab ↵
```

Now remove (or) change the file systems which leads to inconsistency and save the fstab file and reboot the pc

```
#init 6 ↵
```

(or)

```
#reboot ↵
```

Assign the grub password:

The grub password is to be maintained in the file "/boot/grub/grub.conf".

```
#grub-md5-crypt >> /boot/grub/grub.conf
```

when we type the above command then a encrypted password comes to the last line of the file /boot/grub/grub.conf

we have to copy that encrypted password and paste in the same file under the line "hidden menu"

```
password --md5 <encryptedpassword>
```

here we have to paste the encryptedpassword

Recover root & grub password:

Step①: use the Red Hat DVD, boot from it, and choose the option to enter Rescue mode.

```
boot: Linux rescue ↵
```

Select keyboard => select language => select networking

Then a shell will be opened.

at this moment to give the previlage to the root user to maintain the file system

```
#chroot /mnt/sysimage ↵
```

Here we can follow the above mentioned procedures of recovering root password and grub password.

The Superblock Has Become corrupt:

If the superblock on your system has become corrupt, you can re-create it with one of the backup superblocks. If the primary file system has the corruption, you may need to use single-user mode or the rescue environment to perform the recovery.

Step ①: check the state of the file system:

```
#dumpe2fs  h  /dev/sda1 ↵
```

Step ②: find a valid backup superblock:

```
#dumpe2fs  /dev/sda1 | grep -i  superblock ↵
```

Step ③: Repair the file system with a backup superblock:

```
#e2fsck  -f  -b  8193  /dev/sda1 ↵
```

Backup & Restore

→ In information technology, a backup or the process of backing up is making copies of data which may be used to restore the original after a data loss event.

→ Backup have two distinct purposes.

→ The primary purpose is to recover data after its loss, be it by data deletion or corruption. Data loss is a very common experience of computer users. 67% of internet users have suffered serious data loss.

→ The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required.

→ Backup is the most important job of a System administrator, as a System admin it is your duty to take backup of the data everyday.

→ Many companies have gone out of the market because of poor backup planning.

→ The easiest way to backup your first is just copying. But if you have too many files to backup, copying and restoring may take too long time and it is not convenient. If there is a tool that can put many files into one file, the world will be better. Fortunately, 'tar' is used to create archive files.

Compression and Archiving:

→ As you will learn when you become a System Administrator, backups are the number one priority.

→ If something should crash or become corrupt and you can't restore it because you aren't keeping up with your backups or you just don't keep any, you may be looking for a new job. Although we don't address backup programs here, this is good lead into archiving and compression.

tar: Tar means tape archiving

→ It is used for compressing and archiving files and directories.

→ A more common use for tar is to simply combine a few files into a single file, for easy storage distribution.

Syn: tar [options] [FILE]

options:

- -c Creates a new archive
- -v provides verbose output
- -f Specifies the archive file to use
- -t Lists the files in an archive
- -x Extract the backup
- -z Zipping

Step ①: create some random blank files:

#touch file1 file2 file3 another_file↵

Step ②: create a simple archive containing these files:

#tar -cvf sample.tar file1 file2 file3 another_file↵

when an archive is created, you can also apply compression to reduce the amount of space the archive files takes up. Although multiple types of compression are supported with the use of tar, we look only at gunzip (.gz) and bzip2 (bz2) here.

Step ③: Let's re-create the archive using the gunzip compression:

tar -cvzf sample.tar.gz file1 file2 file3 another_file↵

Step ④: view the current directory to see the two current archive files:

#ls ↵

Step ⑤: To see all the contents within the build file:

#tar -tvf sample.tar↵

Step ⑥: Now extract this build file verbosely:

#tar -xvf sample.tar↵

Step ⑦: To extract files on different location

#tar -xvf sample.tar -C /root/Desktop↵

cpio : cpio is a tool for creating and extracting archives or copying files from one place to another.

→ It handles a number of cpio formats as well as reading and writing tar files.

→ cpio like tar but can read input from the "find" command.

→ The basic structure is

: find -name file | cpio [options] [controller] <Dest>

options: -o (out)
-i (In)

controllers:
O (or) > -out
I (or) < -In

Step ①: To take the backup files

#ls file* | cpio -ocvf > /root/backup.cpio ↵

Step ②: To see the backup content:

#cpio -it < /root/backup.cpio ↵

#cpio -it -I /root/backup.cpio ↵

Step ③: To restore the backup file:

#cpio -icuvd < /root/backup.cpio ↵

o → Reads the standard ~~output~~ input
i → Extract files from the standard input
c → Read or write header information in ASCII character
d → Creates directories as needed
u → copy unconditionally (older file will not replace a new file)

DD : (Disk to Disk)

Used to take the backup of one partition to another, here source partition should be given to "if", destination partition should be passed to "of".

Step ① : To take the backup :

#dd if=/dev/hda6 of=/dev/hda7 ↵

Step ② : To recovery :

#dd if=/dev/hda7 of=/dev/hda6 ↵

Scp : (Secure copy)

→ Scp is used to copy data from one unix or Linux System to another unix or Linux Server.

→ Scp uses secured shell (ssh) to transfer the data between the remote hosts.

→ The features of scp are:

- copies files with in the same machine.
- copies files from local machine to remote machine
- copies files from remote machine to local machine
- copies files between two different remote servers.

Syn: scp [options] [user from_HOST : source_file] [user to_HOST :Destination_file]

Options:
- -r Recursively
- -q progress bar not displayed
- -v verbose mode
- -P copy files using the specified port number.

→ copy file from local host to remote server:

scp filename root@server254.Example.com:/root↵

→ copy files from remote host to local server:

scp root@server254.Example.com:/root/backup* .↵

(. ↓ current directory)

→ copying a directory:

scp -r directory root@server254.Example.com:/root↵

→ Improving performance of scp command:

Using blowfish or arcfour encryption will improve the performance of the scp command

scp -c blowfish filename root@server254.Example.com:.↵

→ Specifying the port number:

scp -P 6001 backup_file root@server254.Example.com:/tmp↵

—x—

Remote Access

→ you walk into the server room and install Red Hat on your new server. After the installation is comple, you need to configure numerous packages and then begin setting up users.

→ All these tasks take time, and if you work in data center, chances are office is located somewhere else. Remote access to any system that you work on makes managing and troubleshooting much easier because you don't physically need to be in the same location as your systems.

→ We discuess using telnet, ssh for command line remote access and vnc for graphical remote access.

* Telnet:

→ Telnet is a network protocol which is used to connect to remote computers over TCP/IP network. you can make a connection to a remote host using telnet. once you establish a connection to the remote computer, it becomes a virtual terminal and will allow you to communicate with the remote host foram your computer.

→ Xinetd is a program used to start and stop a variety of Linux data communication applications. Some of these applications, such as Telnet, are installed by default in RedHat Linux.

⇒ Configuring the Telnet:

Step ①: Install telnet server package:

```
#yum install telnet* -y↵
```

Step ②: verify that the package installed correctly:

```
#rpm -qa|grep telnet↵
```

Step ③: make sure that the service is set to start when system boots:

```
#chkconfig xinetd on↵
```

Step ④: verify your changes:

```
#chkconfig xinetd --list↵
```

Step ⑤: open the telnet configuration file:

```
#vim /etc/xinetd.d/telnet↵

disable = no        [By default "yes"]

:wq!↵
```

Step ⑥: Now restart the telnet service:

```
#service xinetd restart↵
```

Step ⑦: Now go to your client system and try to access your server (remote host)

```
$telnet 192.168.1.254↵

login:
password:
```

* **Note:** One of the disadvantages of Telnet is that the data is sent as clear text. This means that it is possible for someone to use a network analyzer to peek into your data packets and see your username & password.

→ A more secure method for remote logins would be via Secure Shell (SSH) which uses varying degrees of encryption.

* Secure Shell (SSH):

→ Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client.

→ SSH is a fairly easy service to setup and is useful in many different ways. Although it is usually installed by default, if the SSH server package is not installed, do the following:

Step ①: Install the required package:

```
#yum install openssh* -y↵
```

Step ②: verify that the package installed:

```
#rpm -qa | grep openssh↵
```

Step③: Ensure that the service is currently running:

#service sshd status↵

Step④: Enables the service during boot:

#chkconfig sshd on↵

Step⑤: Verify that the service is enabled during boot:

#chkconfig sshd --list↵

→ Let's discuss some of the options laid out here:

port : Defines the port used for SSH

protocol : Specifies the protocol being used (1 or 2)

ListenAddress : Defines the IP address to Listen on

permitRootLogin : Determines whether the root user can log in

X11forwarding : Allows the forwarding of GUI programs.

→ All these options should be self-explantory, but there are two options that I recommend changing before you use the SSH service:

#vim /etc/ssh/sshd_config↵

permitRootLogin = No

X11forwarding = No

:wq!↵

Step⑥: you need to restart the service for the changes to take effect:

```
# service sshd restart↵
```

→ Now that the SSH server is setup, you should test it from one of the client systems.

Step①: login server250 and verify that the ssh packages are installed:

```
#rpm -qa | grep ssh↵
```

Step②: connect to server250using the ssh command:

