LINUX CONCEPTS

SYSTEM ADMINISTRATION CONCEPTS:

INTRODUCTION TO LINUX:-

Kernel:-

Kernel is nothing but the core part of an operating system which provides coordination between user and hardware.
Example: vmlinuz for Linux.

Shell:-

Shell is a mediator which is going to translate the human level language to machine level language (binary) and vice versa.

Examples: bash, csh, ksh

History of Linux:-

In 1990, Linus torvalds, a graduate student from University of Helsinky designed a UNIX like kernel on 386 Intel machine and gave this to open source foundation.

Linux distributions:-

1. Red hat
2. SUSE
3. Linux Mandrake
4. Puppy Linux

5. Ubuntu
6. Debain
7. BOSS
8. Turbo Linux
9. Slack ware Linux

Features of Linux:-

Open source:-

Free software along with the source code and documentation.

Multi tasking:-

Capable of running multiple applications and process at the same time.

Multi user:-

Allows multiple users to login and use the resources at the same time (default 7 users can login).

Portability:-

Can be installed on all hardware architecture.

Scalability:-

Same operating system can be used on a desktop to a super computer.

Reliability:-

Large servers have been successfully being running without single second of down time.

Security:-

Inbuilt firewall (ip tables) and SELinux.

File system hierarchy standard:-

File system:-

File system is a mechanism used in the operating system for storing or arranging the data in a systematical manner in a particular storage device.

Types of file system:-

1. Disk based
2. Network based
3. Virtual based

Disk based:-

It is a type of file system used for utilizing the individual storage device.

Example: 1. ext2

2. ext3

Network based:-

Using network file system we can transfer/share the data or resources from one system to a remote system.

Example: 1. NFS [Network File System]

2. CIFS [Common Internet File System]

Virtual based:-

Using virtual file system we can improve the system performance by dedicating apart of hard disk to act as a virtual RAM.

Example: Swap

File system hierarchy:-

/:-

Slash is a top level working directory in Linux and Unix platform. It is also known as parent directory.

/root:-

This is a default home directory of super user. It contains the data generated by super user.

Example: super user

Root---/root

/home:-

This directory contains the profiles of all the normal users.

Example:-

Normal users

1. user1- /home/user1

/boot:-

This directory contains the static data which is used by OS at the time of booting.

Example:-

1. GRUB
2. Vmlinuz

/sbin:-

This directory contains the administrative commands used by super users.

Example: fdisk, netconfig

/bin:-

This directory contains the common commands used by both types of users (administrator & non-administrator).

Example: ls, mkdir

/usr:-

USR stands for Unique System Resources. It contains all the program related files.

/var:-

Var contains all the variable data which keeps on changing.

Example: system log files, e-mail accounts.

/dev:-

Dev contains all the device information connected to a particular system.

Example: cd drive, HDD, mouse etc.

/etc:-

etc contains all the configuration files related to the system and network resources.

/media:-

This directory is used for accessing the external devices like pen drive or cd –Rom.

/opt:-

This directory is basically used for installing the 3rd party applications.

Methods of installation:-

1. Standalone
   a) cd
   b) dvd
2. Network
   a) nfs
   b) ftp
   c) http

Console:-

Console is a default location, where a user is going to interact with the operating system. By default there are 7 consoles.

For graphical based:

Alt + ctrl +f7

For text based:-

Alt +ctrl+f6

Alt +ctrl+f5

Alt +ctrl+f4

Alt +ctrl+f3

Alt +ctrl+f2

Alt +ctrl+f1

#tty is the command to check in which console we are working.

Login prompt:-

[root@localhost~]#

Here root is the user name.

Localhost is the machine name.

~ is the present working directory.

# is the privilege mode.

Note: The administrative account in Linux or Unix platform is given by ‘#’ to indicate that is a privilege mode.

For all the normal users the ‘$’ is being assigned.

Command:

It is nothing but a script or a program used for providing instructions to the OS.

1. To check the OS name:- #uname
2. To check the release of OS :- #uname –r
3. To check the present working user account:- #whoami
4. To check the present working location:- #pwd
5. To list the contents of present working directory:-#ls
6. To list the properties:- #ls –l
7. To check the inode numbers:- #ls -i
8. To check the hidden objects:- #ls –a
9. To list the files with all properties:- #ls –ali
10. To check the system date:- #date
11. To change the system date:-

    #date –s "Thu jun 19 13:20:20 IST 2011"
12. To check the calendar :- #cal
13. To check the calendar of particular year :- #cal 2011
14. To check the calendar of specific month and year :-

    #cal 2 2011
15. To perform calculations:- #gnome-calculator

<u>For creating files:-</u>

1. touch
2. cat

3. vi

For creating file:- #touch file.txt

Drawback of touch command:-

Using this command we cannot insert the text, we cannot modify the text and delete the text.

For creating a file with cat:-

```
#cat   <option>  <filename>
```

Options:-

1. > to create a file
2. < to view the content
3. >> to append the content

Creating a file:-

```
#cat   > linux
---------------------
----------------------
```

Ctrl + d ---for save and quit.

To view the content of the file:-

```
#cat  <   linux
```

To append the content of already existing text:-

```
#cat   >>  linux
```

For creating a single directory or folder:-

```
#mkdir   folder name
```

For creating a multiple directories:-

```
#mkdir    folder1    folder2
```

For changing the directory:-

```
#cd   directory name
```

```
#cd   <path>
```

1. Absolute path:- complete path
2. Relative path: - used only when the file or directory is in the current directory.

To change to previous directory: - #cd -

To change one level back: - #cd ..

To change two level back: - #cd ../..

To move to home directory: - #cd ~

<u>For copying & pasting the objects:-</u>

Syntax:-

```
#cp      <options>   <source>   <destination>
```

Options:

1. –r=recursive
2. –v=verbose
3. –f=forcefully

For copying a file: - #cp /root/install.log /opt

For copying a directory:- #cp -r(v or f) /root/unix /opt

For moving the objects:- (cut & paste)

Syntax:-

#mv <source> <destination>

#mv /root/unix /opt

For renaming the objects:-

Syntax:-

#mv <old name> <new name>

For deleting the objects:-

Syntax:-

#rm <options> < source>

Options:-

1. –r=recursive
2. –f=forcefully

For deleting a file:- #rm filename

For deleting a directory:- #rm -rf directory name

For deleting empty directory:-#rmdir directory name

To remove all files and folders in present directory:- #rm -rf *

<u>Editors:-</u>

There are two types of editors.

In text based:-

1. vi (visual editor)
2. vim

In graphical based:-

gedit

emac’s

<u>vi (visual editor):-</u>

vi editor was Introduced by “Bill joy” for performing a task like creating a file, modifying the content of a file and deleting the text of a existing file.

Levels of vi:-

1. Command mode
2. Insert mode
3. Execution mode

Command mode:-

This is the default mode of vi editor in which we can perform the operations like deleting of lines, copying of lines, pasting of lines, Redo and Undo.

Operations of command mode:-

1. dd = deletes a line
2. ndd= deletes ‘n’ lines
3. yy= copies a line
4. nyy= copies ‘n’ lines
5. p= put(pastes the deleted or copied text)
6. u= undo (you can undo 1000 times)
7. Ctrl + r = redo
8. Shift + g = moves the cursor to the last line of the file.
9. /<word to find>= finds a word (press n for text)
10. dw= to delete a word
11. yw=to copy a word

Insert mode:-

This is the second mode of vi editor in which we can perform the operations like inserting the text and editing the text of a existing file.

Execution mode:-

This is the last mode of vi editor in which we can perform the operation like saving a file or quitting a file without saving.

