

23/07/19

## what is Linux?

→ Linux is an open source O.S developed by Linus Torvalds in 1991. It supports CLI and GUI both mode and written in C and C++ language.

## What is open source?

→ Freeely available to all any one can customized the source code and distribute to all.

## What is Unix?

Unix → minix → Linux [C, C++]  
CLI, 1969

Unix is also an operating system developed by Dennis Ritchie & Ken Thompson 1969. It supports only CLI mode and written in C language.

## Types of open Source O.S

- ① Red Hat Linux
- ② Ubuntu
- ③ CentOS
- ④ Debian
- ⑤ SUSE Linux
- ⑥ Linux Mint
- ⑦ BSD/BSD
- ⑧ Kali Linux

## Features of Linux

- ① Multiuser - allow to login multiple user at the same time and use the same resources.

## Security

In most hat already built-in security like Firewall, iptables, TCP-Wrappers, SELinux.

## Difference between Linux and windows.

### Linux

### windows

- |  |   |
|--|---|
| ① Open source O.S                            | ① GUI & graphical version                 |
| ② much secure from virus                     | ② get easily affect by virus.             |
| ③ Software extension is .rpm                 | ③ In windows the software extension .exe. |
| ④ The file system is ext2, ext3, ext4, ext5. | ④ the file system is fat, ntfs.           |

## What is File System

File System defines how the data stored in your Partition table.

- ⑤ The booting file is lilo, grub, grub2

### ⑤ ntldr

[New technology loader]

## Types of user

① Super user [root]

# → Super user

② Normal user [navi, sambu etc]

\$ → Normal user

## A] How to switch in CLI mode

Ctrl + Alt + F<sub>2</sub> --- F<sub>6</sub>

## B) CLI mode to GUI mode

Ctrl + Alt + F<sub>1</sub>

## How to create user? → Commands

# useradd shweta

# adduser shweta

## How to apply Password → #Passwd username

### How to login

→ # su - username

### How to logout

→ exit / logout + ctrl D

### To remove completely

→ # userdel -rf username

-rf → remove forcefully.

24/07/19

cd → This command used to change directory.

Pwd → To check your current or present working directory path.

e.g # cd /var/log/samba

To back one step → ~~cd ..~~ cd ..

To back two step → ~~cd .. ..~~ cd .. ..

To back three step → ~~cd .. .. ..~~ cd .. .. ..

### Commands

#cd - : To go to previous working directory.

#ls → To check file and folder history.

#ll or ls-l → To check long list of <sup>file &</sup> ~~Folder~~ Folder

cd → folder      - → file.

#l. or ls -d → To check hidden file and folder list.

#ls -a → To check both hidden and unhidden file.

① #ll -a or ls -la → To check long list of both.

② #mkdir → This command used to create directory in local and remote machine.

③ Syntax :- mkdir -option foldername.

④ Option :-  
ex            -v [Verbose] Print command option  
              -P [Parent] .

\* How to create sub-folder or sub-directory

# mkdir -P data/datas1/datas2/datas3 -v

⑤ \* To know tree

# ls -R data

R → recursive

## \* How to create hidden folder

# mkdix .html

## \* Create folder with space count

# mkdix ' New movie'

# mkdix new\movie

## \* Create folder in loop

# mkdix data{1,2,3,4,5}

# mkdix data{1---10}

# mkdix xyz{a---z}

## \* How to delete folder

# rmdir

Note :- This command is used to remove directory but remove only blank directory.

rmdir data\* [remove folder starting with data]

rmdir \*data [remove folder ending with data]

rmdir \*data\* [remove folder starting or ending with data]

rmdir \* [remove every thing]

rm - To remove file and folder body even it is empty or not.

Syntax:- rm -option file/folder

OPTION -i [interactive]

-r [recursive]

-v [verbose]

-f [forcefully]

Note:- In the case of folder always use -r option.

rm -rf file → To remove file.

rm -rf /\* → To remove all data from machine.

### \* How to get file?

touch :- This command is used to create blank file and used to update time stamp of any exist file.

Syntax :- # touch abc

\*) cat :- used to check content of any file

Syntax :- # cat <file>

gedit → also used to make or file.

### \* Backup Utility

In this technique do create compress or archive of any content in a local or remote machine.

In the compress the original file size will be reduced depends on the compress technique and if archive it will create different name and store as a backup.

Types of command or tool to create Archive.

Two method

- 1) Tar
- 2) Zip

Tar :- This command used to create archive of any content.

Types of Tar method

- 1) gunzip
- 2) bunzip

Difference between gunzip and bunzip

gunzip

Bunzip

- ① extension is .gz
- ② speed is fast
- ③ compress ratio is less than bunzip

- ① extension is .bz.
- ② speed is slow.
- ③ compress ratio is much better than gunzip.

Note:- In gunzip or bunzip method we can not add or append extra content, but if there is normal tar then we can append or add.

Syntax to execute tar command

tar -option name - destination content

- option → -c [create]
- v [verbose]
- f [file]

-x [extract]  
-t [checklist]  
-r [read]  
-z [gunzip]  
-j [bunzip]

-C [change extract location or Path].

# du -sh /etc → To know size.

e.g:- To create normal Tar

tar -cvf backup.tar /etc

\* Create archive in gzip method.

tar -czvf abc.gz /etc

\* Create archive in bzip method.

tar -cjvf xyz.bz /etc

\* How to check list.

Interview  
tar -tvf abc.gz

\* How to extract

tar -xvf abc.gz - universal command.

\* change extract Path

tar -xvf abc.gz -c /mut

\* How to update [in normal tar]

tar -rvf test.tar abc3

- only in normal tar we can add abc3 in dest.tar which already include abc1, abc2.

\* How to create compress in gunzip and bunzip  
This will automatically apply extension .gz.

Command :-

gzip new

File name:- new.gz

How to read gunzip file?

zcat new.gz

Backup - restore  
34 MB (etc) -  
tar -cvf abc.gz /etc  
8.4 MB abc.gz

Decompress file in gunzip?

gunzip new.gz

\* Create compress in bzip method

# bzip2 new

To read bzip file?

# bzcat new.bz2

To decompress bzip file

# bunzip2 new.bz2

**Zip** → This command also used to create archive of any file and folder.

```
zip backup.zip /etc/*
```

To decompress →

```
# unzip backup.zip
```

27/07/19

**# wc** → word count

This command used to count line no, word, and character from any file.

Syntax :- #wc filename

e.g.:- wc abc

- 1) To check only line no :- #wc abc
- 2) To check word :- #wc -w abc
- 3) To check character :- #wc -c abc

**# less** :- This command used to check content of any file in short form.

We can scroll up and down the content.

Syntax :-

```
less /etc/passwd <filename>
```

Press q to quit.

# more :- This command used to check content of any file  
It show by default 10 line from top of any file.

# head filename

e.g.: head etc/Password

To check with custom line no:-

# head -n2 /etc/Password

# tail → by default show 10 line from bottom of the line

# tail /etc/Password

Pipe :- (|) → Shift left comm. to right.

# head /etc/Password | tail -n4

# head /etc/Password | head -n2 | tail -n1 >> newfile

↳ To save an  
create file.

# To check harddrive size

# fdisk -l

SATA - Serial advance technology attachment

PATA - Parallel advance

# To check Partition size

# df -Th

df → disk fragment

-Th → Type human readable.

# To check file and folder size

[# du -sh <filename>  
</etc>]

du → disk usage

-sh → show human readable.