```
#ssh user01@192.168.1.254↵
```

*Note: the first time you connect to a host, you are required to accept that you trust the host. After you accept the connection, the host is stored permanently in the ~/.ssh/known_hosts file.

* **VNC Servers**: → Virtual Network Computing Server software.

→ the VNC server allows you to remote into the user's system and view her desktop. with the end user's desktop in view, you can more easily troubleshoot any issues she is having.

→ Setting up a VNC server isn't hard, and in fact, it sometimes comes pre-installed as part of a desktop package:

Step①: Install the package:

```
#yum install tigervnc* -y↵
```

Step②: Query to make sure that package is installed correctly:

#rpm -qa | grep tiger ↵

Step③: ~~Enable vnc to make at boot time~~: open config file:

#vim /etc/sysconfig/vncservers ↵

VNCSERVERS="2:helpdesk"

VNCSERVERARGS[2]="-geometry 1024x768 -nolisten tcp -nohttpd"

:wq! ↵

~~/etc/pam.d~~

→ The first line defines the user who is allowed to log in to the system.

→ The second line lists the arguments passed to the VNC server when the service starts.

-geometry	: Defines the size of the viewer when the client connects.
-nolisten tcp	: Denies ~~Defines~~ TCP connections to the VNC server.
-nohttpd	: Denies web VNC clients from connecting.
-localhost	: forces the use of a secure gateway (port forwarding)

→ The number that appears (2 in this case) is the number of the session for the defined user.

→ The VNC server runs on port 5900, but the actual port that will be used is 5900 + the number defined = 5902 in this case.

Step ④: Set the password for the helpdesk user to be able to connect with him:

```
#useradd helpdesk ↵
#vncpasswd ↵
```

Step ⑤: Start the VNC server to be able to connect to it:

```
#vncserver :1 ↵
```

→ This creates the files required for the VNC server because it has now been started for the first time.

---

* Note: on RHEL5, the VNC has a configuration issue: It will not start the desktop manager without an edit to the ~/.vnc/xstartup file.

Step ①: Edit the ~/.vnc/xstartup file to uncomment the first two lines:

```
#vim ~/.vnc/xstartup ↵

unset SESSION_MANAGER
exec /etc/X11/xinit/xinitrc
```

Step ②: Kill the current VNC session:

```
#vncserver -kill :1 ↵
```

Step ③: Start a new session:

```
#vncserver :1 ↵
```

⇒ Connecting clients:

Step ①: Install the VNC package that contains the client software to connect:

```
#yum install tigervnc* -y ↵
```

Step ②: verify that the package was installed successfully:

```
#rpm -qa | grep tiger ↵
```

Step ③: At this point you can use the vncviewer command to connect to the VNC server:

```
#vncviewer 192.168.1.254:5902 ↵
```

→ The system now prompts you for the password that you setup for the "help desk" user on client01. After you enter the password, a display of the remote desktop appears as if you were sitting at the system.

→ VNC can useful when you're tryying to help end users troubleshoot or show them how to do something.

→ Many times in the real world, however, the desktop managers are not used (only the shell is), so there isn't really a need for VNC on servers.

—×—

DHCP

(Dynamic Host configuration protocol)

→ one of the basic Elements found on all networks is a Dynamic Host configuration protocol (DHCP) server, making it an important part of any network.

→ DHCP makes network administration easy because you can make changes to a single point on your network and let those changes filter down to the rest of the network.

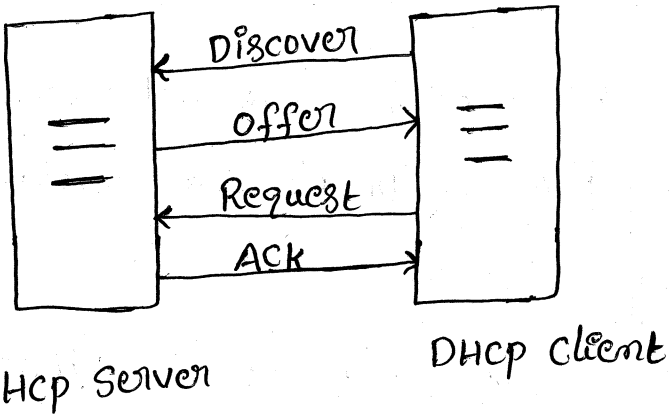
Boot p Server: In this method the administrator used to collect the MAC address of the system and assign corresponding IP address to them. The list of MAC address and IP address was maintained in a server called as a Boot p server. Whenever the client request for IP address Boot p server assign the IP. In this method the administrator used to collect the MAC address.

DHCP: It gives IP-address automatically to the clients who is requesting for an ipaddress.

→ It provides centralized Ip-address management.

→ DHCP reduces the complexity and amount of administrative work by assigning TCP/IP configuration.

→ DHCP follows the "DORA" process.



⇒ Configuration:

Step①: Start by installing the dhcp package:

```
#yum install dhcp -y↵
```

Step②: Verify that the package is installed correctly:

```
#rpm -qa | grep dhcp ↵
```

Step③: make sure that the dhcpd service starts when the system boots as well:

```
#chkconfig dhcpd on↵
```

Step④: Verify that the DHCP service starts on boot:

```
#chkconfig dhcpd --list↵
```

→ To start the configuration, Let's look at the important files that handle the options for the DHCP service:

/etc/dhcp/dhcpd.conf : Main config file for the DHCP service.

/var/lib/dhcpd/dhcpd.leases : IPv4 client lease file.

Step ⑤: To copy the sample file, use the following command:

#cp /usr/share/doc/dhcp-4.1.1/dhcpd.conf.sample /etc/dhcpd/dhcpd.conf

vim /etc/dhcpd/dhcpd.conf ↵

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    #parameters for the local subnet
        option routers                  192.168.1.1;
        option subnet-mask              255.255.255.0;

        option domain-name              "example.com";
        option domain-name-servers      192.168.1.254;

        default-lease-time              21600;
        max-lease-time                  43200;
    #client ip range
        range dynamic-bootp 192.168.1.100 192.168.1.200;
}
```

:wq! ↵

Step ⑥: Check the config file for any errors:

#service dhcpd configtest ↵

⇒ **DHCP Reservation:** Assigning ip address dynamically has some problem that every time a client system boots it is not sure that it will get the same ip, so it will be tedious task for other systems to find the particular system. To solve the above problem we can do MAC address binding of the ip address for this provide its Entity in the fixed address portion.

→ open the main config file:

```
#vim /etc/dhcpd/dhcpd.conf ↵

host server1254 {
    option host-name "server1254.Example.com";
    hardware ethernet 02:B4:7C:43:DD:FF;
    fixed_address 192.168.1.50;
}
```

Step ⑦: Restart the DHCP service

```
#service dhcpd restart ↵
```

⇒ **connecting client:**

→ To test the ip-address: `#dhclient ↵`

—x—

System Security

* Security Through TCP Wrappers:

TCP wrappers is a host service that can be used to limit or control access from remote hosts. Although it is installed by default, verifying things manually is always good.

→ First, check for the TCP wrappers package to make sure it is installed:

```
#rpm -qa | grep wrappers ↵
```

You can limit access to either users or hosts via the /etc/hosts.allow and /etc/hosts.deny files (you can mix and match both users and hosts in either file). The TCP wrappers service scans the two files in the following fashion:

- Search the hosts.allow file.
- Search the hosts.deny file.
- If not found in either, allow.

→ The TCP wrappers service itself uses the following syntax in the two already mentioned files:

```
<daemon_list> : <client_list>
```

Aside from being able to define a hostname or ip address in the client_list field, you can also define any of the following keywords:

ALL	Specifies all networks.
LOCAL	Specifies the local network.
EXCEPT	Excludes a particular user/client.
KNOWN	Indicates all hosts that can be resolved by the system.
UNKNOWN	Indicates all hosts that can't be resolved by the system.

→ These keywords can be used to help keep your rule count under control. Instead of defining each host within your network, you can just use the keyword LOCAL instead.

→ Let's look at a few examples to help drive home the point.

→ Suppose that you want to restrict access to the SSH service and allow connections only from the local network.

```
# vim /etc/hosts.allow ↵

sshd : 192.168.1.

(or)

sshd : 192.168.1.0/24

(or)

sshd : 192.168.1.0/255.255.255.0
```

→ If you want to allow only a single IP address to be able to access the server

```
#vim /etc/hosts.allow ↵

sshd : 192.168.1.250
```

→ Going further with this example, what if you want to allow all users from the 192.168.1.0/24 network except the 192.168.1.100 host? Then you could use the following rule

```
#vim /etc/hosts.allow ↵
sshd : 192.168.1. EXCEPT 192.168.1.100
```

→ While locking down the number of hosts that can access a particular server, you don't want to go crazy either; otherwise, you'll end up with a management nightmare! A common solution in the real world is to use the domain name in which servers and clients are members to provide you with basic management.

→ you can restrict it to hosts from particular domains with the following:

```
#vim /etc/hosts.allow↵
sshd : .example.com
```

⇒ Examples of Denying:

→ To deny the system 192.168.1.250 through ssh:

```
#vim /etc/hosts.deny ↵
sshd : 192.168.1.250
```

→ To restrict all the systems 192.168.1.0/24 Except 192.168.1.100

```
#vim /etc/hosts.deny
sshd : 192.168.1. EXCEPT 192.168.1.100
```

```
:wq! ↵
```

→ To restrict all the hosts in example.com

#vim /etc/hosts.deny ↵

sshd : .example.com

→ To restrict ssh service to every one.