1. :q= quit without saving
2. :q!= quit forcefully with out saving.
3. :w= write(save)

4. :wq= save and quit forcefully

5. :se nu= sets line numbers

6. :se nonu= removes line numbers

7. :84= the cursor goes to line 84

8. :wn= to save & switch to next file

9. :rew= to switch to last file(without saving)

Manipulation commands:-

1. wc

2. grep

3. find

4. head & tail

5. man & info

To count no of lines, words & characters:- #wc   filename

To count no of lines:-#wc –l filename

To count no of words:-# wc –w filename

To count no of characters:-# wc –c filename

To search a word in a file:- #grep   <word> <filename>

To search a word in a 2 files:-

#grep <word>   <filename1> <filename2>

To find a particular file:- #find <location> <parameter> <filename>

Example:- #find / -name hosts

To view top 10 lines in a file:#head filename

To view bottom10 lines in a file:-#tail filename

To view top n lines in a file:-# head –n filename

To view bottom n lines in a file:-# tail –n filename

By default head & tail shows 10 lines.

To get the manual page of mkdir:-#man mkdir

To get the information of mkdir:-#info mkdir

Bash:- (Bourne again shell)

Features of bash shell:-

1. Command history
2. Command aliasing
3. Command completion

To check the available shells:-#cat /etc/shells

To check the present working shell:- #echo $SHELL

To check available aliases:- #alias

To set a alias:-#alias c=clear

To remove a alias:-#unalias c

To check the history of executed commands:- #history

To recall a command from history:- #!464 ---- (464 is a line number)

User:-

Technically the individual who is going to use the available hardware and software resources is nothing but called a user.

System users:-

This type of accounts is generally created by operating system.

The UID's and GID's for this type of users and groups will be ranging from "0 to 499".

Normal users:-

These types of accounts are created by the super user (root account).

The UID's and GID's for this type of users and groups will be ranging in between "500 to 60,000".

Default properties given to a normal user:-

1. UID
2. GID
3. Mail account-- /var/spool/mail
4. Home directory-- /home
5. Shell—by default bash is used.

#vi   /etc/passwd

Username:x:UID:GID:comment:/home/username:/bin/bash

X=mask password

Example:-Vishnu:x:501:501::/home/Vishnu:/bin/bash

#vi /etc/shadow

Username:encrypted password:no of days since 1970:min life of password:max life of password:warning period:::

Example:- Vishnu:$jhdsf:15241:0:99999:7:::

To create a user account:- #useradd username

To assign the password for a user:-#passwd username

Give password for the user.

To login in user account:-#gdmflexiserver --xnest

Or #su – username

To check the user status:-# grep username /etc/passwd

To change the default shell:-# useradd –s /bin/ksh raj

To change the default home directory:- #useradd -d /opt/sunny sunny

To provide a comment to a user:-#useradd –c manager ram

To change an UID to a user:-#useradd –u 555 user5

Put usermod instead of useradd when the user is already exists.

For deleting a user account recursively:-#userdel -r user5

For modifying user properties:-

Syntax:-

#usermod <options> <existing username>

Options:-

1. –L----to lock an account

2. –U----to unlock an account

3. –l-----to change login name

To lock an user account:- #usermod -L username

To unlock an user account:- #usermod -U username

To change the login name:- #usermod -l <new name> <old name>

To check the password status:- #passwd –S username

For managing user accounts in graphical mode:-

#system-config-users

To see complete information of the particular user

#finger username

```
finger vivek
```

Output:

```
Login: vivek                            Name: Vivek Gite
Directory: /iscsi/user/vivek                Shell: /bin/bash
Last login Thu Sep 13 07:58 2007 (IST) on pts/1 from 10.16.15.2
No mail.
No Plan.
```

Shage username (for updateing the password related like expiry etc)

Group administration:-

Group:-

Group is nothing but collection of users basically used for assigning common setup permissions.

Types of groups:-

1. Primary

2. Secondary

Tools:-

1. group add

2. group del

3. groupmod

4. gpasswd

Database files:-

```
#vi   /etc/group
```

groupname:x:gid:members of groups

example: color:x:500:red,yellow

x is the mask password.

```
#vi   /etc/gshadow
```

Groupname:encrypted password:group admin information:members of a group

color:$jhds:black:red,yellow

To create a group account:-

```
#groupadd  color
```

To create a password:-

```
#gpasswd  color
```

For adding/removing users into a group:-

Syntax:-

#gpasswd <options> <existing user name> <existing group name>

Options:-

1. –a=to add a single user
2. –d=to delete a user
3. –M=to add multiple users
4. –A=to make a user as a group admin

For adding a single user:- #gpasswd -a red color

For removing a user:-#gpasswd -d red color

For adding multiple users:- #gpasswd -M red,yellow,green color

For assigning the group admin privilege:- #gpasswd -A black color

To delete the group admin privilege:- #gpasswd -A " " color

For deleting a group account:- #groupdel color

For modifying the group Id:-#groupmod -g 999 sales

For changing the group name:-#groupmod –n newname oldname

<u>Permission:-</u>

Permission is a process used in the system administration for granting the access or denying the access for users and groups on the particular resource.

Types of permissions:-

1. Basic file permission
2. ACL

To list the properties of a file:-#ls   -l   filename

To list the properties of a directory:-# ls   -ld   directory name

Basic file and folderpermission:-

-	rw-	r--	r--
d	rwx	r-x	r-x
types of object	owner	group	others

Access mode	**Access level**
Read(r) -4	owner (u)
Write(w)-2	group(g)
Execute(x)-1	others(o)

Tools:

1. chown
2. chgrp
3. chmod

create a file:- #touch filename

To apply full permissions for group:- #chmod g+rw   /filename

To apply full permissions for others:- #chmod o+rw   /filename

For removing permissions from other & group:-

#chmod   og-rw   /filename

To apply full permission for owner, group and others:-

#chmod a=rw /filename

Numeric values:-

1. execution[x] - 1
2. write[w]   - 2
3. execution + write[x+w] - 3
4. read[r] - 4
5. read + execution[r+x] – 5
6. read + write [r+w] - 6
7. read + write + execute[r+w+x] – 7

To view the statistics of a file:- #stat   /filename

For modifying the permissions for others: - #chmod   6 /filename

For modifying the permissions for all (full permission):-

#chmod 666 /filename

For changing the ownership of a file:- #chown   raju   /filename

For changing the group ownership of the file:-#chgrp   sales   /filename

Drawback of Basic file permission:-

Using basic file permission we can apply permissions globally for one level individually.

ACL (Access Control List):-

It is a mechanism used in the OS environment for providing different set of permission, for different users and groups on a common resource.

Implementation steps on ACL:-

Create the resource and users:-

```
#touch       /filename

#useradd u1 ; useradd u2
```

Applying the ACL permissions:

```
#setfacl   -m   u:u1: ---  /filename

#setfacl   -m   u:u2:r--   /filename

#setfacl   -m   o:r--       /filename
```

To check the ACL:-

```
#getfacl    /filename
```

For removing the ACL on particular user:

```
#setfacl    -x  u:u1   /filename
```

Switch with user account and check the access:-

```
#su  -  u1

#cat   /filename
```

Partitions:-

Partition is nothing but a boundary specified within a storage device, to utilize the available disk space.

Tools of partition:-

1. fdisk (max: 15 partitions)—post installation
2. parted(max : 63 partitions)—post installation

3. Disk druid(pre installation)

For creating a partition in existing OS:-

Syntax:

#fdisk   <device name>

To get the device name and to list the number of parttions:- #fdisk -l

fdisk prompt:

m – Help

d – Delete a partition

n – Adding a new partition

p – Print the partition table

q – To quit without saving

w – To quit with saving

#fdisk /dev/hda

[fdisk prompt]:n

[first cylinder]: press enter

[last cylinder]: +2GB

[fdisk prompt]:w

To update the partition table:-#partprobe   /dev/hda

<u>Formatting:-</u>

Formatting is a process used for specifying a disk base file system over a storage device.

Types of file system:

1. ext2
2. ext3 – latest in RHEL
3. ext4 – latest in fedora

Tools:-

1. mkfs.ext2
2. mkfs.ext3

For formatting a partition with ext2 file system:-

```
#mkfs   -t  ext2   /dev/hda8
```

or

```
#mkfs .ext2    /dev/hda8
```

For formatting a partition with ext3 file system:-

```
#mkfs   -t  ext3   /dev/hda8
```

or

```
#mkfs .ext3    /dev/hda8
```

Mounting:-

Mounting is a mechanism used for mapping or creating a logical link between a storage device to a directory.