[# du -sh \*] → show everything.

\* To check memory or RAM

# free

# free -k → To check size in kb

# free -m → in mb

# free -h → human readable.

\* To check memory utilization.

[# cat /proc/meminfo]

\* To check C.P.U

(i) # lscpu

(ii) # cat /proc/cpuinfo

\* To check U.S.B Port

[# lsusb]

\* To check bios lock

[# dmidecode]

\* To check Psi slot

Psi [Peripheral communication interface or interconnection]

comm →

# lspci

\* To check Kernel version

comm →

# uname -v

\* To check Kernel release Version

comm →

# uname -v

\* To check Kernel Name

comm →

# uname -s

\* To check O.S Name

comm. →

# uname -o

\* To check Processor support.

comm. →

# uname -p

\* To check Node name or hostname

comm. →

# uname -n or #hostname

\* To check all information of Kernel.

comm. →

# uname -a

\* To check Red Hat release Version

# cat /etc/redhat-release

\* To check IP and interface name

(i) if config → ifconfig

ip ip a

(ii) ip addr

\* To check interface speed

# ethtool IPname  
                  {eth0}

\* To check Lancard status.

# mii-tool IPname  
                  {eth0}

\* To check proper speed

# ethtool filename | grep -i speed  
                  {eth0}

i = ignored.

# ethtool eth3 | grep -i "DUPLEX"

#Find :- This command used to search any file, folder and user information over the machine or system, we can search by file/foldername, extension, size, permission and with username.

Syntax to execute find name

# find / -option Searchname

e.g:- to search file and folder information.

# find / -name data

[This use to search body]

\* To search only file

# find / -name data -type f  
f → file.

\* To search only directory

# find / -name data -type d

\* To search by extension.

# find / -name \*.txt

\* To search by size

# find / -size +1M } file or folder body.  
-1M }

# find / -size +1M -f → file.

# find / -size +1M -d → directory.

# To search by Permission

Alpha	num
r	4
w	2
x	1
uwx	7

Command

(i) #find / -perm 777

(ii) #find / -perm ugo=uwx

(iii) #find / -perm o=uwx

# find / -perm 755  
# find / -perm u=rx, g=rx, o=rx.

\* To search user information.

[# find / -user name]  
[# find / -name name]

30/11/19

# Locate :- This command also used to search information over the machine. It is faster than find command because it will work on database.

Syntax →

[# locate searchname]

e.g:- #locate data.

find command data base store inside.

/var/lib/mlocate/mlocate.db

If locate command does not execute then update his data base.

# updatedb

#grep :- [global regular expression Print)

→ This command used to search any pattern or string for any file.

Syntax:- # grep -option Searchname Searchdestination

e.g.: ① To search any Pattern

# grep -o root /etc/passwd

② To search any string

# grep root /etc/passwd

③ To check with line number

# grep -o -n root /etc/passwd  
# grep root /etc/passwd -n

④ To count line no:

# grep -c root /etc/passwd

c => count

⑤ To search case sensitive Pattern or Stream.

# grep -o -i root /etc/passwd

i = ignore.

⑥ To check with numeric value

# grep -w 1000 /etc/passwd -o

o => only

7) To Search commented and uncommented line  
(not used by system)

uncommented

# grep ^[^#] /etc/sudoers

commented

# grep ^[#] /etc/sudoers

/etc/sudoers | ~~root limit~~

To Save it

# grep ^[^#] /etc/sudoers >> new

8) To Search the matching Pattern and before the matching Pattern

# grep -A2 games /etc>Password

9) To Search before the matching Pattern.

# grep -B2 games /etc>Password.

10) To search both [After and before].

# grep -C2 games /etc>Password.

1) egrep or grep -E :- used to search multiple Pattern or  
String from single or multiple file.

# egrep -o 'root/nam' etc/passwd  
<filename>

# grep -E -o 'root/nam' etc/passwd

# multiple Pattern from multiple file.

# egrep -o 'root/nam/nip' etc/passwd/etc/group

# Single Pattern from multiple file.

Fgrep or grep -F

# Fgrep root etc/passwd etc/group etc/shadow

2) CP :- This command used to copy data from source  
to destination.

Syntax:- # cp -option Source Destination

options

- i [interactive]
- r [recursive]
- v [verbose]
- f [forcefully]

e.g:- To copy any file

```
# cp abc /mut
```

13] To copy any folder

```
# cp -r data /mut
```

Note:- To copy or remove in folder always use -r

14] To check message

```
# cp -v abc /mut
```

15] To copy content w/o copying source folder name

```
# cp -rvf data/* /mut
```

<Source>

<destination>

16) mv :- This command used to move data from source to destination.

- move command also used to rename file and folder name.

Note:- In case of copy command inode no. will be change but in the move no. will be the same.

- \* To check i-node no. of any file

```
# ls -i filename  
[abc]
```

i → inode no.

- \* To check i-node no. of any directory or folder

```
# ls -id cluto
```

```
# mv cluto /tmp
```

[To move folder inside folder]

- \* To rename:— This command used to change name of any file and folder.

```
# rename
```

```
e.g:- # mv music mediat
```

Syntax:- # rename old new old

e.g:- # rename mediat linux mediat.

- \* Cut :- This command used to cut any characters, delimiters and fields from any file.  
[: ; , . , ] [word] [word]

Syntax : #cut -option filename

option  
-c [character]  
-d [delimiter]  
-f [field]

e.g:- ① To cut any characters

```
# cut -c 1 /etc/passwd
```

```
# cut -c 5 /etc/passwd
```

```
# cut -c 1,3,5 /etc/passwd
```

```
# head -n1 /etc/passwd | cut -c3
```

```
# cut -c 1-5 /etc/passwd
```

e.g: ② To cut any field with delimiter

```
# cut -d: -f1 /etc/passwd
```

```
# cut -d: -f1,3,6 /etc/passwd >> now  
to save
```

\* Alias :- This command used to create fake name or nickname of any command.

Syntax :- alias K='mkdir'

```
#alias S='systemctl status network'
```

Vim /root/.bashrc

- ① To check aliases → # alias  
② To remove Particular alias → # unalias  
③ To remove all alias → # unalias -a.

29/07/19

# which fdisk  
# chmod 4755 /home/test ] by root.  
# sudo fdisk -l ] by user (test)

Whenever Sudo not working we need to go through above commands.

# find | -perm 000

O/P :- /etc/shadow.

ls -ltx : → To Know File Permissions.

Syntax :- ls -ltx filename.

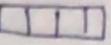
chmod 644 /boo.txt →

29/07/19

LVM - logical volume management/module.

→ This Partition technique use to expand and reduce Partition size with using data.

## Requirement to configure LVM

- ① First create Physical Volume (PV) 
- ② Create VG [Volume group] (multiple PV)
- ③ Create LV [client = 54GB]  
LV (logical volume).

Step 1 :- Create Partition, change hexacode (8C)  
Partition

Step 2 :- Change hexacode (8E)

Step 3 :- Save Partition Table and Update Partition Table.

### command

# fdisk /dev/sda

```

d
c o m m / f n
e e
c o m m : - h

```

```

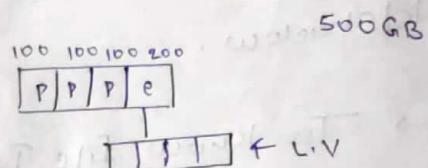
# enter
#
# n
(choose extended) 0 (e)
enter
enter
enter
enter

```

To check:- P [enter]  
medium:- N (Press)  
enter  
give size:- [+2G]  
P [Print]

Partition - 4

extended - 1



# fdisk /dev/sda

enter

n

3 times enter

n

2 times enter

Last sector : +2G

if you want to make more go through it.