#vim /etc/hosts.deny ↵

sshd : ALL

→ To restrict all TCP wrappered services to every one:

#vim /etc/hosts.deny ↵

ALL: ALL

:wq! ↵

→ When troubleshooting TCP wrappers, you can use the "/var/log/secure" file to view any information that is recorded. this helps you determine if something is wrong or being blocked for a specific reason. you should not use TCP wrappers as your only line of security because there are ways to fool it; however, it is a great layer of security. combined with a firewall and SELinux, TCP wrappers is a nice addition to hardening your servers.

— x —

NFS

(Network File Systems)

→ There are many different ways you can share files with users on your network.

→ NFS provides a way for other systems on the network to store files in a centralized place. This ensures that backups are easier and security remains intact on a single point. Keeping your data in a centralized place will make your life much easier as a system administrator.

→ The Network File Systems (NFS) protocol works great when it comes to Linux systems because it allows for client flexibility, centralized management of files, and some other great features.

→ To get NFS working properly, you need to set up the NFS server first and then setup the client to test access to the server. As with any other service, you need to install a few packages before doing anything else.

→ There are four different versions of NFS; version 4 is the most current. Although you can disable what versions the server listens for, the client actually determines which version it will use when connecting to the server.

→ When RHEL5 was introduced, it came with both NFS versions 3 & 4 available for use, but version 3 was used by default. On RHEL6, again both versions are available, but version 4 is now the default.

⇒ **Features:**

(i) Every one can access same data this eliminates the need to have a redundant data on server systems.

(ii) Reduces storage cost.

(iii) provides data consistency.

(iv) Reduces the system administrators overhead.

(v) Data transfer rate in 4.0 is
3.0 is 32kb bit
2.0 is 8 kb bit.

⇒ **Limitations of NFS:**

(i) We can only exports the directories which are started with "/".

(ii) We can only exports the files only to the homogeneous Environment.

(iii) only local file systems can be exported.

(iv) It uses only in private network.

⇒ **Configuring NFS:**

→ The NFS & rpc bind services both control a number of daemons on the system when they are started. There are

- rpcbind : Forwards incoming requests to the appropriate subservice.
- rpc.idmapd : Maps the UID & GID to users and groups.
- rpc.lockd : Manages file locks and releases in case of client disconnect
- rpc.nfsd : Responds to client requests for file access.
- rpc.rquotad : provides statistics on disk quotas to clients
- rpc.statd : Works with rpc.lockd to provide recovery services.

→ Let's look at the config files that you will be dealing with:

/etc/sysconfig/nfs : Main config files for the NFS service.

/etc/exports : List of resources that will be exported to clients.

→ Here are some additional files that will use when working with NFS:

/var/lib/nfs/etab : A List of currently exported resources.

/var/lib/nfs/rmtab : A List of remotely mounted resources.

Step①: Installing an NFS server

```
#yum install nfs* -y ↵
```

→ verify the package installation:

```
#rpm -qa | grep nfs ↵
```

Step②: The NFS server uses three different services to function properly. you need to enable them all at boot for the NFS server to function the way it should:

```
#chkconfig nfs on ↵
#chkconfig nfslock on ↵
#chkconfig rpcbind on ↵
```

Step ③: Verify that all three services are set to start on System boot:

```
#chkconfig --List nfs ↵
#chkconfig --List nfslock ↵
#chkconfig --List rpcbind ↵
```

Step ④: Verify that the service is off:

```
# service nfs status ↵
```

Step ⑤: Next, let's work with the /etc/exports file. The syntax of the /etc/exports file is

```
<mountpoint>    <host><permissions/options>
```

Mount options:

- rw : Sets read/write permissions.
- ro : Sets read-only permissions.
- insecure : Allows the use of ports over 1024.
- sync : Specifies that all changes must be written to disk before a command completes.
- root_squash : prevents root users.

→ As an example, you can use the following two locations to export to the clients:

```
#vim /etc/exports ↵
/home    192.168.1.0/255.255.255.0(rw, sync)
/opt/data    *(rw, sync)
:wq! ↵
```

Step ⑥: Start the two NFS services

```
# service nfslock start ↵
# service nfs start ↵
```

Step ⑦: Verify that the services have started successfully:

```
# service rpcbind status ↵
# service nfslock status ↵
# service nfs status ↵
```

* Note: If you already started the services before creating an /etc/exports file, you can also use the exportfs command to manually export any new resources added to the /etc/exports file.

Syn: exportfs [options]

-a	Exports/unexports all directories
-r	Reexports all directories
-u	Unexports one or more directories
-v	provides verbose output.

```
#exportfs -avr ↵
```

→ Alternatively, you can also get the same effect by restarting only the NFS service, which ~~is~~ in turn restarts all daemons:

```
# service nfs restart ↵
```

* Tip: It is better to manually export the directories than to restart the service because you don't disconnect your clients when exporting new directories, but you do disconnect them when the service is started.

→ you can use the rpcinfo command to verify that all the parts of the NFS service are running properly.

#rpcinfo -p ↵

you can view both local and remote connection information.

⇒ Troubleshooting NFS:

There are three management commands that help with troubleshooting NFS from both the server & client sides:

mountstats : Shows information about mounted NFS shares

nfsstat : Shows statistics of exported resources

nfsiostat : Shows statistics of NFS mounted shares.

Step①:

→ First, Let's look at which resources are exported. for this, you can check the /var/lib/nfs/etab file.

#cat /var/lib/nfs/etab ↵

Step②: from the client side, you can use the nfsstat command, for similar results.

Syn: nfsstat [options]

-m Shows statistics on mounted NFS.

-n Shows NFS statistics.

⇒ Connecting clients:

Setting up a client to use NFS is relatively simple when you have the NFS server in place.

Step①: To start, you need to install the required packages:

```
#yum install nfs* -y ↵
```

Step②: To ensure that the required service is set to start on boot:

```
#chkconfig rpcbind on ↵
```

Step③: Create two local directories:

```
#mkdir /mnt/{data,temp} ↵
```

Step④: To check the nfs server sharing information:

```
#showmount -e <NFS server_ip>
#showmount -e 192.168.1.254 ↵
```

Step⑤: Mount the data NFS share:

```
#mount -t nfs 192.168.1.254:/opt/data /mnt/data ↵
#cd /mnt/data ↵
#ls ↵
```

→ Assuming your permissions and security restrictions are correctly in place, you should now be able to move into the /mnt/data directory and actually access the NFS share on the server.

→ If you don't want to always mount NFS shares after your system has booted, you can, of course, add an entry to the /etc/fstab file to have them mounted automatically at system boot:

```
#vim /etc/fstab ↵
192.168.1.254:/opt/data  /mnt/data  nfs  rw,sync  0 0
:wq! ↵
```

→ Using the mount command, you can verify that the resource was mounted properly:

```
#mount | grep nfs ↵
```

—— x ——

SAMBA

→ As a Linux administrator, when you think Windows, you should also think Samba.

→ Samba is a great technology that you can run on Linux allowing you to communicate and interact with windows servers and clients.

→ A Samba server can host windows shares, act as a print server, and in some more advanced cases act as a backup domain controller for windows domains.

→ Samba is a free software re-implementation of SMB/CIFS networking protocol, originally developed by Australian Andrew Tridgell.

→ Samba, which uses the CIFS/SMB protocol, is commonly brought up when you want Linux and Windows machines to be able to share files together. Aside from the file sharing uses, Samba also has some built-in functionality to run as a member server on a windows domain, print server, or file server.

⇒ **Features of SAMBA:**

(i) File / Directory sharing.

(ii) Browsing.

(iii) Resource Sharing.

(iv) User Authentication & Authorization.

→ If you have never worked with Samba before, the number of options can seem over-whelming.

→ First, let's look at the two services responsible for running samba:

smbd : Samba Server daemon

nmbd : NetBIOS service daemon

→ There are also a handful of config files:

/etc/samba/smb.conf : Contains main config file

/etc/samba/smbusers : Maps Samba & RedHat users.

/etc/samba/smbpasswd : Contains samba user passwords.

⇒ **Configuring Samba:**

Step ①: Install the required packages for Samba:

```
#yum install samba* -y ↵
```

Step ②: Verify the package installation:

```
#rpm -qa | grep samba ↵
```

Step ③: Enable the service to start during boot:

```
#chkconfig smb on ↵
```

Step ④: Verify that the service is set to start on boot:

```
#chkconfig smb --list ↵
```

Step ⑤: Create a directory for sharing:

```
#mkdir /opt/company_data↵
#cd /opt/company_data↵
#touch a ab abc↵
#ls↵
```

Step ⑥: you need to edit the main config file to set up the samba server and directories that you'd like to make into samba shares.

```
#vim /etc/samba/smb.conf↵
```

Define our workgroup & hostname info.,###

```
workgroup      = INDIA          #line no 74;
netbios name   = Server254
```

→ Next go to last line of the file:

```
[company_data]

comment        = Directory for all employees
path           = /opt/company_data
valid users    = user01
public         = no
writable       = yes
browseable     = yes
hosts allow    = 192.168.1.
```

```
:wq!↵
```

Step ⑦: Now you need to check that the config file has no syntax errors by using the testparm command:

```
#testparm ↵
```

Step ⑧: Before you can start connecting clients, however, you also need to create Samba users because they are separate from system users.