To check the mounted partitions:- #mount

To mount a partition:-

1. create a directory:-# mkdir   /directoryname

2. to mount the partition:-#mount   /dev/hda   /directory name

For unmounting the partition:- #umount /dev/hda8

For rebooting the system:- #reboot

For mounting a partition permanently:-#vi /etc/fstab

Type a new line:-

/dev/hda8   /directory name ext3   defaults   0   0

:wq

To update mount table:- #mount -a

Label:-

Label is a process used for assigning individual identification for a particular partition.

To check the label of a partition:-#e2label /dev/hda1

To assign a label:-#e2label   /dev/hda8   songs

To remove a label:-#e2label   /dev/hda8 “ ”

For mounting a partition with label:-

#mount LABEL=songs   /directory name

For checking the mount labels:-#mount   -l

Swap:-

It is a virtual file system basically used for improving the system performance by dedicating a part of hard disk to act as a virtual RAM.

Creating a swap partition:-

Create a partition:- #fdisk /dev/hda

Update the partition table:-#partprobe /dev/hda

To format a partition with swap file system:-#mkswap /dev/hda9

To enable a swap partition:-#swapon /dev/hda9

To check already existing swap memory:-#swapon -s

<u>LVM (Logical Volume Manager):-</u>

Logical volume manager is a mechanism used in the OS environment for having a flexibility of increasing or decreasing the partition sizes of an existing drive.

Volumes of LVM:

1. physical volumes
2. volume group
3. logical volume

Installation steps of LVM after OS installation:-

Step no 1:-

Create the partition:- #fdisk /dev/hda

```
                     [fdisk prompt]:n
                    [first cylinder]: press enter
                    [last cylinder]: +10GB
```

[fdisk prompt]:w

Create the partition:- #fdisk /dev/hda

[fdisk prompt]:n

[first cylinder]: press enter

[last cylinder]: +10GB

[fdisk prompt]:w

To update the partition table:-#partprobe   /dev/hda

Provide LVM support:- #pvcreate   /dev/hda10

#pvcreate   /dev/hda11

To check the physical volume:-#pvdisplay

Step no 2:-

Create the volume group:-#vgcreate zoom /dev/hda10   /dev/hda11

To check the volume group:- #vgdisplay

Create the logical volume:-#lvcreate -L +1GB –n /dev/zoom/linux

Step no 3:-

Format the logical volume:-#mkfs.ext3   /dev/zoom/linux

For mounting the logical volume:-

#mkdir   /data

#mount   /dev/zoom/linux   /data

Step no 4:- resizing

For extending the logical volume:-

```
#lvresize  -L   +1GB  -n /dev/zoom/linux

                  Or

#lvextend   -L +1GB   /dev/zoom/linux

#resize2fs   /dev/zoom/linux
```

For reducing the logical volume:-

```
#lvresize  -L   -500MB  -n /dev/zoom/linux

                  Or

#lvreduce   -L -500MB   /dev/zoom/linux

#resize2fs   /dev/zoom/linux
```

For checking the logical size:-#lvdisplay /dev/zoom/linux

<u>Quotas:-</u>

A quota is a mechanism used for restricting the disk consumption by a particular user or a group of users. It is a method of allocating specific size of hard disk for a particular user.

<u>Levels of quota's:-</u>

1. user level quota
2. group level quota

<u>Methods of quota's:-</u>

1. Inode
2. Block

<u>Tools:-</u>

1. quotacheck
2. quotaon
3. quotaoff
4. edquota

<u>Implementation of quota's:-</u>

Step no 1:-

Create the partition:- #fdisk /dev/hda

```
                                  [fdisk prompt]:n
                                 [first cylinder]: press enter
                                 [last cylinder]: +2GB
                                 [fdisk prompt]:w
```

To update the partition table:-#partprobe   /dev/hda

Format the patition:#mkfs.ext3   /dev/hda12

Step no 2:-

#mkdir   /quota

Mount the partition with quota's support:-

#mount   -o usrquota,grpquota   /dev/hda12   /quota

Provide full permission:- #chmod 777   /quota

Step no 3:-

For scanning the partition:#quotacheck -cugv   /dev/hda12

Enabling the quota’s:#quotaon /dev/hda12

To check whether it is ON or OFF:#quotaon   /dev/hda12   -p

Edit the quota’s file:- #edquota   -u rajiv

```
Filesystem  blocks  soft  hard   inodes  soft   hard
/dev/hda12     0           0    0           0       2        4
```

:wq

For verification:- switch with a user account created:-# su - rajiv

Enter into the mount point:-#cd   /quota

Create the files(upto hard value):- touch {1..4}.txt

Block method:-

To check the block size of a partition:-#blockdev --getbsz /dev/hda12

To change the block size of a partition:- #mkfs.ext3 -b 2048 /dev/hda12

For applying quotas in block method:-

Create a user account:- #useradd sandy

Edit the quota’s file:- #edquota   -u sandy

```
Filesystem  blocks   soft    hard  inodes  soft  hard
/dev/hda12         0         2         4       0           0      0
```

:wq

Verify by creating a files or directories up to 4 blocks:-

#su - sandy

#touch sandy{1..5}

```
#mkdir   navin
```

For applying quotas for existing partition:-

```
#mount   -o  remount,usrquota     /dev/hda3    /var
```

To get users quotas:-#repquota   -a

Run levels:-

init 0 ----- shutdown or halt

init 1 ----- safe mode or single user mode

init 2 ----- multiuser text mode without nfs support

init 3 ---- multiuser text mode with support for all services

init 4 ---- unused

init 5 ---- GUI & multiuser mode with support for all services

init 6 ---- reboot or restart

To check the default run level:- #runlevel

For providing new password for super user:-

- Reboot the machine to boot the machine in single user mode.
- Press ‘ESC’ key at booting time to stop the boot process.
- Press ‘e’ key to edit the title.
- Select the second line ‘kernel’ & press ‘e’ key & provide single space and type ‘1’ or ‘S’ which indicates single user mode.
- Press ‘b’ to boot in single user mode.

- Sh-3.1# passwd root

    Give new password

  Sh-3.1#init 5 --- to go to graphical screen

For assigning a password to a boot loader:-

#grub-md5-crypt

Password:

Retype password:

$nbdsks7839084rjdsjhksd ----- encrypted password. Copy this encrypted password.

Edit the boot loader configuration:

#vi /boot/grub/grub.conf

Under 13th line hidden menu

14 password --md5 paste the encrypted password.

:wq

<u>Backup:-</u>

It is a method used for preventing the data loss in a system. It is a method used for maintaining a Xerox or duplicate copy of required data.

Methods of backup:-

1. Local backup
2. External backup
3. Network backup

Tools of backup:-

1. **Local backup:**

    a. cp

    b. tar

    c. cpio

2. **External backup:**

    a. dump

    b. kb III

    c. nero

3. **Network backup:**

    a. scp

    b. rsync

<u>For taking backup with tar:-</u>

<u>Syntax:</u>

#tar <options> <backup file name> <source>

Options:-

1. –c **---** create a backup file
2. –v --- verbose
3. –f **---** forcefully

4. –x --- to extract the backup

Create the source:- #mkdir /linux

```
 #touch    /linux/sample.txt{1..10}
```

For taking the backup:-#tar -cvf /opt/backup.tar /linux

For checking the backup:-

```
#rm  -rf  /linux
```

For extracting the backup:-#tar -xvf /opt/backup.tar

To restore the backup in required location:-

```
#tar  -xvf  /opt/backup.tar  -C  /var
```

For taking backup with cpio:-

Create some your own files:- #touch file{1..10}.txt

Syntax:-

```
#ls   i* | cpio <options>  >  <backuppath & file name>
```

Options:-

o – output

i – input

v – verbose

f – forcefully

```
#ls   file* | cpio –ovf  > /opt/file.cpio
```

For checking the backup:-

```
#rm   -rf  file*
```

For restoring the backup:-

```
#cpio   -ivf  <   /opt/file.cpio
```

<u>For taking backup with dump:-</u>

Syntax:-

```
#dump  <options>  <back up file or raw partition or tape drive> <source>
```

Options:

0-9 – level of backup

u – update

f --forcefully

Level of backup:-

0 – full backup

1-8 – incremental backup

9 – differential backup

Full backup:-

Using this level of backup we can take the complete file systems image in a backup file or special device (tape drive).