To change hexacode Press t

Partition no: 5

Hex code :- 8E

Print :- P

To change hexacode:- t

Partition no: 6

hexacode: 8E

To Save :- w

# Partprobe /dev/sda :- To update Partition Table.

\* Create PV

# Pvcreate /dev/sda5 /dev/sda6

# Pvcreate /dev/sda {5,6}

\* To check PV

# Pvs

# Pvdisplay

\* To create VG

# Vgcreate myvg /dev/sda5. /dev/sda6

\* To check VG

# Vgs

# Vgdisplay.

\* Create LV

# Lvcreate -l +500M -n mylv myvg

{to give complete  
space of vg to lv} l → length  
iv. lv → name

# Lvcreate -l +100%FREE -n my\_vol /dev/vol0

lv name                      vg name  
my\_lv                      /dev/vol0

mylv - lv name.

myvg - vg name.

\* To check lv:-

```
# lvs  
# lvdisplay
```

\* Assign the file system or Format the disk

```
# mkfs.ext4 /dev/myvg/mylv
```

Note:- @ In ext file system (ext [2,3,4]) we can extend and reduce both.

② but in xfs file system, we can only extend but not reduce.

\* To check Format

```
# blkid
```

\* Create a mount point

```
# mkdir /test
```

```
# mount /dev/myvg/mylv /test
```

# OR  
+ TTY

\* To mount

```
# df -Th
```

\* To mount Permanent

```
# vim /etc/fstab
```

bottom  
→ UID  
→ write

# /dev/myvg/mylv /test ext4 defaults 0 0

(mount pt) (file system) (local storage)  
→ (disks) → (file system)

Save and quit. ~~wq~~.

1<sup>st</sup> o → disable checking file system.

2<sup>nd</sup> o → disable repairing file system.

\* To verify ~~fstab~~ file

# mount -o

\* How to extend LV<sub>m</sub> [in ext File System].

\* Step 1:- 1<sup>st</sup> check vg space availability.

# vgs

\* Step 2:- To extend

# lvextend -L +200M /dev/myvg/mylv

\* 3 :- # lvs

check df -Th.

\* 4 :- # resize2fs /dev/myvg/mylv

This command used to resize the file system who ~~is being~~ <sup>formatting</sup> extending data..

existing

df -Th. ← To check.

\* How to extend LV<sub>m</sub> [in xfs File System].

1 :- —||—

2 :- # lvextend -L +100M /dev/myvg/mylv

3 :- —||—

4 :- # xfs\_growfs /dev/myvg/mylv.

\* How to reduce LV<sub>m</sub>

Note:- in the case of extending LV<sub>m</sub> we can expand it online but in case of reducing set partition in offline mode.

To offline :- umount /test  
(mount point)

1:- lvls

2:- To check file system type

# e2fsck -f /dev/myvg/mylv

To verify  
partition corrupt  
or not.

(check inode-no, size, blocks, directory)

3:- To keep aside which data want

# lvresize -p /dev/myvg/mylv 400M  
↳ Point

4:- To minus data which we don't want

# lvreduce -L -300M /dev/myvg/mylv  
↳ Length

5:- Again mount it

# mount /dev/mylv /test

6:- # lvls

7:- # vgs

How to rename lv name.

# lvrename /dev/myvg/mylv /dev/myvg/lv1  
↳ Path

[Renamed mylv to lv1 in vg group]  
Check # lvls

→ To moname go into shell

# vim /etc/fstab

O/P:- /dev/myvg/lv1

## \* How to Scan LVM

```
# lvs
```

To check active, inactive logical volume

Op:- ACTIVE

## \* How to extend vg :-

To extend vg first create PV and then extend

```
# vgextend myvg /dev/sda7
```

## \* How to merge vg :-

First create PV then VG and then merge.

```
# vgmmerge myvg vg1
```

PVS - To check,

by default VG of  
PV size is 8G

## \* How to reduce vg :-

```
vgreduce myvg /dev/sda8  
<Partition name>
```

vgs -s 8M name  
VG.

## \* How to rename VG name :-

```
# vgrename Old_name New_name  
<myvg> <new.vg>
```

# PVS

```
# vim /etc/lfstab → To rename.
```

## \* How to Scan VG

```
# vgs
```

```
# pvs
```

## \* How to remove lv

1 → umount /test

umount mount p.v.

2 → remove that Parameter from fstab file.

3 → # lvmremove /dev/new-vg/mylv

## \* Remove vg

# vgremove vgname  
<new.vg>

## \* Remove PV

# Pvremove /dev/sda{5,6,7,8}

↳ /dev/sda{5..8}

## \* Remove Partition from Partition Table.

— fdisk /dev/sda

— 2 -> 3PV  
— enter

— Press d

— choose Partition no.

— w [exit]

Raid :- [Redundant area of independent disk array]

This Partition mainly used to store backup of data.

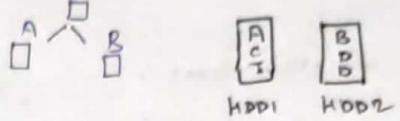
We can store single data in a multiple drive.

If any hard drive store fault then we can store data from other disk.

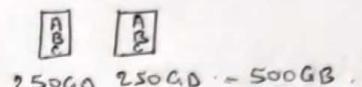
## Types of raid

① Raid0 - min 2 hard drive maintained with same size and same configuration, speed is fast, it work.

Striping technique. if 1 hard drive goes faulty then we cannot store the data.

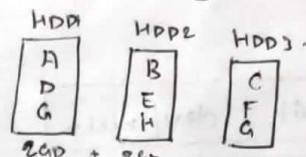


② Raid1 - min 2 hard drive maintained with same size and same configuration, it works on mirror technique. Speed is slow, it use 50% of storage, if one hard drive goes faulty then we can store the data.



$$250GB \text{ } 250GB = 500GB$$

③ Raid5 - min 3 hard drive maintained with same size, same config, speed is fast, it work on <sup>with</sup> striping <sup>Parity</sup> technique. if one hard drive goes faulty then we can store the data.



Requirement to configure Software raid(5)

Step 1 → Package should be install and package name is = mdadm  
(by default already there)

Step 2 → To check package available or not

# rpm -qo mdadm

or

# rpm -q mdadm

Step 3 Configure raid5

1:- Create 3 Partition with same size change hexicode  
#fd.

Save Partition table and update Partition table.

## Step 2:- To create RAID

```
# mdadm -c /dev/molo -a yes -l 5 -n 3 /dev/sd[0-2]
```

-C - create

molo - RAID name.

a → add or not.

l → RAID Label (RAID 5)

n → no. of disk [3 disk]

## Step 3:- To check RAID details

```
# mdadm -D /dev/molo
```

D - details.

```
# mdadm --detail /dev/molo
```

## Step 4:- Assign the file system.

```
mkfs.ext4 /dev/molo
```

## Step 5:- Create a mount point and mount.

```
# mount /dev/molo /data
```

save some file (e.g. abc{1..10}) in /data  
and check after faulty disk.