Syn: Smbpasswd [options] [user]

options:

-a	Add a user
-d	Disable a user
-e	Enables a user
-x	Deletes a user

```
#useradd user01 ↵
#Smbpasswd -a user01 ↵
```

→ verify that the user was created successfully

```
#pdbedit -w -L ↵
```

* Tip: Whenever you make changes to the Samba users, you need to restart the service before you are able to use them.

```
#Service Smb restart ↵
```

Step ⑨: verify that the service is running:

```
#service Smb status ↵
```

⇒ Samba Clients:

Now that all your Samba shares are set up, you can access them from one of the client systems. Be aware that you need to install the client samba packages before you can connect to any samba shares.

Step ①: Install the client packages:

```
#yum install samba* -y ↵
```

Step ②: Verify that the install was successful:

```
#rpm -qa | grep samba ↵
```

Step ③: Create a local directory where you will mount your samba share:

```
#mkdir /mnt/company_data ↵
```

→ Using the Smbclient command, you can now mount the samba share.

Syn: Smbclient [options]

options:

-L	Lists samba shares
-U	Defines the user to connect with
-P	Defines the password to connect with
-N	Defines anonymous login.

Step ④: List the Samba Shares on the Server254 Samba Server:

```
#Smbclient -L 192.168.1.254 -N ↵
```

Step ⑤: Mount the remote Samba Share:

```
#mount.cifs //192.168.1.254/company_data /mnt/company_data
        -o username=user01,password=<password> ↵

#cd /mnt/company_data ↵
#ls ↵ verify
```

Step ⑥: you can verify that the mount worked successfully by using the Smbstatus command.

Syn: Smbstatus [options]

options: -p shows processes only
-S shows shares only
-L shows Locks only
-V provides verbose output.

```
#Smbstatus ↵
```

Step ⑦: Create an entry in the /etc/fstab file:

```
#vim /etc/fstab ↵
//192.168.1.254/company_data /mnt/company_data cifs
        user=user01,pass=<password> 0 0

:wq! ↵
```

Step ⑧: Add the credentials that you'd like to use to a file:

#echo "username=user01" > /etc/samba/smbcred ↵

#echo "password=password" >> /etc/samba/smbcred ↵

→ update the entry in the /etc/fstab file to reflect the changes to how the credentials are read:

//192.168.1.254/company_data /mnt/company_data cifs

credentials=/etc/samba/smbcred 0 0

:wq!

→ you can use the umount.cifs command to unmount the samba share and reboot the system to make sure that the share mounts correctly when the system reboots.

⇒ FTP Method:

→ Access the share through FTP service:

#smbclient //192.168.1.254/company_data -U user01 ↵

password: <smb user password>

smb> ls ↵

> bye ↵

⇒ For windows clients: open Run prompt → type

\\192.168.1.254/company_data (or) \\192.168.1.254 ↵

—X—

⇒ LINUX Creating CD-ROM ISO image:

→ dd is a perfect tool for copy a file, converting and formatting according to the operands. It can create exact CD-Rom iso image.

→ This is useful for making backup as well as hard drive installations require a working the use of ISO images.

Step ①: put the CD into CDROM

Step ②: Create CD-Rom iso image with dd command:

```
#dd if=/dev/cdrom  of=/tmp/cdimage.iso↵
```

where: dd → is the program used to convert and copy a file.

if → Defines an input file.

of → Defines an output file.

Note: Although we have been talking a lot about file systems as they relate to disk drives, the mount command can be used to mount other types of file systems as well.

→ for example, you usually have a /media directory off the root partition that is commonly used to mount the CD/DVD-ROM drive.

```
#mount -o loop /tmp/cdimage.iso /media↵
#cd /media↵
#ls↵
#vim /etc/fstab↵
/tmp/cdimage.iso  /media  iso9660  ro,loop  0 0
:wq!↵
```

FTP

(File Transfer protocol)

→ There are many different ways you can share files with users on your network.

→ This capability is important because you don't always want your users storing things locally on their desktop or laptop.

→ This protocol is used to upload and download the files over the Internet.

→ To transfer a file using the FTP protocol, a user must log in to an FTP server, which can be done with credentials or anonymously.

→ When the user is connected, she can traverse the directory structure for any directory or file for which she has permissions.

→ If the protocol is not configured properly, this can leave your entire system open to attack and make it hard to track if the attack is done through an anonymous connection!

→ The second big issue with the FTP protocol is that when the user logs in with a username & password, they are passed over the network in clear-text, meaning that anyone listening can see them.

→ So, why use the FTP protocol at all? It's easy to set up, and when used correctly, it's highly effective for delivering files to end users.

⇒ Configuring FTP:

Step ①: Grab the required package:

```
#yum install vsftpd -y ↵
```

Step ②: verify it was installed successfully:

```
#rpm -qa | grep vsftpd ↵
```

Step ③: Ensure that the service will start on system boot:

```
#chkconfig vsftpd on ↵
```

Step ④: verify the service starts on boot:

```
#chkconfig vsftpd --list ↵
```

→ To start the configuration of the FTP server, you need to look at the config file. For vsftpd, there is only one main config file; it's located at /etc/vsftpd/vsftpd.conf, which is where you configure the settings of the FTP server.

→ Let's look at which options are available in the config file:

```
# grep -v ^# /etc/vsftpd/vsftpd.conf ↵
```

Step ⑤: Open the configuration file

```
#vim /etc/vsftpd/vsftpd.conf ↵
```

```
anonymous_enable=YES          # Line no 12;
```

Defaulty anonymous users are enable. If you want to disable login permissions to anonymous users then

```
anonymous_enable=NO
```

Step (6):

→ once loged into a vsftp server, you'll automatically have access to only the default anonymous FTP directory "/var/ftp" and all its subdirectories.

→ Go to sharing location:

```
#cd /var/ftp ↵
#mkdir Download ↵
#cd Download ↵
#touch file1 file2 abc ↵
```

} To create a directory & files for downloading.

→ To create a directory for uploading:

```
#mkdir /var/ftp/upload ↵
#chmod 777 /var/ftp/upload ↵
```

Accessing the private users:

→ open the config file:

```
#vim /etc/vsftpd/vsftpd.conf ↵
```

```
local_enable=YES          # allows local users to log in
anon_upload_enable=YES    # for upload permissions
ftpd_banner = Welcome to FTP    # for ftp banner
write_enable=YES
```

Step ⑦:

→ Create the local users:

```
#useradd ftp1 ↵        #passwd ftp1 ↵
#useradd ftp2 ↵        #passwd ftp2 ↵
```

Step ⑧: Restart the service:

```
#service vsftpd restart ↵
```

→ To verify the service:

```
#service vsftpd status ↵
```

→ users should now able to login via FTP to the server using their new user names and passwords.

→ If you absolutely don't want any FTP users to be able to write to any directory then you should comment out the write_enable line in your config file:

```
#write_enable=YES
```

FTP Security: Let's look at some other options that can be used for basic security. you can disable the anonymous_enable option to prevent nonauthorized users from accessing the FTP server. the local_enable option, which is enabled by default, allows local system users to log in to the FTP server. keeping this option is usually safe option so that you don't need to maintain a second list of users that you want to be able to log in to the FTP server.

→ There is one other security step you should take for the FTP server. The userlist_enable option, which is set to YES by default, allows the vsftpd service to consult the "/etc/vsftpd user_list" file. When this option is used in conjunction with the user_list_deny option, all users in this file are denied access to the server and not even prompted for a password.

→ If you want to restrict any normal users to login into the FTP server then mention their names in the file

#vim /etc/vsftpd/ftpusers ↵

ftp1 #restrict ftp1

:wq! ↵

→ If you want to change this setting, however, you could set the userlist_deny option to NO. Then all users except for those listed in /etc/vsftpd/user_list are denied access. This setting is useful if you want only select individuals to be able to log in and not all your system users.

#vim /etc/vsftpd/user_list ↵

ftp2 #allow user

:wq! ↵

→ open the config file : #vim /etc/vsftpd/vsftpd.conf ↵

Userlist_Deny = NO

:wq! ↵

FTP users can't login telnet:

```
#usermod -s /sbin/nologin ftp1 ↵
#usermod -s /sbin/nologin ftp2 ↵
```

Now telnet users should not login.

⇒ Connecting FTP Server: (Method ①):

```
#ftp <FTP_Server_ip>
#ftp 192.168.1.254 ↵
username :
password :
```

FTP prompt commands:

ftp> pwd → Display serverside directory.
ftp> ! pwd → Display clientside directory.
ftp> ls → List the serverside files.
ftp> ! ls → List the clientside files.
ftp> cd → change directory at serverside
ftp> ! cd → change directory at clientside.
ftp> get → Download single file
ftp> mget → Download multible files.
ftp> put → upload single file
ftp> mput → upload multible files.
ftp> bye → To quit ftp prompt.

⇒ Connecting to FTP Server: (Method ②)

You need to test the FTP server from one of the clients, client01. To save time during the exam and when testing in the real world, you can use the command line FTP client lftp. This command includes many features for quick testing and verification that the FTP server is functioning properly.