Incremental backup:-

Using this level of backup we can take the backup of only newly generated data.

Differential backup:-

Differential backup is also a type of full backup in which we are going to take a full backup of all incremental backups.

For recovering the backup with restore:-

Syntax:-

```
#restore  <options>  <backup filename>
```

Options:

1. –r – recursive
2. –f – forcefully

For taking full backup:- #dump -0uf   /opt/full.dump   /dev/hda7

For taking incremental backup:- #dump -1uf /opt/first.dump   /dev/hda7

Up to 8 we have to take incremental backup.

For taking differential backup:- #dump -9uf /opt/diff.dump /dev/hda7

For checking the backups:-

```
#cd  /home
#rm  -rf  *
```

For restoring the backup:-

```
#restore  -rf  /opt/full.dump
#restore  -rf  /opt/first.dump
#restore  -rf  /opt/diff.dump
```

Compression tools:-

1. gzip[.gz]

2. bzip2[.bz2]

Decompression tools:-

1. gunzip
2. bunzip2

syntax:

```
#gzip filename

#gunzip filename with extension

#bzip2 filename

#bunzip2 filename with extension
```

To check the IP address:-

```
#ifconfig   [interface configuration]
```

To assign IP address:-[temporarily]

```
#ifconfig <device name>  <IP address>

#ifconfig eth0  192.168.0.1
```

To assign a permanent address:-

```
#netconfig
```

To update the service:-

```
#service network restart
```

To check the LAN connectivity:-

```
#mii-tool
```

To disable the LAN card temporarily:-

```
#ifdown eth0
```

To enable the LAN card:-

```
#ifup eth0
```

To check the database information of IP:-

```
#cd  /etc/sysconfig/network-scripts
#cat ifcfg-eth0
```

Package management:-

Package management is a process used in Linux platform for installing, upgrading, uninstalling and querying a package.

Tools:-

1. rpm
2. yum

rpm:-

Red hat Packet Management is a default Packet Management tool up to RHEL4 which is used for installing or uninstalling an application.

For installing or uninstalling a rpm:-

Syntax:-

```
#rpm  <options>  <package name>
```

Options:

1. –i – install

2. –v – verbose
3. –h – hash
4. –e – to erase a package

To install or uninstall a package forcefully:-

#rpm <options> <package name> --force

To install or uninstall a package without dependencies:-

#rpm <options> <package name> --nodeps

For installing the application in stand alone method:-

First mount the media:-#mount   /dev/cdrom   /mnt

Enter to location of rpm's:-#cd   /mnt/Server

For installing the package forcefully:-#rpm -ivh squid-* --force

For uninstalling the package:-#rpm -e squid

For removing the required package without supporting:-

#rpm -e squid --nodeps

For querying a package:-

Syntax:

#rpm   <options> <package>

Options:

1. –q – to query a single package
2. –qa – to query all package
3. –qi – to query information

4. –qc – to query all configuration
5. –qd – to query all documentation

To query a single package:- #rpm –q squid

To query all installed package:- #rpm –qa squid

To query the information package:- #rpm –qi squid

To query documentation:- #rpm –qd squid

To query configuration:- #rpm –qc squid

For installing the package with Network method with NFS:-

To check the shared content:-#showmount -e 192.168.0.X

For creating link to server:-#mount 192.168.0.X:/var/ftp/pub /mnt

For installing the package:-#cd /mnt/Server

```
                  #rpm –ivh vsftpd*  --force
```

For installing a package using FTP method:-

#rpm -ivh ftp://192.168.0.x/pub/Server/nfs* --force

Yum:- (Yellowdog Updates Modifier)

yum is a interactive package installation tool newly added in RHEL5. Using yum we can install or uninstall a package with the user's confirmation.

For installing/uninstalling a package:-

Syntax:-

```
#yum  <options>  <package>
```

Options:

1.install

2. remove

3. list

4. info

For installing a package using yum:-

Edit the configuration file of yum:-

```
#vi  /etc/yum.repos.d/rhel-debuginfo.repo

        Line 3 baseurl=ftp://192.168.0.x/pub/Server

                4 enabled=1

        :wq
```

For installing a package:-#yum install sendmail*

For removing a package:-#yum remove sendmail*

For checking the package:-#yum list sendmail*

For installing or uninstalling a package in graphical mode:-

```
#pirut
```

How to create local repository for yum

Recently thinking to install some package on my office PC which has Fedora 12 installed as desktop OS, found that it will be taking a hell lot of time to download due to internet connection inconsistency. A thought came to mind, it will be good if I can create a local repository for yum where I will copy OS in a directory. So just copied Fedora 12 DVD in a directory and created a local repository for yum following steps.

We need to install "createrepo" if not installed.

```
#yum install createrepo
```

Then we have to create metadata for the packages we copied in directory. For example say we create directory /fedora to copy all packages we need to run following command.

```
#createrepo /fedora
```

This will take a little while to create metadata. As this command finishes the local repository is ready.

Now, we have to tell yum to check this local repository. We know that yum related files can be found at /etc/yum.repo.d/. Just create a file with name "local.repo" and add below text into it.

```
[localrepo]
name=Fedora Core $releasever - Local Repo
baseurl=file:///fedora/
enabled=1
gpgcheck=0
#gpgkey=file:///path/to/you/RPM-GPG-KEY
```

In base url we have used file:// which shows that the url to refer is a local location.

That is it. We have created a local repository for yum.

Another method

Another method of Yum local repository for Centos and Fedora

SERVER

1. You should have following rpm packages installed:
   i) httpd
   ii) yum,yum-updatesd
   iii) createrepo

2. Copy all the rpm packages from media to local hard-drive

under newly created directory.
For e.g # /home/yum/
Create directory for diff Distro

3. Then give following command:
   createrepo <your_dipath_to_local_repo>

4. Start apache service
5. create custom dir under apache docroot
   For e.g # /var/www/html/yum

6. mount the directory (where your repos are stores) to bind to
   custom dir under apache docroot
   For e.g # mount --bind /home/yum /var/www/html/yum

CLIENT

1. edit Base repo(or/and related files if exists) file under /etc/yum.repos.d
2. Under base section comment mirrorlist and uncomment baseurl
3. replace your baseurl and gpgkey as http://IP_of_localyum_server
4. In remaining sections add following line:
   enabled=0

For e.g

```
      [base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os
baseurl=http://1.1.2.2/yum/{Centos/Fedora}
gpgcheck=0
```

Note : just create dir in yum directory then create sub dir as base to keep all rpms in base dir..
then run createrepo with the path of the dir

One more method

hanks to Balkrishna for suggesting more more way to do it. Posting his mail as it is on behalf on him.

1) first dump ur linux DVD to /var/ftp/pub location.
2) install vsftpd rpm. rpm -ivh <package>
3) install createrepo package which is there in /var/ftp/pub/Server

creating repository:

4) createrepo -g /var/ftp/pub/Server/repodata/comps-xxxx.xml /var/ftp/pub/Server

5) it takes some time to create repository

6) if it says remove .olddata remove that.

7)#yum clean all

editing yum configuration:

vim /etc/yum.repos.d/rhel-debuginfo.repo

make sure u have these lines in ur configuration.

```
[core]
name=Red Hat Enterprise Linux $releasever - $basearch - Debug
baseurl=ftp://10.193.185.98/pub/Server
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

save it.