## Step 6:- To mount it Permanent.

```
vim /etc/fstab
```

UUID

```
# /dev/molo /data ext4 defaults 0 0
```

## Step 7:- To verify mount pt.

```
mount -o
```

\* How to set any disk as a faulty.

```
# mdadm -f /dev/mdb0 /dev/sda8
```

f → faulty.

} To check status  
mdadm -D /dev/mdb0

\* How to remove faulty disk.

```
# mdadm -r /dev/mdb0 /dev/sda8
```

\* How to add new disk

1:- First create Partition with same size

Enter

n

E

E

+2G.

2:- 

```
# mdadm -a /dev/mdb0 /dev/sda8
```

\* How to save raid service permanently?

```
[# mdadm -D --scan]
```

```
[# mdadm -D --scan >> /etc/mdadm.conf]
```

create file.

To save  
raid service.

```
[# cat /etc/mdadm.conf]
```

~~#mdadm --detail --scan~~

\* How to remove raid

```
[# umount /datac]
```

```
[# rm -rf /etc/mdadm.conf]
```

```
[# vim /etc/fstab]
```

remove from fstab.

```
[# mdadm -S /dev/mdb0 → To stop completely]
```

O/P:- stopped

```
[# mdadm -D /dev/mdb0
```

~~# /sbin/fdisk -D~~

## \* Remove Partition From Partition Table.

- Fdisk /dev/vdb
- d
- 8, f, b, s
- w
- Partprobe /dev/sda.

To reboot : ~~#init 5~~ #init 6

31/07/19

## Package management.

- ① rpm
- ② yum

rpm :- Red Hat Package manager

- This command useful to install, install, query, Search, update, upgrade any package.
- It works offline mode.
- cannot resolve dependencies automatically.

Syntax:-

# rpm -option Pkgname.

- option:-
- q → query
  - a → all
  - i → install
  - v → verbose
  - h → hash(++)
  - e → erase or uninstall

- U → Update or upgrade [window 7 to window 8]  
(7.1 to 7.2)

- R → R

\* To check Package install or not

# rpm -qa - zip      or      # rpm -qv zip

zip-3.0-10.214.x86-64  
↓      ↓      ↓  
Package    version    release      architecture  
name        version

# rpm -qv -- vim\* → multiple files.

To query all Package.

# rpm -qa

To count how many files.

# rpm -qvc | wc -l

# rpm -qa | grep zip

To know info

# rpm -qvi | grep -i zip

To check info of installed Package.

# rpm -qi zip → information

# rpm -i zip → installed

How to remove any Package

# rpm -evy zip

e → erase

h → y.

How to install Package.

1:- download or copy Package in your local file and then install that package.

```
# rpm -ivh zip-3.0-10.el7.x86_64.rpm
```

```
# rpm -qa zip
```

\* Install or repair any package forcefully.

```
# rpm -ivh zip-3.0-10.el7.x86_64.rpm --force
```

\* Install any package w/o dependencies

```
# rpm -ivh httpd-2.4.6-17.el7.x86_64.rpm --nodeps
```

```
# rpm --nodeps -ivh httpd-2.4.6-17.el7.x86_64.rpm --force
```

\* How to upgrade any package

```
# rpm -Uvh zip-3.0-10.el7.x86_64.rpm
```

\* To check Package information before installation.

```
# rpm -qip MariaDB-5.5.35-3.el7.x86_64.rpm
```

\* To check Package documentation.

```
# rpm -qad zip
```

\* To check file <sup>information</sup> installed via which rpm

Packages-  
file.

```
# rpm -qf /etc
```

e.g. - → # which useradd.

e.g.: # rpm -qf /usr/sbin/useradd.

O/p Shadow

\* How to verify all Packages

# rpm -Va

\* To verify Particular Package

# rpm -Vp zip-3.0-10.el7.x86\_64.rpm

\* Verify Package before installation.

# rpm -qPR mariadb-5.5.35-3.el7.x86\_64.rpm

R → dependencies.

\* To check recently installed package.

# rpm -qc --last

\* Remove Package without dependencies.

# rpm -evh --nodeps zip

Yum :- Yellowdog Updater modifier

- This command also used to install, uninstall, query, search, update, upgrade any package.
- It work online mode and offline mode and resolve dependencies automatically.
- It work on repository technique.

What is Repodata

It is heart of yum. It store all packages dependencies on archive mode. When we install any package it update

automatically resolve dependency from repository folder.

## \* How to create offline yum repository.

Step 1:- download or copy all package in your local file.  
and check repository folder exist or not.  
if not exist then we need to create that.

```
# cp -r * /data
```

\* → everything.

2:- To configure repository.

```
# cd /etc/yum.repos.d
```

pwd

ls

```
drwxr-xr-x 2 root root
```

ls

3) To create file with any name with .repo as extension.

```
# vim new.repo
```

by sitting in yum.repos.d.

\*- [first]

↳ repository [no space] in id

- Name = this is yum repo

\*- baseurl = file:///data

\*- gpgcheck = 0

- enabled = 1 } option.

GPG → gnu-pubkeycard check = 0.

wq!

# yum clean all ] To remove cache/history of yum.

How do verify yum is running or not :

# yum repolist all

or

# yum list all

178.85.254.254/content → enter To know Packages Online.

How to install Package

# yum install http\*

# yum install http\* -y

y → yes

cd

df

mkdir /date

mount /dev/sda1 /date

cd /date

How to install multiple package

# yum install http\* ftp\* bind\*

install package in group

① # To check group list.

# yum grouplist

② To install group list.

# yum groupinstall

'Development Tools'  
(group names)

Mkdirs, rm -rf, touch abc → at a time 2 commands.

To check Package available or not before installation.

# yum list zip

No fail

Opp:- zip from repository anaconda/7.0

To check Package information.

# yum info zip

# yum info zip\*

→ all package uploaded to zip

To search Package name.

# yum search zip

How to remove Package.

# yum remove http\* -y

To update any Package.

# yum update httpd

To upgrade any Package.

# yum upgrade httpd

To check Yum history.

# yum history

cd /etc/yum → all info.

## \* How to create repository?

- To get error remove metadata from repository
- To setup, nest one the metadata install "create srpm Package".

# rpm -ivh createmepo-0.9.9-23.el7.noarch.rpm --source  
<Package name>.

→ Then

# createmepo -v /data

# yum clean all  
# cd /repodata  
# ls

# yum repolist all

## \* online download.

EPEL → extra package for enterprise linux. (Fedora).

## \* How to install any 3 Party <sup>extension</sup> package via EPEL.

## \* How to enable EPEL.

# dnf install  
# yum repolist all

{ Network setting  
bridge adapter → yes } Network connectivity

EPEL → open in browser.

wiki

Take link.

Open terminal.

# wget copy link.

# rpm -ivh copylink  
ls

EPEL.repo → EPEL-testing.

# yum repolist all.

who -r

Shutdown -h now.

4/08/19

## operation of vi and vim

- These are Powerful Editor used to create, edit and modify any file and used in both mode.

Difference between Vi and Vim.

Vi

- ① Visual editor
- ② Old version of editing
- ③ Content show in black and white mode
- ④ No error check
- ⑤ No line no. shown

Vim

- ① visual simple editor
- ② latest version of editing.
- ③ Content show in colourful mode.
- ④ its check error.
- ⑤ it show line no.

Types of mode in Vi and Vim

Total 3 mode:

- ① Escape mode
- ② Command or Colon mode.
- ③ Insert mode

① **Escape mode** :- In Escape mode we can copy, Paste, cut, delete, undo, redo etc.

e.g.:- **# viw** [edit] Password

To copy any line.