Step ①: Install the lftp package on the client01 system.

```
#yum install lftp -y ↵
```

Step ②: Verify the installation of the lftp package:

```
#rpm -qa | grep lftp ↵
```

Step ③: Now you can connect to anonymous

```
#lftp 192.168.1.254 ↵
```

Step ④: On the client01 system, you connect to server254:

```
#lftp 192.168.1.254 -u ftp1 ↵
```

Now you are prompted for your password, and then you have FTP access to the server. From here, you can upload and download files using standard FTP commands.

—X—

DNS

(Domain Name Service)

→ When you're toying to access a website, you type in the name you are looking for and it comes up. In the background, through, DNS is what translates that website name into an IP-address so that the site may be accessed. This translation also occurs when you are connecting to other systems on your network through their hostnames instead of their IP-addresses.

→ DNS plays a critical role not only in your networks, but also on the Internet as a whole.

→ Domain Name Service, provides resolution of names to IP-addres and IP-address to Names.

⇒ Host file :

→ It provides resoultion of Hostnames to IP-address.

→ It can only resolve the name provided in the local host file.

→ you can add the name and IP-address in /etc/hosts file but we should have to maintain it all the Systems

⇒ The /etc/resolve.conf file:

This file is used by DNS clients to determine both the location of their DNS Server and the domains to which they belong.

nameserver 192.168.1.254

:wq!

=> The zone files:

→ In all zone files, you can place a comment at the end of any line by inserting a semi-colon ";" character then typing in the text of your comment.

→ By default, your zone files are located in the directory "/var/named".

Zone: Zone is a storage database. which contains all zone records. Two types of zone records are available.

(a) Forward Lookup Zone (FLZ):

→ Used for resolving hostname to ip address

→ It maintains host to IP-address mapping information.

(b) Reverse Lookup Zone (RLZ):

→ Used for resolving ip-address to host name.

→ It maintains IP-address to Host name mapping information.

→ Each zone file contains a variety of records. There are:

SOA (Start of Authority): The very first record is the Start of Authority record which contains general administrative and control information about the domain.

NS (Name Server): contains the IP-address or CNAME of the nameserver.

A (Address): Maps the hostname to an IP-address.

Step ⑥: open the second config file:

```
#vim /etc/named.rfc1912.zones ↵
```

→ Go to last line:

```
zone "example.com" IN {
    type master;
    file "example.for";
    allow-update { none; };
};

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

```
:wq! ↵
```

Step ⑦: Go to zones location:

```
#cd /var/named ↵
```

⇒ **configure the FLZ:**

→ copy named.localhost file into example.for:

```
#cp named.localhost  example.for ↵
```

→ Change the group name of example.for

```
#chgrp named example.for ↵
```

PTR (pointer): Maps the IP-address to a hostname.

MX (Mail Exchange): Lists the mail servers for your domain.

CNAME (Canonical Name): used as an alias.

⇒ configuring a DNS server:

Step ①: Install the required packages:

#yum install bind* -y↵

Step ②: verify that the packages have been installed:

#rpm -qa|grep bind↵

Step ③: Service is set to start on System boot:

#chkconfig named on↵

Step ④: verify that the Service is set to start on boot:

#chkconfig named --list↵

Step ⑤: open the main config file:

#vim /etc/named.conf↵

listen-on port 53 { 127.0.0.1; 192.168.1.254; }; #line no 11;

allow-query { localhost; 192.168.1.0/24; }; #line no 17;

:wq! ↵

#vim example.rev ↵

```
$TTL  1D
@   IN  SOA  server254.example.com.  root.example.com. (
                                        0   ; Serial
                                        1D  ; refresh
                                        1H  ; retry
                                        1W  ; expire
                                        3H) ; minimum
        IN      NS      server254.example.com.
server254   IN      A       192.168.1.254
254         IN      PTR     server254.example.com.   } Network
250         IN      PTR     server250.example.com    } Hosts
```

:wq! ↵

Step ⑧ : configure the hostname

#hostname server254.example.com ↵

(or)

#vim /etc/sysconfig/network ↵

HOSTNAME = server254.example.com

→ **Add the DNS IP-address:**

#vim /etc/resolv.conf ↵

nameserver 192.168.1.254

:wq! ↵

#vim example.for↵

```
$TTL  1D
@     IN    SOA   server254.Example.com.  root.example.com.(
                                          0     ; Serial
                                          1D    ; refresh
                                          1H    ; retry
                                          1W    ; expire
                                          3H )  ; minimum
@          IN     NS     server254.example.com.
@          IN     A      192.168.1.254
server254  IN     A      192.168.1.254
server250  IN     A      192.168.1.250
www        IN     CNAME  server254
```

Network Hosts

:wq! ↵

⇒ Configure the RLZ:

→ copy named.loopback file into example.rev

#cp named.loopback example.rev↵

→ Change the groupname of example.rev

#chgrp named example.rev↵

Step ⑨: To check the test configuration files

```
#named-checkconf  /etc/named.conf ↵
#named-checkconf  /etc/named.rfc1912.zones ↵
```

Step ⑩: To check the errors at zone files location:

```
#named-checkzone  example.com  /var/named/example.for ↵
#named-checkzone  example.com  /var/named/example.rev ↵
```

Step ⑪: Now you can start the service:

```
#service named restart ↵
```

⇒ DNS Utilities and Troubleshooting:

→ for the server and client, there are a handful of utilities you can use to verify the functionality of DNS.

dig	:	DNS lookup utility
host	:	DNS lookup utility.
ping	:	Network or hostname from an ip address
nslookup	:	Utility to lookup a hostname foram an Ip-address.
hostname	:	Utility to sets or show the system hostname (FQDN).

→ The most basic test after the DNS server has been set up properly is to ping the hostname of the name server and the domain itself. If both return a reply, your name server is querying properly.

Step ①: ping the hostname of the name server for your network.

```
#ping server254↵
```

Step ②: ping the domain name to ensure that the primary name server

```
#ping example.com↵
```

→ Another useful tool that can help test whether your DNS server is functioning properly is the host command.

Step ③:

```
#host server254↵
#host 192.168.1.254↵
```

→ Another useful tool nslookup:

Step ④:

```
#nslookup example.com↵
#nslookup server254↵
#nslookup 192.168.1.254↵
```

→ Next, we look at a more in-depth utility: the dig command.

Step ⑤:

```
#dig @server254↵
#dig @server254 example.com↵
#dig -x 192.168.1.254↵
```

Step ⑥: Query the current FQDN of your system:

```
#hostname↵
```

Web Services

→ The most commonly used web server in the world today is Apache - and with good reason. Built with security in mind, Apache is a solid and stable web server that has been around for years. The module design allows for scalability and ease of use. Apache can also be used to host multiple websites at a single time through the use of its virtual hosts feature. There is also an option to use the SSL protocol, making websites safe and secure. This secure base provides a platform for developers to use when writing secure code for banks, retail sites and so on.

⇒ The Apache Web server :

→ Today, with web 2.0 on the rise and Software as a Service (SaaS) becoming more prevalent, Apache has begun to play a larger role. It is important to know how to install and secure Apache correctly.

→ Let's look at some of the new features in Red Hat 6.

- Apache has been upgraded to version 2.2 from 2.0.
- It has improved caching modules.
- It provides support for proxy load balancing through mod_proxy_balancer.
- It provides support for large files, allowing web servers to handle files larger than 2GB.
- It has improved authentication and authorization support.

→ Now that the web server is installed, we can shift our attention to the config files and directories. During the installation, a directory (/var/www) is created with a set of subdirectories. This directory tree is the place where you store your websites.

→ There are also a few config files to look at:

/etc/httpd/conf/httpd.conf	: Main config file
/var/log/httpd	: Log file directory for the web server.
/usr/lib64/httpd/modules	: Modules for Apache.

→ In this main config file, we discuss specifically the global environment and main server options. Here are some common options for the global sections:

ServerRoot	: Defines where the config files are held.
Timeout	: Specifies the time before a request time out (default 120 sec)
Listen	: Indicates the port number to listen on
User	: Identifies the user to run the web server as
Group	: Identifies the group to run the web server as
LoadModule	: Defines a module to load when the web server starts.
DocumentRoot	: Defines where the website files are located.
ServerName	: Defines a server name or IP address and port number.

Step ②: Go to web page location

```
#cd /var/www/html ↵
#vim index.html ↵  Creates a web page
```

```
<html>
<body bgcolor=yellow>
<marquee><h1> THIS SAMPLE WEB PAGE </h1>
                                    </marquee>
</body>
</html>
:wq! ↵
```

Step ③: Open the hosts file:

```
#vim /etc/hosts ↵
```

```
192.168.1.254    server1254.Example.com    server1254
```

```
:wq! ↵
```

Step ④: setting the hostname

```
#vim /etc/sysconfig/network ↵
```

```
HOSTNAME = server1254.Example.com
```

```
:wq! ↵  (or)
```

```
#hostname server1254.Example.com ↵
```

Step ⑤: To restart the httpd service:

```
#service httpd restart ↵
```

⇒ Installing Apache:

Step①: Install the required packages:

```
#yum install http* -y ↵
```

Step②: verify that the packages were installed correctly:

```
#rpm -qa | grep http ↵
```

Step③: make sure that the service is set to start when system boots:

```
#chkconfig httpd on ↵
```

Step④: verify your changes:

```
#chkconfig httpd --list ↵
```

⇒ configuring the web server:

→ Open the main config file:

Step①: `#vim /etc/httpd/conf/httpd.conf ↵`

→ go to last line of the config file

```
<VirtualHost *:80>
    ServerAdmin root@server1254.Example.com
    DocumentRoot /var/www/html
    ServerName server1254.Example.com
    ErrorLog logs/server1254.Example.com-error_log
    CustomLog logs/server1254.Example.com-access_log common
    DirectoryIndex index.html
</VirtualHost>
```

Step ⑥: To only reload the service

```
# service httpd reload ↵
```

* **Note:** One other option to keep in mind is the graceful parameter. It restarts the web server, allowing it to read the new config file changes without disconnecting any currently connected clients. The only downfall here is that the currently active connections use the old config file until they terminate their connection and reconnect. You can use it as follows.