```
#yum clean all
#service vsftpd restart.
#chkconfig --level 345 vsftpd on
```

that's it ur done.

try installl some package.

```
#yum install iptraf* -y
```

NETWORK ADMINISTRATION CONCEPTS

File server:-

Using file servers mechanism we can share the resources from one centralized location to all the clients connected in a same network.

Types of File servers:-

1. NFS Server [Network File System]
2. FTP Server [File Transfer Protocol]
3. Samba [Smb] Server [Server Message block]

1. NFS Server: [Network File System]

NFS service is a platform dependant service used for sharing the resources only between UNIX and LINUX clients.

Drawbacks for NFS:

NFS uses a session protocol called RPC [Remote Procedure Call] which in turn generates a lot of network traffic by providing individual connections for every client.

Requirements:-

Packages:-

1. portmap*

2. nfs*

Port numbers:-

1. portmap-111

2. nfs-2049

Configuration files:-

vi /etc/exports

Services:-

1. portmap
2. **nfs**

Installation steps for NFS Server:-

Step No 1:- Provide the hostname

```
# hostname nfs.zoom.com
```

Make the hostname permanent:-

```
#vi      /etc/sysconfig/network
```

Line 3: HOSTNAME=nfs.zoom.com

```
:wq
```

Provide the IP address:-

```
#netconfig
```

Give IP address.

Map the IP with host name:-

```
#vi   /etc/hosts
192.168.0.x    nfs.zoom.com    nfs
:wq
```

Update the service:

```
#service network restart
```

Step no 2:- Install the packages.

```
#yum install nfs* portmap*
```

Create the shared resource:-

```
#mkdir   /redhat

#touch    /redhat/{1..10}.rpm
```

- Edit the configuration file:-

```
#vi    /etc/exports

/redhat     *(rw)

:wq
```

Step no 3 :- Update the services

```
#service portmap restart

#service nfs restart
```

Client side configuration:-

```
#showmount  -e 192.168.0.x

#mount   192.168.0.x:/redhat      /opt

#cd    /opt

#ls
```

Auto mounting:-

It is a mechanism used in the NFS client for mounting the shared content of NFS server automatically or on the request.

Implementation of Auto mounting at client side:-

- Edit the first mapper file:-

```
#vim   /etc/auto.master
```

Erase all the lines except this line.

```
1) +auto.master
2) /-        /etc/auto.misc   --timeout=10
:wq
```

- Edit the second mapper file:-

```
#vi   /etc/auto.misc
```

Remove all the lines.

```
Type 1) /share   -fstype=nfs      192.168.0.x:/redhat
:wq
```

Update the service:

```
#service autofs restart
```

Note: x means the server's IP.

2. FTP Server:- [File Transfer Protocol]

FTP is a one of the oldest TCP/IP protocol used for transferring the data from one machine to another machine in the form of uploading and downloading.

Methods of FTP server:-

1. Standard mode (needs authentication)

2. Anonymous mode (no need of authentication) any body can access.

Requirements:-

Package:-

vsftpd*

Port numbers:-

For data transfer-20

Client connection-21

Configuration file:-

```
vi  /etc/vsftpd/vsftpd.conf
```

Data base directory:-

/var/ftp

Service:-

vsftpd

Debugging tool:-

vsftpd

Implementation steps for FTP server:-

Step no 1:- Provide the hostname and IP.

Step no 2:- Install the package

```
#yum install vsftpd*
```

- Edit the configuration file:

```
#Vi  /etc/vsftpd/vsftpd.conf

Line no 12 anonymous_enable = yes
                              Or no for standard mode
          15 local_enable = yes
          27 anon_upload_enable=yes

:wq!
```

Step no 3:- create the shared resource.

```
#cd     /var/ftp/pub

#touch file{1..10}
```

Update the service:

```
#service vsftpd restart
```

Client side configuration:-

```
#ftp 192.168.0.x

Username:ftp

Passwd: press enter key

ftp>cd pub

ftp> get file1

ftp>bye
```

For uploading permission:-

In server side:-

Create the folder in server for uploading.

```
#mkdir   -p /var/ftp/upload
```

```
#chmod 777 /var/ftp/upload
```

Update the service:

```
#service vsftpd restart
```

Client side configuration:-

```
#ftp 192.168.0.x
```

Username:ftp

Passwd: press enter key

```
ftp>cd upload
```

```
ftp> put filename
```

```
ftp>bye
```

3. **SAMBA Server:-** [Server Message block]

   Server Message Block is an open source protocol used for performing file sharing between different platforms of operating system. SMB was introduced by Andrew Tridgell which uses Common Internet File System [CIFS].

Features:-

1. File sharing
2. Device sharing
3. PDC
4. BDC

Requirements:-

Packages:-

Samba*

Port numbers:-

137

138

139

Configuration file:-

vi   /etc/samba/smb.conf

Service:-

smb

Debugging tools:-

1. testparm
2. findsmb

Implementation steps for samba server:-

Step no 1:- Provide the hostname and IP.

Step no 2:- Install the package.

```
#yum   install   samba*
```

- Edit the configuration file:

```
#vi      /etc/samba/smb.conf
```

Go to the line number 265 and make the commented lines to enable.

```
[share]
Comment  =  this is samba shared drive
Path = /samba
Validusers = pavan ram
Writable = yes
Printable = no
Workinggroup = sales marketing
:wq
```

- Create the shared resources and users:

```
#mkdir  /samba
#touch    /samba/{1..10}.tar
#chmod 777 /samba
```

<u>Step no3:-</u>

Create the users

```
#useradd ram
#useradd pavan
```

For providing universal password:

```
#smbpasswd -a ram
#smbpasswd -a pavan
```

Update the service:

```
#service smb restart
```

Client side configuration:-

For linux as a client:

```
#smbclient   //192.168.0.x:/share  -U   ram
```

For windows as a client:

```
#rdesktop  192.168.0.xx  -U username –p passwd &
```

Now you will get a remote windows desktop and do the below work.

Mycomputer –Mapdrive-assign letter-IP-My network places-view work group computers-Microsoft windows network-my group-samba server.

For accessing windows shared folder in linux system:

```
#nautilus    --browser   smb://<windows IP>
```

4. DHCP Server:- [Dynamic Host Configuration Protocol]

DHCP is a type of network service used for assigning IP addresses for all the clients connected in a same network using dynamic method (automatic).

The communication between DHCP server and DHCP client is also called as Handshaking Process or DORA Process.

Requirements:-

Packages:-

dhcp*

Port numbers:-

67

68

Configuration file:-

```
vi    /etc/dhcpd.conf
```

Service:

dhcpd

Debugging tool:-

dhcpd

Implementation steps for DHCP server:-

Step no 1:- Provide the hostname and IP.

Step no 2:- Install the package.

```
#yum install dhcp*
```

Copy the sample file:

```
#cd  /usr/share/doc/dhcp-3.0.5/
#cp     dhcpd.conf.sample          /etc/dhcpd.conf
```

- Edit the configuration file:

```
#vi     /etc/dhcpd.conf
```

```
Line no 21:   range dynamic-bootp 192.168.0.1   192.168.0.254;
          22:    default-lease-time 21600;
          23:   max-lease-time 43200;
```

```
:wq!
```

Update the service:

```
#service dhcpd restart
```

Client side configuration:-

```
#dhclient –r [for releasing the past IP]
#dhclient
```

Reservation:-

Reservation is a mechanism used in the DHCP server for assigning a static address to the client from a DHCP server.

To check the connectivity:

```
#ping 192.168.0.10 (client's IP)
#arp –a
```

Mac address will display

Copy the Mac address you want.

- Edit the configuration file:

```
#vi   /etc/dhcpd.conf
```

Edit the 26 to 30 lines

```
host ns{
            Next server name flat name or FQDN
           Hardware Ethernet-- paste the copied mac address;
```

```
            Fixed address - give your desired IP;
 }
:wq!
```

Update the service:

```
#service dhcpd restart
```

5. **DNS Server:-**

   Domain Naming System is one of the important network service used for providing naming resolution in a network.

   DNS is a responsible for converting given names to a particular IP address and vice versa.

Zone of DNS:-

1. Forward Look up zone. [converting Names to IP]
2. Reverse Look up zone. [converting IP to Names]

Resource records:-

1. SOA – Start Of Authority
2. NS – Naming Server
3. A – Address
4. PTR – Pointer
5. MX – Mail Exchange

6. CNAME

Requirements:-

Packages:-

bind*

caching*

Port Number:-

Named - 53

Configuration files:-

1. vi /etc/named.rfc1912.zones
2. vi /etc/named.caching-nameserver.conf

Update service:-

named

Debugging Tools:-

1. named-checkzone /etc/named.rfc1912.zones
2. named-checkconf /etc/named.caching-nameserver.conf

Data base Directory:-

cd /var/named/chroot/var/named

1. vi localhost.zone
2. vi named.local

Implementation steps for DNS Server:-

Step no 1:- Provide the hostname and IP.

<u>Step no 2:-</u> Install the packages.