→ Keep cursor on line at any character or and press **yy**

**yy** = To copy 1 line.

**2yy** = To copy 2 line.

**3yy** = —||— 3 line.

**;** → O/p - 3 line Yanked.

**4yy** = —||— 4 line.

To Paste

→ Press <sup>(small)</sup> **^P** To Paste. [Press in bottom of the line].

**Shift + P** → To Press above of the line.

To cut any line

**cc** → To cut 1 line

**2cc** → —||— 2 line.

!

**ucc** → —||— n line.

To cut line after the cursor

**Shift C**

To delete any line :- Press **dd** = delete 1 line  
**2dd** = delete 2 line  
**3dd** = delete 3 line.  
**n dd** = delete n line

To undo the lines :-

To redo the lines :- **Ctrl R**

To insert line in bottom of other line.

Press :\_

Shift + o :- To insert line in above of other line.

\*Command or colon mode :-

To go in command or colon mode Press Shift + colon .

e.g:- To set line no. → : set nn. : Se nn we should be in escape mode

To unset line no. → :Se nnnn

To Search any Pattern → :/root  
|root  
?root

To Search case Sensitive Pattern → : Set ic  
(or)  
: Se ic

To unset case Sensitive → : Set noid

To jump cursor only on highlighted Pattern :- Press u

To jump reverse :- Shift + u

To replace or substitute any Pattern :-

: %S | root | maj | g  
S → Substitution  
g → globally. [whole line]  
% → word whole file

To replace or substitute any Particular Pattern  
: 2,3s / sbin / szz / g

To unhighlight any Pattern:-

:nohl

:q → quit w/o save

:w → save

:wa → Save and quit.

:x → Save and quit.

:q! → quit forcefully

Example of insert mode.

Press i to insert into any file.

Replace mode :- Shift + R

(Keep cursor and just write it will automatically override)

Shift + V → To go into visual.

:edit |root|new → filename  
copy and ↑  
Paste content in any other file :  
or  
Cut and Paste.

## Runlevel

- It's a Process that define which mode System will be bo.  
[CLI or GUI].

→ In most version the first process name is init.  
and its PID is 1  
Older & newer

→ In most of the first process name is Systemd  
and its PID is 1

When user login the first process name is bash  
(bounce again shell).

To check Process ~~list~~ tree → PsTree

To check PID → Pidof Systemd

To check User Process → PS

Type of run level in each init 6.

There are 7 types of run level.

- ① init 0
- ② init 1
- ③ init 2
- ④ init 3
- ⑤ init 4
- ⑥ init 5
- ⑦ init 6

**init 0** → To Shut down or Power off mc.

**init 1** - Single user mode or Troubleshooting mode.

**init 2** - Multi user mode w/o networking.

**init 3** - Full multi user mode with networking and in CLI.

**init 4** → Not in use.

**init 5** → Full multi user mode in Networking or GUI mode.

**init 6** → To reboot mc.

## Types of run level in red box ↴

So there are 4 types of run level

- ① **emergency-target** - To break root Password.
- ② **rescue-target** - Same as init 1.
- ③ **multi/<sup>user</sup>target** - Same as init 3.
- ④ **graphical-target** - Same as init 5.

To check run level → # runlevel (or) who -r

~ 5 - no run level before 5

To check target in red box ↴ : #systemctl get-default

How to change run level :- #init 3 6,5,7 → RH.  
(Temporary)

# init 3

or

# systemctl isolate

→ only in red box ↴

multi-user-target

## \* How To Break Root Password → (in wd unit).

Step 1:- Reboot your PC.

Step 2:- Press arrow key (up and down) To Pause Kernel

- Step 3:- Select Kernel Parameter and Press e To edit.  
<sup>ISI one.</sup>

Step 4:- Select or Search "linux 16" from this cursor to "end option".  
end of line. Press <sup>space</sup> end. break.

Press Ctrl-X to start.

Emergency mode :-

NOTE :- Console = ttys0 - This lines have been removed.

# chroot /sysroot - change shell.

# mount -o remount rw /

Overwrite -o

Mount write -rw

# Passwd root

# touch /.autorelabel → To update SELinux Policy.

# exit.

# exit.

How to apply grub Passwd. ← H.W

## \* How to break root Password in R.H. 6

(1) Step 1 → Reboot your PC.

(2) Step 2:- Press up and down arrow Key.

(3) Step 3:- Press e to edit.

(4) Step 4:- Select Kernel Parameter.

(5) Step 5:- Again Press e to edit.

Step 6:- Type l or s or single.

7:- Press b to boot.

8:- # setenforce 0 → To Stop SELinux

9:- # passwd root (Set Password)

10:- # reboot.

How to Set run level Permanent Parameters in init 7.

Note:- There are 2 method to set run level Permanent.

① File method

② Command method.

In R.H. 7 to set run level Permanent we have a command method.

In R.H. 6 and older version to set run level Permanent we have a file method.

# systemctl set-default multi-user.target

# reboot

(Command method)

# echo \$shell → for finding current shell.

How to Set run level Permanent in init 6.

→ # vim /etc/initab → go into that file.

→ change :id:3:initdefault:

→ Save and quit and given reboot

How to check and change Service running in which run level.

There are 2 method to check and change.

① File method.

② Command method.

\* File method -

go inside this file

# cd /etc/init.d  
# ls

# cat ucsd.d

K → Service is Stop

S → Service is running.

To check and change via command method.

# chkconfig. or chkconfig --list

To change service status.

chkconfig --level 5 network off

To Stop Service in run time to check service status.

To check Service Status.

Systemctl status sshd.

To Stop Service in run time.

# systemctl stop sshd.

Enabled means start service on boot time.

disabled means stop service on boot time.

## How to Stop Permanent

```
# systemctl disable sshd
```

- RHEL 7

## How to Start and Stop Service in and out 6.

```
# service sshd restart
```

RHEL 6

```
# service sshd stop
```

## To start and stop permanent

```
# chkconfig sshd on
```

RHEL 6

```
# chkconfig sshd off.
```

**MASK** - mask is a technique to suppress any service on particular status.

(no one can start that service)

To start the service unmask and then restart.

```
# systemctl mask sshd
```

{Service name}

unmask :-

```
# systemctl unmask sshd.
```

To check status command

```
# systemctl is-active sshd
```

```
# systemctl is-enabled sshd.
```

**Crontab :-** This service used to schedule any job we can schedule any command or any script.

### Types of fields in crontab

- ① minute [0 - 59]
- ② hours [0 - 23]
- ③ day of month [1 - 31]
- ④ month [1 - 12] or jan, feb, mar, ..., dec
- ⑤ day of week [0 - 6] (Sunday = 0 or 7) or sun, mon, tue, wed, thu, fri, sat
- ⑥ command to be execute.

### Requirement to configure crontab

- ① Package should be install and Package name is cronjobs.  
**Daemon - controller**
- ② Daemon = crond.  
daemon → it is a controller to control the particular service.  
(every service has its own daemon)

Log File → **# /var/log/cron**

To check Package installed or not

**# rpm -qa cronjobs**

(08)

## # temporary cronjobs.

Service should be active or running.

```
# SYSTEMCTL status command  
# SYSTEMCTL restart command
```

To create folder via cronjob.