```
# service httpd graceful ↵
```

⇒ **Troubleshooting Apache:**

→ One of the best tools available for troubleshooting Apache is its log files. Each log file has a separate directory from the other log files on the system, which makes them easy to pick out.

→ There are two basic files you can you to troubleshoot it:

/var/log/httpd/access_log : Logs all access to the server.

/var/log/httpd/error_log : Logs error messages from the server

→ If you're using a secure site, for SSL:

/var/log/httpd/ssl_access_log : Logs access to the secure site

/var/log/httpd/ssl_error_log : Logs error messages from the secure site

/var/log/httpd/ssl_request_log : Logs requests made to the server from clients.

→ Another useful tool to troubleshoot web server issues with is the elinks browser. This text-based browser lets you easily check websites.

Step ①: Install the required package:

```
#yum install elinks -y↵
```

Step ②: you can test your site with the following:

```
#elinks 192.168.1.254↵
        (or)
#elinks server254.Example.com↵
```

Step ③: If you want to test for a secure site

```
#elinks https://192.168.1.254↵
```

Step ④: To quit the elinks browser, just press q.

⇒ For GUI Test: → Run the firefox

→ In URL Type : server254.Example.com

(or)

http://192.168.1.254↵

⇒ Apache Security:

→ This section goes more in depth with apache security because it is such a large topic. For the exam and particularly in the real world, you need to be able to configure host-based and user-based security for Apache.

(a) Host-Based Security :

To start, you can limit the IP address on which the server can listen for incoming connections. you use the Listen option to define an IP-address and a port, usually 80. This capability is helpful if you have multiple IP-address because it allows access only to the IP-address, and therefore that network, you specify.

→ Let's configure this Apache server to allow clients to access it only from the 192.168.1.0/24 networks.

→ Let's look at the <Directory> section, which holds options pertaining to the main server config. within this section, the first thing you do is restrict the networks, IP addresses, or domains that have access to the web server.

→ The comple <Directory> section now looks like this:

```
<Directory "/var/www/html">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from 192.168.1        (or) #.example.com
</Directory>
```

→ After you determine the hosts that you want to allow or deny access to your web server, you next need to define which order they are applied in:

Order allow,deny : Allows first and then denies everything else.

Order deny,allow : Denies first and then allows everything else.

Options Indexes FollowSymLinks : Allows indexing of the directories and allows Symlinks outside this <Directory> section.

AllowOverride None : Does not allow any normal user to make changes in Document Root.

(b) User-Based Security:

→ Now that we have configured some host-based authentication, we can move on to user-based authentication. This provides a way to allow only certain users or groups to access the web server or portions of the web server. Here are the options that can be used for user based security:

AuthType : Defines the authentication type

AuthName : Adds a comment for the user to see on login

AuthUserFile : Specifies the file used to define username & password.

AuthGroupFile : Is similar to the user file but for groups.

Require : Specifies the users or groups that can log in.

→ Suppose you want to password protect the main site because it contains information for human resources (HR) that shouldn't get out.

Step ①: Define the following under the main server section in the config file:

```
<Directory "/var/www/html">
    AuthType Basic
    AuthName "password Restricted Area"
    AuthUserFile /etc/httpd/conf/userfile
    Require user user01
</Directory>
```

Step ②: Create the sole user who will need access to this site:

```
#useradd user01↵
#htpasswd -cm /etc/httpd/conf/userfile user01↵
```

Step ③: Restart the web server:

```
#service httpd reload↵
```

→ Now Access the main page by pointing your web browser from any system on the 192.168.1.0/24 network to http://192.168.1.254/index.html. you should ~~also~~ prompted for a username and password. This is great! you now have a secure main site, and HR can begin posting documents here.

⇒ Virtual Hosts:

→ One of the big benfits of Apache is that you can run multiple websites on a single host. this is done through a virtual host configuration, where you can define different sites in your main Apache config file.

→ We have already discussed the global options and main server options in the main config file.

NameVirtualHost	: Specifies the hostname (or) IP-address for the virtual host
ServerAdmin	: Indicates the email address for the web master
DocumentRoot	: Defines the directory for the virtual host files.
ServerName	: Defines the URL for the virtual Hosts
ErrorLog	: Specifies the location for the error log.
CustomLog	: Specifies the location for a custom log.

Step①: open the main config file:

#vim /etc/httpd/conf/httpd.conf ↵

```
<VirtualHost *:80>
    ServerAdmin     root@server254.mysite.com
    DocumentRoot    /var/www/site1
    ServerName      www.site1.com
    ErrorLog        logs/site1_access error_log
    CustomLog       logs/site1_access_log common
</VirtualHost>
```

Step ②: In main config file line no 990, remove the #

```
nameVirtualHost *:80
```

Step ③: Create a new directory under "/var/www".

```
#cd /var/www
#mkdir /var/www/site1 ↵
#vim index.html ↵ under /var/www/site1
- - - - -
- - - - -
- - - - -
:wq! ↵
```

Step ③: Open the host file:

```
#vim /etc/hosts ↵
192.168.1.254    www.mysite.com
:wq! ↵
```

Step ④: Don't forget to verify the syntax before running with the config:

```
#httpd -S ↵
```

Step ⑤: Restart the service httpd:

```
#service httpd reload ↵
```

→ go to firefox check the site www.mysite.com

```
http://www.mysite.com ↵
```

⇒ How to add Virtual IP-address in Linux:

→ Now in linux operating system lets consider a server which is connected to large environment or consider a web servers used to host multiple information then we can give different ip_address to the single Host System.

→ So the virtual IP address (VIP's) allows you to use multiple ip address in single physical network Interface.

→ So let us consider the IP-address assigned and the device name as "eth0".

→ Now let us see how to add another ip address in the same physical address eth0:0

→ To create an IP_address temporarly:

```
#ifconfig eth0:0 192.168.1.100 netmask 255.255.255.0
                                                    up↵

#ifconfig ↵ To verify
```

→ To create an IP-address permanently:

Step ①: #cd /etc/sysconfig/network-scripts ↵

Step ②: #cp ifcfg-eth0 ifcfg-eth0:0 ↵

Step ③: #vim ifcfg-eth0:0 ↵

```
DEVICE=eth0:0
ONBOOT=yes
IPADDR=192.168.1.100
NETMASK=255.255.255.0
:wq!
```

Step ④: #service network restart ↵ Restart the network

#ifconfig ↵ To verify

Squid web proxy

→ A proxy server is a device that usually sits between a client and the destination the user is toying to reach. It can provide security, anonymity, and even protection for the client behind the proxy. To help in this process is squid, which is a web proxy server for Red Hat.

→ It sits between the client and web server that the user is toying to connect to. Many times these devices are used when you want to control access to the Internet (think web filtering).

→ As a web proxy, it can also cache data that users request from the web and make it locally available, reducing the load on your external devices such as gateways and firewalls.

→ When setting up your proxy server, you need to know the following items:

/etc/sysconfig/squid	: Startup options for the config file.
/etc/squid/squid.conf	: Main config file for the service.
/var/spool/squid	: Cache location on the proxy server.
/var/log/squid	: Log files for the proxy server.

→ Let's look at some of the main configuration options:

http_port	: Specifies the port to listen on
visable_hostname	: Identifies the name of the Squid Server
access_log	: keeps track of the web pages that are downloaded.
acl	: Defines an access control list
http_access	: Defines which System or Network have access

⇒ Configuring the proxy :

Step ①: Install the package with the following command:

```
#yum install squid* -y↵
```

Step ②: To verify that package:

```
#rpm -qa | grep squid ↵
```

Step ③: Enable squid to start at boot:

```
#chkconfig squid on↵
```

Step ④: Verify the service will start at boot:

```
#chkconfig squid --list↵
```

Step ⑤: you can set the visible_hostname option to the name of your server:

```
#vim /etc/squid/squid.conf ↵

        visible_hostname = server1254

:wq! ↵
```

⇒ Web proxy Security:

→ Squid uses host-based security through the use of access control lists. These ACL's are configured in the main config file, /etc/squid/squid.conf. In the config file, you can define an ACL for your network and give all other networks access to the proxy server.

Step ① `#vim /etc/squid/squid.conf ↵`