```
#yum  install    bind*   caching*
```

- Edit the first configuration file:

```
#vi   /etc/named.rfc1912.zones
Line 21 zone “zoom.com” IN{
                        type master;
                 file “localhost.zone”;
};
:wq
```

- Edit the second configuration file:

```
#vi   /etc/named.caching-nameserver.conf
Line 15   listen-on port 53 {192.168.0.x ;};
         23  allow-query {any ; };
         32 match-clients {any ;};
:wq
```

<u>Step no 3:-</u>

Create the zone data base file

```
#cd   /var/named/chroot/var/named
```

```
#vi    localhost.zone

Line 2  @    In SOA dns.zoom.com.    root(

       9           In NS dns.zoom.com.

      10   dns  In A 192.168.0.x

:wq
```

Update the service:

```
#service named restart
```

Client side configuration:-

Provide the DNS address:

```
#vi   /etc/resolv.conf

Line 1 nameserver    192.168.0.x

:wq
```

Update the service:

```
#service network restart

#dig   dns.zoom.com
```

6. WEB Server:-

Web service is basically used for sharing the information of a particular organization in the form of website.

Applications of web server:-

1. TUX

2. APACHE

Method of website hosting:-

1. Name based
2. IP based
3. Port based

Requirements:-

Package:-

httpd*

Port numbers:-

http – 80

https - 443

Configuration files:-

```
 vi  /etc/httpd/conf/httpd.conf
```

Data base directory:-

/var/www/html

Update service:-

httpd

Debugging tool:-

```
httpd -S
```

Implementation steps for web server:-

Step no 1:- Provide the hostname and IP.

Step no 2:- configure the DNS server with FLZ only.

Step no 3:- Install the packages.

```
#yum install http*
```

- Edit the configuration file:

```
  # vi    /etc/httpd/conf/httpd.conf
```

```
Line 250  ServerAdmin     root@zoom.com
     264   ServerName       www.zoom.com:80
     280   DocumentRoot   "/var/www/html"
     390   DirectoryIndex    zoom.html
:wq!
```

- In DNS server:

```
#cd /var/named/chroot/var/named
# vi   localhost.zone
```

At last type

```
Web     In   A   192.168.0.webserver's IP
www  In CNAME web
:wq!
```

Update the service:

```
#service named restart
```

Step no 4:- In web server

Create the web page.

```
# cd   /var/www/html
        # vi   zoom.html
        Write the your own data.
        :wq
```

Update the service:

```
#service httpd restart
```

Client side configuration:-

Provide the DNS address:

```
#vi   /etc/resolv.conf
Line 1 nameserver    192.168.0.x
:wq
#service network restart
```

For accessing the web page:

```
#firefox www.zoom.com &
```

Implementing authentication for a website:-

- Edit the configuration file:

```
#vi   /etc/httpd/conf/httpd.conf
```

Go to the last line

```
<Directory  "/var/www/html">
AuthName  zoom.com
AuthUserFile  /etc/httpd/passwd
```

```
AuthType     basic

Require      valid-user

</Directory>

:wq
```

Create the valid user:

```
#useradd user1
```

Provide the htpassword for users:

```
#htpasswd   -c /etc/httpd/passwd user1
```

Update the service:

```
#service httpd restart
```

7. Virtual Web Hosting:-

Apache can serve multiple sites easily known as ‘Virtual Hosting’.

Method of website hosting:-

1. Name based
2. IP based
3. Port based

In DNS Server:-

```
#vi   /etc/named.rfc1912.zones

        Line 21 zone “zoom.com” IN{

                                type master;
```

```
                    file “localhost.zone”;
        };
```

Add new lines for new web.

```
        zone “google.com” IN{
                              type master;
                    file “google”;
        };
:wq
```

```
        #vi   /etc/named.caching-nameserver.conf


        Line 15   listen-on port 53 {192.168.0.x ;};
                 23  allow-query {localhost; any ; };
                32 match-clients {localhost; any ;};
        :wq
#cd     /var/named/chroot/var/named
#cp   -p localhost.zone google
#vi    google
Line 2  @    In SOA dns.google.com.    root(
       9          In NS dns.google.com.
      10   dns  In A 192.168.0.x
```

```
            Web     In   A   192.168.0.webserver IP
            www  In CNAME web
:wq
```

Update the service:

```
#service named restart
```

In web server side:-

```
#vi   /etc/httpd/conf/httpd.conf
```

Go to line number 972 and remove the comment.

And go to line number 984

```
<virtualhost *:80>
          ServerAdmin     root@zoom.com
          ServerName       www.zoom.com
           DocumentRoot   "/var/www/html"
           DirectoryIndex    zoom.html
</virtualhost>
<virtualhost 192.168.0.x:80>      (--IP based)
               Or
Listen 5000
<virtualhost 192.168.0.x:5000>            (--Port based)
         ServerAdmin     root@google.com
```

```
            ServerName       www.google.com
             DocumentRoot   “/var/www/html”
             DirectoryIndex    google.html
</virtualhost>
:wq
```

Create the web page:

```
#cd   /var/www/html
#vi google.html
```

Write the data.

```
:wq
```

Update the service:

```
#service httpd restart
```

Client side configuration:-

Provide the DNS address:

```
#vi   /etc/resolv.conf
Line 1 nameserver    192.168.0.x
:wq
```

Update the service:

```
#service network restart
```

For accessing the web page:

```
#firefox www.google.com &
```

#firefox www.google.com:5000 &   (---Portbased)

8. PROXY Server :-

Proxy is a type of network service used for sharing the internet access coming from one connection to the entire clients connected in a LAN.

Features of Proxy server:-

1. Internet sharing
2. Caching of website
3. Firewall

Requirements:-

Packages:-

squid*

Port number:-

squid – 3128

Configuration file:-

Vi   /etc/squid/squid.conf

Data base directory:-

/var/spool/squid

Service:-

squid

Debugging tool:-

squid

Implementation steps for proxy server:-

Step no 1:- Provide the hostname and public & private IP.

Step no 2:- Install the package.

```
#yum install squid*
```

- Edit the configuration file:

  ```
  #vi   /etc/squid/squid.conf
  ```

  Go to line 2410

  ```
  acl    rule1 src 192.168.0.0/255.255.255.0

  http_access   allow rule1

  acl rule2  url_regex  www.yahoo.com

  http_access  deny rule2


  :wq
  ```

Update the service:

```
#service squid restart
```

Client side configuration:-

Open the web browser

```
#firefox &
```

In fire fox click edit-select preferences – advanced -network-click connection settings-select manual proxy and give the IP address & port number-click ok.

9. MAIL Server:-

Mail server is basically used for sending and receiving mails within the Intranet as well as Internet.

Agents of Mail server:-

1. MUA – Mail User Agent
2. MTA – Mail Transport agent
3. MDA – Mail Delivery Agent

MUA:-

Mail User Agent is mostly used in the client side for providing a connectivity to mail server to view, delete and composed the mail.

Example: For Unix and Linux

1. Mozilla
2. Evolution
3. Thunder bird

MTA:-

Technically a mail server is also called as Mail Transport Agent.

The job of MTA is to send and receive mails based on “to address”.

Example:

1. Send mail
2. Post fix
3. Qmail

MDA:-

Mail Delivery Agent is basically used for redirecting the mails stored in “MTA” to a specific user’s Inbox.

Example:

1. Procmail

Requirements:-

Packages:-

1. sendmail*

2. m4*

Port numbers:-

SMTP-25

POP-110

IMAP-143

Configuration files:-

vi /etc/mail/sendmail.cf

vi /etc/ mail/sendmail.mc

Data base directory:-

/var/spool/mail

<u>Update service:-</u>

sendmail

<u>Debugging tool:-</u>

sendmail

<u>Implementation steps for Mail server:-</u>

<u>Step no 1:-</u> Provide the hostname and IP.

<u>Step no 2:-</u> configure the dns server with forward lookup zone only.