Note:- To execute any command via cronjob first check that command binary [optional]

To check command binary.

```
# which mkdir  
# type mkdir
```

To check

```
# mountab -e
```

→ This comm. edit cronjob config file.

```
# mountab -e -u www
```

root can cronjob config in www.

bin → any user can execute this command (mkdir)  
Sbin → only super user execute. (useradd).

Procedure:-

```
# mountab -e
```

33

18

↓  
min ↓ \* \* \*  
hrs any and ↓ any days.  
date

/usr/bin/mkdir /root/data.

# www.  
is

# cronjob -l → To check cronjob list.

# cronjob -e -u name → root what current it has  
it log & check timing.

\* To schedule any mail via cronjob

echo → To print msg.

# which echo } To check binary.

# cronjob -e } To make cronjob file.

Schedule task.

39 18 \* \* \* /usr/bin/echo "This is test msg".

# mail → To check mail.

# date → To check date.

# cronjob -l.

# date - 2 times

# mail

# !

\* How to broadcast any message

# wall "This is emergency"  
<msg>

# which wall

# cronjob -e

→ /usr/bin/wall

# 46 18 \* \* \* /usr/bin/wall

"This is  
Emergency msg"

# cronjob -l

# vim /etc/passwd.

\* Schedule monjob every minute.

```
# mountab -e
```

\* / 1 18 \* \* — II — ~~miss~~ every 1 min

\* / 2      18      \*      \*      \*      ——— 11      ← every 2 min.

\* / 1 19 \* \* \* ————— 11 ————— previous page

\* / \* \* \* \* — 11 — 82 hour to 82 min 1/4

\* / 1      19, 21, 23      \*      \*      \*      — 11 ←      APR 19, 21, 23  $\frac{1}{2}$   
 $\overline{\text{Exhibit A}}$

1 19, 20, 23 \* \* \* — 11 ← 19 min → 1 min  
20 — 11 ←  
25 — 11 ←

1 19-25 \* \* \* —— 11 —— beg 19 Jn 25.

| 19 | \* \* — 11 — every month date 1 at  
date days. 429 9492

| 19 \* | \* —|| ————— everyjan  
monday

1 19 \* 1-5 \* —— 11 ← Jan → May

1 19 \* \* 0-5 —— 11 ————— every sun.

\* Print msg on new year.

\* 00 12 50 dec \*

00 00 1 jan \* "Happy new year".

\* How to deny any user to use mountab.

- # vim /etc/mou.allow
- # man
- # :wa
- # mountab -e.

- **# touch /etc/mou.allow** - automatically all user deny.  
current and future.

# **Vim /etc/mou.allow** - only 1 user allow  
# man [write name of user] and mounting all deny

# **dm -rf /etc/mou.allow** - To allow all user.

How to execute any script by mountab.

series of command.

- 1 → create a script.
  - 2 → Vim new.sh
  - 3 → - mksel | root/jarv
  - touch | root/x42{1-10}
  - cp -rvf #wa1 | root/jarv | lmp
- } write in vim.

# !S

[# chmod +x new.sh]

# !S.

[# cronlab -e]

26 19 \* \* \* |root|new.sh

[# cronlab -d]

To give ~~task~~ Task yearly.

@yearly |usr/bin/echo "Happy New Year"

To give task monthly.

@monthly

@daily → To give daily.

@hourly

@weekly

How to remove cronlab

[# cronlab -e] → go into that file and press dd.

[# cronlab -r] → To remove all cronlab in that particular user.

[# cronlab -r -u name] → [To remove cronlab from user account by root].

## \* Service differences between RHEL6 and 7?

# Service <servicename> status (temporarily)

# service sshd status → to check the status

# service sshd start → to start the status

service sshd restart → to restart the services

service sshd stop → to stop the service

RHEL7  
#

systemctl status network

systemctl start network

systemctl stop network

systemctl restart network

RHEL6/7: for permanently stop/start the services RHEL6/7

chkconfig --list → for checking all the number services whether on (on) or off

chkconfig --level 5 sshd on → to "on" the services for sshd service on runlevel 5.

chkconfig --level 5 sshd off → to stop the services

RHEL7:

systemctl is-active sshd

systemctl is-enabled sshd

Shutdown

shutdown -h now → To shutdown.

6/08/19

## Some Basic command.

Extra

How to open terminal

Keyword :- Alt + F<sub>1</sub> to go application type.

Keyword :- Alt + F<sub>2</sub> to open run and Type  
gnome-terminal → enter → (\*) networking

[Graphical network object module environment].

How to maximize the terminal.

→ Alt + F<sub>10</sub>

How to minimize terminal

→

Alt + F<sub>5</sub>

or Alt + F<sub>10</sub>

To increase font size

→ Control + ++ --

How to open multiple terminal

→ Control + Shift + T

To switch multiple terminal

→ Control + Switch button [→]

To close the terminal

Alt + F<sub>4</sub>

Exit.

Control + cl.

How to open terminal

→ Alt + F<sub>1</sub> + to go application type.

How to open multiple tab :-

Ctrl + Shift + T

How to close multiple tab

Control + cl

#exit.

Switch between Tab's .

Control + Page up or down.

To clear page :- Type `#clear`  
Ctrl + L

[root@localhost ~]#

root → Username.

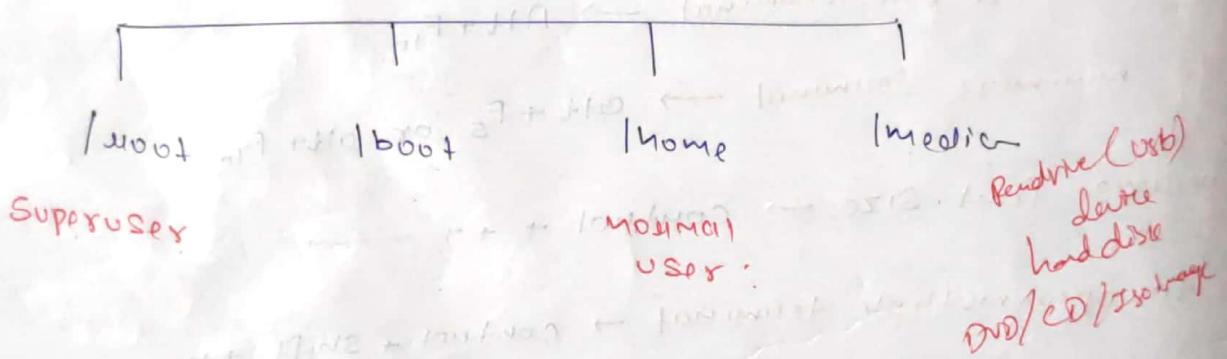
@ comment

localhost → Host name

~ → Home account.

# → Symbol of Superuser.

## Parent directory



# grep ^[#] /etc/Sudoers | root/list

To copy all un-commented files from Sudoers to root/list.

Cat → This command use to read file, you can create new file and open any file but can not modify &

# cat abc. ← To view filename.

# cat > abc ← To append . To create a new file.

# cat >> abc ← To append the file .

# cat -n new ← To check count of line no.

# tac new ← It will print file in reverse .

# gedit abc ← This command used to create edit and modify but only in gedit .

7/08/19

## User Management

① In this technique we are going to manage system users in a local and remote file. We can manage User Home Account, Shell, User's Policy and Password Policy.

② When you create user in a file automatically created some information.

(a) Create user home account in /home . folder .

(b) Create Username, Userid and shell in /etc/passwd .

(c) Create group information in /etc/group .

(d) Create Password information in /etc/shadow .

(e) Create mail account. /var/spool/mail/username .