```
acl my_networks src 192.168.1.0/24 192.168.2.0/24
acl allow_dom dstdomain example.com
acl badsite url_regex www.facebook.com
acl badsites url_regex "/etc/squid/squid_list"
acl restrictedhost src 192.168.1.100
acl restrictednetwork src 192.168.2.0/24
acl badtime time 14:00-23:00
```

→ you also need to enable HTTP access for those networks:

```
http_access   allow   my_networks
http_access   allow   allow_dom
http_access   deny    badsite
http_access   deny    badsites
http_access   deny    restrictedhost
http_access   deny    restrictednetwork
http_access   deny    badtime.
```

(or)

```
http_access allow my_networks allow_dom
http_access deny  badsite badsites restrictedhost
                  restrictednetwork badtime
```

:wq! ↵

Step ②: Now you can start the squid service to test the proxy:

```
# service squid start ↵
```

Step ③: To verify that the squid:

```
# service squid status ↵
```

Step ④: Test the squid :

→ open the firefox → go to edit → preferences → advanced → Network → Settings → ⊙ Manual proxy configuration:

HTTP proxy: 192.168.1.254 port: 3128

NIS

(Network Information Service)

→ Generally NIS is called as a yp service.
↳ yellow page.

→ NIS is a simply client/server data base it was developed by SunMicro Systems as part of their SUN operating System.

→ It is used for Directory service which shares the user, group, password, host and protocol information.

→ NIS maintain only single domain information but not multible domains.

→ NIS is called as ~~as~~ domain concept it maintain the centralized hierarchy structure.

→ NIS is used in intranetwork, we can't share the multible domain information.

NIS : Network Information Service.
→ NO port number of NIS.

LDAP : Lightweight Directory Access protocol.
port no: 389

ADS : Active Directory protocol.

→ NIS using the following daemons with start service:

portmap : the foundation Rpc daemon upon which NIS runs.

yppasswdd : Lets users change their passwords on the NIS server from NIS clients.

ypserv : Main NIS server daemon

ypbind : Main NIS client daemon

ypxfrd : used to speed up the transfer of very large NIS Maps.

⇒ <u>configuring the NFS:</u>

<u>Step①</u>: Install required package for nfs server:

#yum install nfs*-y↵

<u>Step②</u>: verify that the packages have been installed:

#rpm -qa | grep nfs ↵

<u>Step③</u>: Service is set to start on System boot:

#chkconfig nfs on↵

<u>Step④</u>: verify that the service is set to start on boot:

#chkconfig nfs --List↵

Step ⑤: To share /home folder of nis server.

```
#vim /etc/exports ↵
    /home    *(rw,sync)
:wq! ↵
```

Step ⑥: Show the exported folder:

```
#exportfs -avf ↵
```

Step ⑦: Restart the nfs service:

```
#service nfs restart ↵
```

⇒ Configuring the NIS:

Step ①: Install required packages for NIS server:

```
#yum install yp* ↵
```

Step ②: Assign the NIS Domainname:

```
#nisdomainname india.com ↵ (or)
#vim /etc/sysconfig/network ↵
    NISDOMAIN = india.com
:wq! ↵
```

Step ③: Run the database tool for creating home directory:

```
#/usr/lib64/yp/ypinit -m ↵
```

→ It will ask next host to add
press ctrl+D then Y ↵

Step ④: Edit your yp.conf file:

```
#vim /etc/yp.conf↵
    ypserver 127.0.0.1
:wq!↵
```

Step ⑤: Create a user:

```
#useradd user01↵
#passwd user01↵
```

* Note: If your nis server is already running, and you create a new user, then you have to update the NIS domain's authentication files by executing the make command in the /var/yp directory:

```
#cd /var/yp↵
#make↵
```

Step ⑥: Restart following services:

```
#service ypserv restart↵
#service yppasswdd restart↵
#service ypxfrd restart↵
#service ypbind restart↵
```

Step ⑦: Service is set to start at boot time:

```
#chkconfig ypserv on↵
#chkconfig yppasswdd on↵
#chkconfig ypxfrd on↵
#chkconfig ypbind on↵
```

⇒ client configuration:

The authconfig or the authconfig-tui program automatically configures your NIS files after prompting you for IP-address and domain of the NIS server.

#authconfig-tui ↵

↓

[*] Use NIS → Next ↵

↓

Domain : india.com

Server : 192.168.1.254 → Ok ↵

→ NIS client commands:

ypwhich : Displays the name of the master NIS server.

ypcat : print the entries in an NIS database.

yppasswd : changes user passwords and information on the NIS server.

ypmatch : print the value of one or more entries in an NIS server.

yppoll : Displays the server and version number of an NIS map.

→ print the NIS server's password database:

#ypcat passwd ↵

→ print user01's password entry:

#ypmatch user01 passwd ↵

→ To display a list of the maps the NIS server is sharing using:

#ypcat -x ↵

⇒ Using AutoFS:

→ To make your life as a System administrator easier, you also can use AutoFS, which is an automated file system. The benfit of this is that remote resources can be mounted automatically and without the need for the root user to perform the mount. This is done through the use of a special config file called maps.

→ There are two key files to know when working with AutoFS.

/etc/sysconfig/autofs : Main config file for the service.

/etc/auto.master : Master map file

Step ①:

→ Here is what my /etc/auto.master file looks like:

```
#vim /etc/auto.master↵
/misc   /etc/auto.misc
/home   /etc/auto.remote
:wq!↵
```

Step ②:

→ To create /etc/auto.remote file:

```
#vim /etc/auto.remote↵
user01   -fstype=nfs,soft   192.168.1.254:/home/user01
                (or)
*        -fstype=nfs,soft   192.168.1.254:/home/&
                (or)
:wq!↵            -rw,sync
```

Step ③: Stop the autofs service:

```
#service autofs stop↵
```

Step ④: we need to start autofs service:

```
#service autofs start↵
```

Step ⑤: login the user01: #su - user01↵

Email Services

→ The world today runs on email, and without it, we would have a hard time functioning. Because of this, we need solid and reliable email servers to ensure that our email is processed correctly and either delivered or received on time.

→ For Red Hat, Sendmail is the default for sending mail and Dovecot is the default for ~~xxxx~~ receiving. Here, we focus more on postfix for sending and Dovecot for receiving.

→ The email system is divided into three different parts. There are

(a) Mail user agent (MUA)

(b) Mail Delivery agent (MDA)

(c) Mail Transfer agent (MTA)

(a) **Mail User Agent (MUA):** A Mail User Agent is a program that allows you to receive and send e-mail messages; it's usually just called an e-mail program. The MUA is a mail client of some sort, such as Thunderbird or Evolution.

(b) **Mail Delivery Agent (MDA):** The Mail delivery agent handles the delivery of mail from the receiving mail server to the spool where the mail sits until an MUA picks it up for the user.

(c) **Mail Transfer Agent (MTA):** The mail transfer agent is responsible for moving mail from one server to another until it arrives at its destination.

→ There are two main protocols used for retrieving email on an Mail Delivery Agent (MDA):

(a) post office protocol (pop3)

(b) Internet Message Access protocol (IMAP)

(a) **post office protocol:** The pop3 is an application layer internet standard protocol used by local e-mail from a remote server over a TCP/IP connection. which is used for retriving email and, in certain cases, leaving a copy of it on the server.

(b) **Internet Message Access protocol:** which is used for coordinating the status of emails (read, deleted, moved) across multiple email clients. with IMAP, a copy of every message is saved on the server, so that this synchronization task can be completed.

⇒ **SMTP with postfix:**

Red Hat provides both Sendmail and postfix as viable mail programs. we focus only on postfix for multiple reasons.

→ postfix provides for easier administration, allows increased security, and supports virtual domains.

→ up until RHEL5, Sendmail was the default mail program for the Red Hat operating System, but this has changed to postfix with the release of RHEL6.

→ Here are the management commands for postfix:

mailq : Allows you to view the mail queue.

postmap : postfix lookup table management

postsuper : Allows you to perform maintenance jobs on the postfix queue

postconf : postfix configuration utility.

→ The main config file for postfix are located in the "/etc/postfix".

master.cf : Contains settings to control the master service.

main.cf : Opens the primary config file for postfix.

access : provides access control.

transport : Maps email addresses to relay hosts.

⇒ Configuring postfix:

→ postfix actually starts a service called master, which is its main service. This master service starts three other services beside itself: **nqmgr, pickup and smtpd.**

nqmgr: This service is responsible for mail transmission, relay, and delivery.

pickup: This service transfers messages.

smptpd: This service directs incoming mail.

Step ①: Install the postfix package

```
#yum install postfix* -y↵
```

Step ②: verify that the package installed correctly:

```
#rpm -qa | grep postfix ↵
```

Step ③: you need to stop the sendmail service, Because you are going to start postfix in place of the default Sendmail:

```
#service sendmail stop↵
```

Step ④: you also need to prevent it from starting during system boot:

```
# chkconfig sendmail off ↵
```

Step ⑤: verify:

```
# chkconfig sendmail --list↵
```

Step ⑥: change the default mail program to postfix:

```
#alternatives --config mta↵
```

Step ⑦: verify that the current default for mail is postfix:

```
#alternatives --display mta | grep current
```

Step ⑧:

→ the following variables need to be set for the postfix server to work properly:

myhostname : Defines the full hostname of the postfix server.

mydomain : Defines the Domain name

myorigin : Defines the name that outgoing mail originates from

inet_interfaces : Identifies the interface on which to receive mail

mydestination : Defines the domains for which postfix accepts mail

mynetworks : Lists trusted networks

virtual_alias_maps : Defines virtual aliases for incoming mail.

→ Open the configuration file:

#vim /etc/postfix/main.cf ↵

myhostname = server254.example.com # line no 75;
mydomain = example.com # line 83;
myorigin = $mydomain # line no 99;
inet_interfaces = ~~$myhostname~~ all # line no 113; # 164;
mydestination = $myhostname, localhost.$mydomain, localhost
mynetworks = 192.168.1.0/24, 127.0.0.0/8 # line 245;

Step (9): check that the directory structure and config file are correct:

#postfix check ↵

Step (10): Now you can restart the service as follows:

service postfix restart ↵

→ Alternatively, you can query to ensure the three domains are running properly:

#ps aux | grep post ↵

Step (11): To verify the service postfix:

#service postfix status ↵

⇒ **postfix Security:** Because mail servers are omnipresent, it is vital that you understand how to lock down particular features of them. For outgoing mail servers that deal with the SMTP protocol like postfix, you should make sure that it is not left open to be used as a mail relay. This would allow outsiders to use your server for spam.

→ If you want to allow server250 to relay mail, but not either of the client systems, you could do the following:

#vim /etc/postfix/access ↵

192.168.1.250 RELAY

192.168.1.10 REJECT

client02 REJECT

:wq! ↵

→ Define a relayhost option with the name of the smarthost you'd like to relay through:

#vim /etc/postfix/main.cf ↵

relayhost = mail.example-a.com

:wq

#service postfix restart ↵

⇒ Alias Mapping:

Postfix is able to use aliases for managing domains and users. The /etc/aliases file contains the current mappings and should be edited to reflect any changes required for your network. you can use the aliases file to create distribution groups or redirect mail to users who no longer exist in your domain. Example admin mails should be received by raju.

Step ①: #vim /etc/aliases ↵

admin: raju

:wq! ↵

Step ②: then run the newaliases command to update the database:

#newaliases ↵

⇒ Receiving Mail with Dovecot:

Now that you can send mail, you also need to be able to receive it. Dovecot enables you to set up an incoming mail server that allows for multiple protocols to be used when accessing mail.

Step ①: you first need to setup Dovecot by installing the correct package:

```
#yum install dovecot -y ↵
```

Step ②: verify the installation:

```
#rpm -qa |grep dovecot ↵
```

Step ③: Enable the service to start on system boot:

```
#chkconfig dovecot on ↵
```

Step ④: verify the service will start at boot:

```
#chkconfig dovecot --list ↵
```

* **Note:** In RHEL6, the config file for Dovecot has been moved. It is now located at /etc/dovecot/dovecot.conf. previously in RHEL5, it was located at /etc/dovecot.conf.

Step ⑤: Start by opening the file for editing:

```
#vim /etc/dovecot/dovecot.conf
```

Define the protocols that you'd like to have the Dovecot Server

```
protocols = imap pop3
```

You should also define the ip_address for the server to listen on, disable SSL, and define where user mailboxes should be stored

```
listen = 192.168.1.254
ssl_disable = yes
mail_location = maildir:~/maildir
```

:wq!↵

Step ⑥ : Now start the dovecot service

```
# service dovecot start↵
```

Step ⑦ : Verify that it is running properly:

```
# service dovecot status↵
```

⇒ Testing the Mail Server:

Now verifying the functionality of your mail servers is always a good idea to make sure they are working properly.

→ First, you need to check the postfix server both locally and remotely to make sure outgoing mail is working.

→ You can use the mail command to make some quick tests to the SMTP protocol.

Step ①: for the local mail test, use the following:

#echo "Hello user1254" | mail -s "Local Test" user101↵

Step ②: for the remote mail test, use the following:

#echo "Hello again user1254" | mail -s "Remote test"

user101@example.com

→ After your messages are sent, you can use the mailq command to view the queue of messages that have been sent or are waiting to be sent.

→ Now you can see that everything for the postfix server seems to be operating normally. Now let's move on the Dovecot Server.

→ you can use the mutt command to read mail from the Dovecot server that you just sent to $\frac{user01}{server1254}$.

Syn: mutt -f <imap|imaps|pop|pops>://<user><port>

#mutt -f imap://user01143↵

→ Display current mail in the queue:

#mailq ↵

→ for some reason, the message seems to be stuck in the queue you can delete it from the queue and send it again later.

Syn: postuser [options]

-d Deletes one message with the named queue ID.
-r Requeues a message
-v provides verbose logging.

→ Delete the stuck message on the queue:

#postsuper -d 099FCA110E ↵

→ verify that the queue is now clean:

#mailq ↵

Step ③: A third way to test the mail server is accepting connections properly is to telnet into the postfix server on port 25.

#telnet 192.168.1.254 25 ↵

#telnet 192.168.1.254 110 ↵

username: user01 ↵

password: xxx ↵

→ you can see that everything connected fine. Both the mail services are running properly.

→ Display current mail in the queue:

#mailq ↵

———x———

Network Install

→ Installing Red Hat Enterprise Linux is an important topic, even though it is no longer included on the Red Hat exams.

→ Network installations are still included, however, and knowing which method to use when can help you by saving time on installations.

→ Using kickstart is also key in deploying RHEL in the real world because it is a heavily used technology.

⇒ Kickstart Server Setup :

→ The most widely used network installation setup for Red Hat is done through a kickstart server.

→ It enables you to perform network installations with flexible options such as pre- and post-package customization, custom scripts, logging, and more. It also has benefit of being fully automated.

→ Kickstart enables you to install Red Hat over the network via the HTTP, FTP (or) NFS protocols. I chose to use the HTTP protocol here because it was the quickest to set up and slightly easier than the other two protocols.

→ An HTTP kickstart server also has fewer configuration steps, for those attempting this for the first time.

Step①: To start, you need to install the Apache web server:

```
#yum install http -y ↵
```

Step②: verify the package was installed:

```
#rpm -qa | grep httpd ↵
```

Step③: Start the apache service:

```
#service httpd start ↵
```

Step④: Enables the service to start on boot:

```
#chkconfig httpd on ↵
```

Step⑤: verify:

```
#chkconfig httpd --List ↵
```

Step⑥: Create the following directory:

```
#mkdir /var/www/pub ↵
```

* **Note:** The /var/www directory is the default location where Apache stores files that clients can access. It is within that directory that you create a "pub" directory, which really is just used to hold the contents of the Red Hat DVD that will later be installed on the client.

Step ⑦: you should ensure that the Red Hat CD is mounted in the CD drive:

```
#mount /dev/dvd /mnt↵
```

Step ⑧: Now copy the files from DVD to the directory previously created:

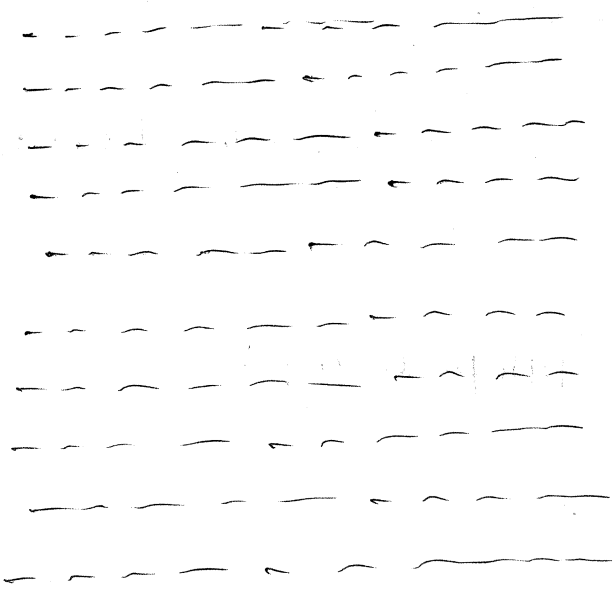
```
# cp -VR /mnt/* /var/www/pub↵
```

Step ⑨: when the install files are in place, you need to make one last directory:

```
#mkdir /var/www/pub/kickstart↵
```

Step ⑩: At this point, you would normally create your kickstart file

```
# touch /var/www/pub/kickstart/redhat-base.cfg↵
#cat /var/www/pub/kickstart/redhat-base.cfg↵
```



→ To install the GUI tool, use the following:

Step ⑪: #yum install system-config-kickstart↵

→ To launch it, use the command:

#System-config-kickstart↵

→ One benfit of installing the GUI tool on a server where you may not have a desktop manager is that it comes with a command-line syntax validator. This command can be used to verify the syntax of your kickstart files, which help in the troubleshooting process. My current production kickstart files are a couple of hundred lines each, so having something to check syntax is always helpful.

Step ⑫: After configure of the above dialogue box save the file with name "redhat-base.cfg" under the directory "/var/www/pub/kickstart".

Step ⑬: To give permissions to "redhat-base.cfg" file.

#chmod 777 redhat-base.cfg↵

Step ⑭: configure DHCP service:

Step ⑮: Restart the service

#service dhcpd restart↵