```
#cd   /var/named/chroot/var/named
```

```
# vi   localhost.zone
```

```
Line 9            In MX 1   mail.zoom.com.

Line 12   mail     In   A   192.168.0.mailserver IP

:wq!
```

Update the service:

```
#service named restart
```

<u>Step no 3:-</u> Install the packages.

```
#yum   install sendmail*  m4*
```

- Edit the configuration file:

  #vi   /etc/mail/sendmail.mc

  Comment line 116 by adding dnl #

  Go to line 155   Local_domain(‘zoom.com’)dnl

```
                    160  MASQUERADE_AS(‘zoom.com’)dnl
                    164 FEATURE (masquerade_envelope )dnl
:wq
```

Compile the configuration:

```
#cd   /etc/mail
#m4 sendmail.mc > sendmail.cf
```

Step no 4:-

Create the user account

```
#useradd raj
#passwd raj
```

Update the service:

```
#service sendmail restart
#mail raj
Subject: mail server
This is mail server
.
Cc:
#su – raj
#mail
```

Step no 5:- To check the mail in graphical mode.

```
#yum install squirrelmail* dovecot* perl php curl http* cyrus*
```

Update the services:

```
#service httpd restart
#service dovecot restart
#service cyrus-imapd restart
```

Restart only either dovecot or cyrus-imapd service.

For accessing the mail server in web browser:

```
#firefox    mail.zoom.com/webmail &
```

10. NIS Server:

Network Information Service is basically used for providing centralize authentication for the clients.

NIS is a platform dependant service which can provide authentication to Linux or Unix client.

Requirement:-

Packages:-

1. yp*
2. nfs*
3. portmap*

Port numbers:-

nfs-2049

portmap-111

ypserv uses random port numbers above 1024.

Configuration files:-

```
 vi   /etc/exports
vi    /var/yp/Makefile
```

Update service:-

1. portmap
2. nfs
3. ypserv
4. yppasswdd

Step No 1:- Provide the hostname & nisdomain name

```
 # hostname nis.zoom.com
#nisdomainname central
```

Make the hostname permanent:-

```
#vi /etc/sysconfig/network
```

```
Line 3: HOSTNAME=nis.zoom.com
            NISDOMAINNAME=central
:wq
```

Provide the IP address:-

```
#netconfig
```

Give IP address.

Map the IP with host name:-

```
#vi /etc/hosts
```

```
192.168.0.x    nis.zoom.com    nis
:wq
#service network restart
```

Step no 2:- Install the package.

```
#yum install nfs* portmap* yp*
```

- Edit the NFS configuration file:-

```
#vi  /etc/exports
/home     *(rw)
:wq
```

- Edit the NFS configuration file:-

```
#vi    /var/yp/Makefile
Line 32 MINUID = 500
        33  MINGID = 500
109     all: passwd group mail \;
:wq
```

Step no 3:-

Create the user account

```
#useradd user1
#passwd user1
```

Update the user data base:

```
#cd     /var/yp
```

```
#service portmap  restart

#service ypserv restart

#make
```

Update the services:

```
#service portmap restart

#service nfs restart

#service ypserv restart

#service yppasswdd restart
```

Client side configuration:-

Provide NIS server authentication.

```
#authconfig-gtk

#mount  192.168.0.x:/home    /home

        Or

#vi   /etc/fstab

192.168.0.x:/home      /home    nfs  defaults   0  0

:wq
```

11. KICKSTART:-

Kick start is a network service used for installing or deploying the entire image of the operating system from one centralized location to all the clients.

Methods:-

1. Standalone
    a. cd
    b. dvd
2. Network
    a. nfs
    b. ftp
    c. http

Requirements:-

1. File sharing
2. DHCP server
3. Dump or Image of OS

Packages:-

1. vsftpd*
2. dhcp*
3. system-config-kickstart*

Port numbers:-

ftp – 20,21

dhcp – 67,68

Configuration files:-

```
vi  /etc/vsftpd/vsftpd.conf
```

vi /etc/dhcpd.conf

ks.cfg

Database directory:-

/var/ftp/pub

Services:-

vsftpd

dhcpd

Implementation steps for kick start service:-

Step no 1:- Provide the hostname and IP.

Step no 2:- Install the packages.

```
#yum   install   vsftpd*    dhcp*    *kickstart*
```

- Edit the configuration files of DHCP & VSFTPD.

  Copy the media of OS.

  For first CD (copy completely)

  ```
  #mount     /dev/cdrom    /mnt
  #cp  -rvf   /mnt/*     /var/ftp/pub
  ```

  For copying 2,3,4&5 CD’s

  ```
  #mount      /dev/cdrom      /mnt
  #cd    /mnt
  #cp  -rvf   *.rpm*     /var/ftp/pub/Server
  ```

Step no 3:-

create the kickstart configuration file.

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

Provide the execution permission

```
#chmod    +x  /var/ftp/pub/ks.cfg
```

Update the services:

```
#service vsftpd restart
#service dhcpd restart
```

Note:-

The client needs to be booted with the help of bootable media for the first time to perform the network installation.

Client side configuration:-

After putting the bootable CD or DVD.

```
boot: linux  ks=ftp://192.168.0.x/pub/ks.cfg
```

Drawback:-

Kick start service is a platform dependant service which can install same flavor of OS from Kick start server to a client.

RAID’S:-

RAID’S is a technology used for utilizing multiple hard drives as an array or Meta device.

Features:-

1. Better performance
2. Storage capability
3. Fault tolerance

RAID Levels:-

RAID0 (Striping without parity)

RAID1 (Disk mirroring)

RAID4 (Parity)

RAID5 (Striping with parity)

RAID1:-

Disk Mirroring

Requirements:-

Minimum   2 disks

Maximum   2 disks

Features:-

1. Write speed is slow & Read speed is fast.
2. 100% fault tolerance
3. 50% over head [wastage]

Implementation steps to RAID1:-

Step no 1:-

Create the two partitions.

```
#fdisk    /dev/hda
```

```
#partprobe   /dev/hda
```

Create the meta device.

```
#mdadm  -C  /dev/md0   -n2   /dev/hda{10,11}  -l1
```

Step no 2:-

Format the meta device.