③ How to create user

# useradd username  
<options>

# adduser username .

④ How to apply Password # Password meenue.

⑤ How to change user home account

There are 2 methods ① File method  
② Command method.

In which cases we need to change home account?

→ Space issue.

### File method

① First create home account # mkdix /data

② # vim /etc/default/useradd → edit this file and change home account.

HOME = /data.

③

Change user home account via command method.

### Command method.

# useradd -m *username* *username*  
# usermod -d /home/*username* *username*  
↓ *username*

Usermod -d /home/*username* *username*  
# cd /data

Fields inside Password. # vim /etc/passwd

Passwd  
Main :x:1001:1001::/home/*username*:/bin/bash.  
↓ Username      GID      HomeDir  
  ↓                VID      Comment      LoginShell

How to change or rename username

# usermod -l yahoo jaym  
l = login name.

Note:- when we rename username Password file, shadow file and mail account will be change and will not be changeusr home account and group account.

How to check and change user id.

Note :- in most host system user id start from 201 - 499 normal user id start from 500 - 60,000

In most host system user id start from min 201 and max 999 normal user id start from 1000 - 60,000.  
(by default root UID and GID is 0)

All UID and GID value define in

# vim /etc/login.defs

\* How to check UID of any exist user:

# id username

\* How to change UID of any exist user.

1 → First check id availability

# grep 1010 /etc/passwd /etc/group

If o/p come ← already used : ID

If o/p dont come ← not used : ID

~~# usermod~~

**# usermod -u 1010 Saro**

-u → UID

This command for existing user

\* New user with unique id

**# useradd -u 1020 waj**

\* How to apply comment.

For existing user

**# usermod -c "IT Team" Saro.**

For new user

**# useradd -c "IT Team" waj.**

\* How to check and change shell.

Types of shell.

① To check shell type

**# cat /etc/shells**

or

**chsh -l**

O/P :- /bin/sh - unix os

/bin/bash - Linux O.S

/bin/nologin - non interactive shell

/bin/CSH - C SHELL

To check default shell

# echo \$SHELL

To check bash version

# echo \$BASH\_VERSION

How to change shell of exist user

# usermod -s /sbin/nologin same. {for existing}

# useradd -s /sbin/nologin same. {for new}

(or)

# chsh -s /sbin/nologin same. (for usermod)

# chsh -s ~~/root/bin/bogus~~ same. (for useradd)

How to apply Password in bulk

# chpasswd

# Ram:123

# Same:modest

# vim /etc/shadow.

!v → To get previous command. [Put starting letter of command].

Types of algorithm to encrypt Password.

① SHA512 :- Secure hash algorithm version 512

② SHA 256 :-

③ MD5 → message digest version-5

④ DES → digitally encapsulation/encryption system

⑤ NONE → Password saved in Plain Text.

Note:- In method 6 Password encrypted in MD5 algorithm.

In method 7 Password encrypted in SHA512 algorithm.

Password algorithm depends on.

Vim /etc/login.defs

Change algorithm via command line

# chattr -c

# chpassword -c MD5

c → script.

To check, → # vim /etc/shadow

# vi -Vmct! wreset all

→ To wreset.

8/08/19

How to disable or lock user account

# usermod -L sara

L = lock

To unlock account

# usermod -U sara

only admin can do this.

How to lock user password

# passwd -l sara

To unlock

# passwd -u sara

How to delete user password

# passwd -d sara

d → delete

How to create user in bulk

# newusers

Enter

Sara:x:1020:1020::/home/Sara:/bin/bash

Control D → To save and quit.

id sara → To check.

## Create user via file method

1 → Create home account

```
# mkdir /home/maj
```

2 → go inside Password file.

```
# vim /etc/passwd
```

maj:x:1030:1030::/home/maj:/bin/bash ← Add manually.

3 → Edit vim /etc/group

Add manually.

```
# maj:x:1030:
```

:wq!

### Change home account permission.

```
# chmod 700 /home/maj
```

To check :- ls -ld /home/maj  
Change ownership and group ownership

```
# chown maj:maj /home/maj
```

### Copy the ~~skel~~ file.

```
# cp -r /etc/skel/* /home/maj
```

l. ← hidden file

```
# su - maj → To check.
```

ls -al → To check.

cd /home/linux,

## How to check and change user Password Policy

- ① File method
- ② Command method

### File method

1:-

# vim /etc/shadow

← This file contains the Password Policy info.

Command meth:-

# chage [option] [username]

← To change Policy.

# chage -option value [username]

Option

- l → To check Password Policy length.list
- d → To effect Set the date of last password change
- m → minimum no. of days before Password change.
- M → max no. of days before Password change.
- w → change warning days.
- E → Set account expire days.
- I → Set password inactive after expire account

To check Password Policy list

# chage -l [username]

Set the date of last Password change.

# chage -d 0 [username]

↳ immediately change [no days]

# chage -d yy/mm/dd [username]

(2020/01/01)

## How to delete user

# userdel -rif name → remove everything.

# userdel name → home and mail will not be deleted.

-r → remove.

## Group management

In this technique we are going to manage system group by local and remote file.

When we create group in a file automatically it adds some info in file.

- ① Create group name and group id in /etc/group
- ② Create group password in /etc/gshadow

## Types of groups

There are 2 types of group

① Primary (G)

② Secondary (G)

**Primary (G)** - we can create single primary member or multiple users but group can become multiple primary member of multiple user.

**Secondary (G)** - we can create multiple secondary member of multiple users, we can delete secondary member in multiple times but can not remove primary.

by default group user created name  
↓  
man(3)

① Create users

② Check membership.

# groups username,  
e.g. man,

O/P : man : man : HR f  
↓      ↓  
username      Primary group.  
                  member

③ How to create group

# groupadd groupname  
(e.g., HR, IT, sales)

④ Change Primary membership

# usermod -g HR man

g → Primary group  
HR → group

O/P :- man:HR

⑤

# usermod -g HR sauday

SAUDAY/HR

How to add secondary member

# usermod -G IT man

man:HR IT

# usermod -G Sales man

O/P :- man:HR Sales

O/P :- man:HR IT Sales

Add more Secondary member

# usermod -aG Sales man

O/P:- HR IT Sales.

How to remove secondary membership

# gpasswd -d man Sales

How to rename group name.

# groupmod -n yahoo Sales

How to apply group Password.

# viw /etc/gshadow

How to remove group Password

gpasswd -x HR

How to remove group

# groupdel groupname

# newgrp groupname ↪

## Permissions:-

108/19 It is a technique to apply permission for any folder and file & users to be read, write and execute by user, group and others.

### Types of Permission Technique.

- ① chmod
- ② chown
- ③ chgrp
- ④ Sgid
- ⑤ sudo
- ⑥ acl
- ⑦ chattr
- ⑧ Sticky-bit.
- ⑨ Suid

### Types of Permissions.

Alpha	numeric
r	4
w	2
x	1
—	—
uwx	7

## Super user

\$ touch total

7	5	5
/	1	1
rwx	rx	rx
v	9	0

\$ touch file

6	4	4
↓	↓	↓
rw-	rw-	r

## Normal user

\$ mkdir Java

7	7	5
/	↓	↓
rwx	rwx	rx
v	9	0

\$ touch xyz

6	6	4
↑	9	0
rw-	rw-	r

\* - All permission value define via umask

What is umask?