```
#mkfs.ext3     /dev/md0
```

Mount the meta device

```
#mount     /dev/md0    /mnt
```

To check the properties

```
#mdadm    -D   /dev/md0
```

Step no 3:-

For verifying the RAID array

```
#mdadm  -S /dev/md0  ------ for stopping
```

Mount the drives

```
#mount    /dev/hda10  /opt
```

```
#mount    /dev/hda11 /mnt
```

- **SERVICES PORT NUMBERS**: (for quick reference)

1. HTTP (80)

2. HTTPS (443)

3. NFS (2049), PORTMAP (111)

4. FTP (20,21)

5. SAMBA (137, 138&139)

6. DHCP (67,68)

7. DNS (53)

8. SQUID [PROXY] (3128)

9. TELNET (23)

10. MAIL Server

a. SMTP (25)

b. POP (110)

c. IMAP (143)

11. NIS

α. NFS (2049)

β. PORTMAP (111)

χ. YPSERV (Random port numbers above 1024)

12. KICKSTART

a. FTP (20,21)

b. DHCP(67,68)

13. SSH (22)

7 Examples to Manage Linux Password Expiration and Aging Using chage

by Dhineshkumar Manikannan on April 23, 2009

Photo Courtesy: mattblaze

Best practice recommends that users keep changing the passwords at a regular interval. But typically developers and other users of Linux system won't change the password unless they are forced to change their password.

It's the system administrators responsibility to find a way to force developers to change their password. Forcing users to change their password with a gun on their head is not an option!. While most security conscious sysadmins may be even tempted to do that.

In this article let us review how you can use Linux **chage command** to perform several practical password aging activities including how-to force users to change their password.

On debian, you can install chage by executing the following command:

```
# apt-get install chage
```

Note: It is very easy to make a typo on this command. Instead of chage you may end up typing it as change. Please remember chage stands for "change age". i.e chage command abbreviation is similar to chmod, chown etc.,

1. List the password and its related details for an user

As shown below, any user can execute the **chage command** for himself to identify when his password is about to expire.

```
Syntax: chage –-list username (or) chage -l username

$ chage --list dhinesh
Last password change                                    : Apr 01, 2009
Password expires                                        : never
Password inactive                                       : never
```

```
Account expires                                          : never
Minimum number of days between password change           : 0
Maximum number of days between password change           : 99999
Number of days of warning before password expires        : 7
```

If user dhinesh tries to execute the same command for user ramesh, he'll get the following permission denied message.

```
$ chage --list ramesh
chage: permission denied
```

Note: However, a root user can execute chage command for any user account.

When user dhinesh changes his password on Apr 23rd 2009, it will update the "Last password change" value as shown below.

Please refer to our earlier article: Best Practices and Ultimate Guide For Creating Super Strong Password, which will help you to follow the best practices while changing password for your account.

```
$ date
Thu Apr 23 00:15:20 PDT 2009

$ passwd dhinesh
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully

$ chage --list dhinesh
Last password change                                     : Apr 23, 2009
Password expires                                         : never
Password inactive                                        : never
Account expires                                          : never
Minimum number of days between password change           : 0
Maximum number of days between password change           : 99999
Number of days of warning before password expires        : 7
```

2. Set Password Expiry Date for an user using chage option -M

Root user (system administrators) can set the password expiry date for any user. In the following example, user dhinesh password is set to expire 10 days from the last password change.

Please note that option -M will update both "Password expires" and "Maximum number of days between password change" entries as shown below.

```
Syntax: # chage -M number-of-days username
```

```
# chage -M 10 dhinesh

# chage --list dhinesh
Last password change                                    : Apr 23, 2009
Password expires                                        : May 03, 2009
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 10
Number of days of warning before password expires       : 7
```

3. Password Expiry Warning message during login

By default the number of days of warning before password expires is set to 7. So, in the above example, when the user dhinesh tries to login on Apr 30, 2009 — he'll get the following message.

```
$ ssh dhinesh@testingserver
dhinesh@testingserver's password:
Warning: your password will expire in 3 days
```

4. User Forced to Change Password after Expiry Date

If the password expiry date reaches and user doesn't change their password, the system will force the user to change the password before the login as shown below.

```
$ ssh dhinesh@testingserver
dhinesh@testingserver's password:

You are required to change your password immediately (password aged)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for dhinesh
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
```

5. Set the Account Expiry Date for an User

You can also use chage command to set the account expiry date as shown below using option -E. The date given below is in "YYYY-MM-DD" format. This will update the "Account expires" value as shown below.

```
# chage -E "2009-05-31" dhinesh

# chage -l dhinesh
Last password change                                    : Apr 23, 2009
Password expires                                        : May 03, 2009
Password inactive                                       : never
Account expires                                         : May 31, 2009
Minimum number of days between password change          : 0
```

```
Maximum number of days between password change          : 10
Number of days of warning before password expires       : 7
```

6. Force the user account to be locked after X number of inactivity days

Typically if the password is expired, users are forced to change it during their next login. You can also set an additional condition, where after the password is expired, if the user never tried to login for 10 days, you can automatically lock their account using option -I as shown below. In this example, the "Password inactive" date is set to 10 days from the "Password expires" value.

Once an account is locked, only system administrators will be able to unlock it.

```
# chage -I 10 dhinesh

# chage -l dhinesh
Last password change                                    : Apr 23, 2009
Password expires                                        : May 03, 2009
Password inactive                                       : May 13, 2009
Account expires                                         : May 31, 2009
Minimum number of days between password change          : 0
Maximum number of days between password change          : 10
Number of days of warning before password expires       : 7
```

7. How to disable password aging for an user account

To turn off the password expiration for an user account, set the following:

- **-m 0** will set the minimum number of days between password change to 0
- **-M 99999** will set the maximum number of days between password change to 99999
- **-I -1** (number minus one) will set the "Password inactive" to never
- **-E -1** (number minus one) will set "Account expires" to never.

```
# chage -m 0 -M 99999 -I -1 -E -1 dhinesh

# chage --list dhinesh
Last password change                                    : Apr 23, 2009
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

This article was written by **Dhineshkumar Manikannan.** *He is working at* bk Systems (p) Ltd*, and interested in contributing to the open source. The Geek Stuff welcomes your tips and* guest articles

create yum repository on local machine

Posted by Rishikesh Vispute Categories: Basic Linux, Email Marketing Series, How to

If you want to install software/packages after installation of linux (CentOS, Fedora etc.). You can create the yum repository to install all the software/packages which is present into the instillation CD. When you have try to install software/packages then some time it shows dependencies problems. To fix this problem I suggest your create the local machine yum repository by using the following steps.

1) Create directory

```
mkdir -p /root/install/RPMS
```

2) Copy all the software/packages RPMS from instillation CD/DVD to /root/install/RPMS directory

3) Install createrepo RPM from /root/install/RPMS directory using rpm command

```
rpm -ivh createrepo-0.4.11-3.el5.rpm
```

3) Now, we will have to create repo of the directory in which we have coied the RPMS. Following is the command to create the repo

```
[root@server ~] createrepo /root/install/RPMS
```

Once the above command gets completed you will find repodata directory in /root/install/RPMS folder

4) configuing YUM to work with local repository. Create a new file in /etc/yum.repo.d/ or open /etc/yum.conf and paste following

[local repo] name = OS $release - MyLocalRepo baseurl = file://root/install/RPMS enabled=1 gpgcheck=0

Now Try to install any package using ” yum ” command

for example:

```
yum install mysql
```

```
yum install php*
```

Done

USB FLASH DRIVE MOUNTING

Become root.

```
$ sudo -s
```

1. Plug in USB drive to a USB port.

2. Identify the correct partition name corresponding to the USB drive.

   For my Debian system, it is sda, and partition 1.

   ```
   $ dmesg |grep -i 'SCSI device'
   ...
   SCSI device sda: 3903488 512-byte hdwr sectors (1999 MB)
   ```

   Alternatively,

   ```
    $ grep  SCSI /var/log/messages
   ...
   Dec  1 11:52:26 tiger kernel: SCSI device sda: 3903488 512-byte hdwr
   sectors (1999 MB)
   ```

3. Mount the partition to an existing mount point (directory).

   ```
   $ mkdir -p /mnt/myusb
   $ mount -t vfat -o rw,users /dev/sda1 /mnt/myusb
   ```

   users give non-root users the ability to unmount the drive.

   You can verify the drive is indeed mounted as follows:

   ```
    $ mount
   ```

   You should see a line in the output that looks like:

   ```
   /dev/sda1 on /mnt/myusb type vfat (rw,noexec,nosuid,nodev)
   ```

TO RETRIEVE USB DRIVE

You must unmount the partition before physically unplugging the USB device.

```
$ umount /mnt/myusb
```

You can run the mount command again (with no argument) to verify that the volume is indeed mounted.

- Unplug USB drive.