# umask

This command line will be used to assign the numeric value of command.

by default superuser umask value is 022 and normal user is 002

#

Star → (7 7 7)  
Solder → 0 2 2  
-----  
7 5 5

Site → (6 6 6)  
Solder → #  
-----  
0 2 2

\$  
7 7 7  
- 0 0 2  
-----  
7 7 5

\$  
6 6 6  
- 0 0 2  
-----

How to check and change

umask value.

- 0 0 0 2

# umask 0 7 7  
(Temp)

- To change.

How to set umask for permanent

write in bottom

# vim

1400t/.bashrc

# umask 077

for all users

Vim

1etc/.bashrc

bottom

# umask 077

# wq!

} by this all file and folder created by root will get permission like sudo.

# chmod → This comm. used to change permission of exist file and folder.

To be read, write and execute by user, group and others.

Syntax:-

# chmod value file/folder.

Note:- chmod comm. apply permission for all current and future user.

e.g:- # chmod 757 /data  
      / /  
      ^ 0

# ls

# chmod 756 /data → other user can't even execute and write.

754 → can't even read and write

751 → can execute but not open ls / To check.

/data → execute

753 → can execute but not read.

11 - d → T<sub>0</sub>

# chmod +f /data → u g o  
o/p ↴ 007. 0 0 0  
u w, ↴ 000 0 0 0

# chmod +s /data → u g o  
o/p ↴ 075. 0 0 0  
u r, ↴ 075

\* Apply Permission recursively.

# chmod -R 755 /data

\* Apply Permission via alphabetic value.

# chmod ugo=rwx /data  
o/p ↴ 077

# chmod a=rwx /data.

# chmod u=rwx, g=rx, o=--- /data.  
11 - d /data → To check.

# chmod o=rwx /data → only other will change.

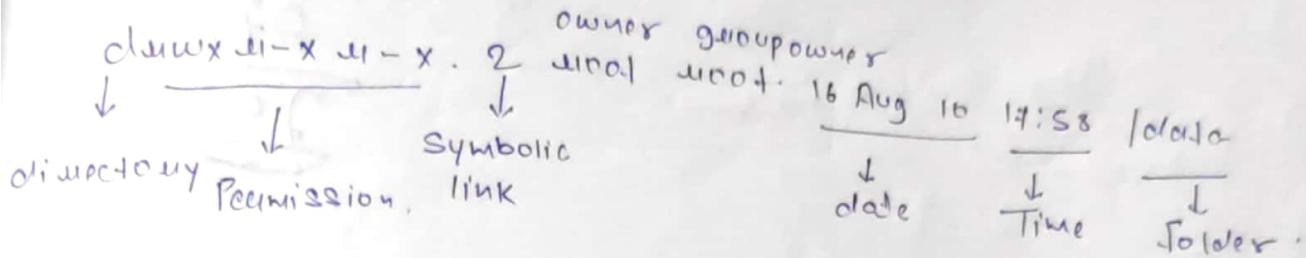
# chmod o+u /data → user will add in original  
# chmod o=w /data → overwritable by others.  
11 - d → To check.

# chmod -x /data → from all x will remove  
(ugb)

a-x  
ugo-x  
+x ← x will add

## chown → Change ownership

This command used to change ownership of any file and folder.



```
# chown user group file(s)
```

chgrp → This comm. used to change group ownership of any file and folder.

1 → Create group → #groupadd admin

2 → Add membership and change group permission.

```
# usermod -G admin man . } man & man will be
```

```
# usermod -G admin manvi } secondary mem. of group admin.
```

```
# chgrp admin manvi
```

" -d /data

# chown	root : root	/data	} To change both ownership and group ownership,
# chown	man : admin	/data	

Sgid → set group id or super group id.

This permission make any group as a super, any one can file and folder inside the supergroup folder automatically. Group ownership set to go to Parent folder.

How to apply Sgid 2 method,

① numeric .

2

② alphabetically g+s.

Numerically:-

# chmod 2775 /data

(08)

Alphabetically:-

# chmod g+s /data

O/p

imp

chmod uwsu-x  
↳ Super group.  
# cd /data  
# touch xyz  
# ll

How To remove ,

# chmod g-s /data.

# ll -d /data → To check.

Suid - set user id or super user id.

10/08/2019

This permission apply for any command's binary to execute particular comm. or all comm. by any other user.

To apply Suid there are two method:-

- ① alphabetic — u+s
- ② numeric — 4

Steps:-

1 → check Suid comm. binary # which comm. or # type comm.

2 → ll -d /usr/sbin/useradd → To check.

3 → 

# chmod	4755	/usr/sbin/useradd
---------	------	-------------------

or

# chmod	u+s	ll
---------	-----	----

O/P: drwsx  
↳ user

How to remove Suid

① Alphabetic

# chmod	u-s	comm.binary
---------	-----	-------------

  
(/usr/sbin/useradd)

Sudo :- Super user do

This comm. also apply permissions for any comm. binary to execute particular comm. or all comm. by particular user or group.

To apply sudo permission

edit this file 

# vim /etc/sudoers
--------------------

## (8) # visudo

- For testing create user and apply password.

For e.g.: - Allow Particular user to execute all comm.

Login by root → # vim /etc/sudoers

Write any where → userame ALL=(ALL) ALL.  
e.g. man ! / ↓  
anywhere any command.

Testing :-

Login via user

# sudoers  
Useradd username  
# sudo Password root.

Note:- before execute any comm. use sudo.

Allow Particular user to execute Particular command.  
or limited.

# which command name (disk-d)

# vim /etc/sudoers

Write → man ALL=(ALL) ! /usr/sbin/fdisk, ! /usr/sbin/useradd

How to deny some command.

Write :- man ALL=(ALL)

ALL, ! /usr/sbin/useradd, ! /usr/sbin/fdisk

Same thing w/o Password.

Write:- man ALL=(ALL)

COPASSWD: ALL, ! /usr/sbin/useradd

Allow sudo permission to any particular group

- ① Create group #groupadd groupname add membership  
# usermod -G admin man  
# usermod -G admin manvi

- ② vim /etc/sudoers.

Syntax:- %admin ALL=(ALL) ALL

How to create command aliases.

Vim /etc/sudoers.

Command Alias SOFT = /usr/libexec/useradd, /usr/sbin/fdisk, /usr/sbin/paste

Testing

Vim /etc/sudoers.

man ALL=(ALL) SOFT

manvi ALL=(ALL) !SOFT

%admin ALL=(ALL) SOFT

Note: ALIAS Name always in capital letter.

Chattr

= This permission used to stop accidentally deletion,

no one can delete (root) the file because via chattr.

Types of attributes to apply chattr permission.

① a

② i

③ a = In a attribute we can read, copy and open any file.  
and can not do other operations.

Syntax:- chattr +a abc  
(file name)

To check chatter Permission.

# lsattr abc.

To remove:-

[# chattr -a abc.]

I can be removed → rm -rf abc

② i - giv i attribute can do read and copy and can do other operation.

[# chattr +i abc.]

To remove.

[# chattr -i abc.]

To Secure

# chattr +ai abc ← only i work here.  
-ai ← To remove

**Sticky-bit** :- This Permission also used to stop deletion, owner of that file folder or root can delete or meet other user only can read.

How to apply sticky bit

There are 2 methods.

① alphabetic -s o+t

② numeric - 1

by root / Tst

mkdir data

11 -d / data

chmod 777 data

11 -d / data

Apply via numeric.

# chmod 1777 folder

or

# chmod 0+t folder

↳ other sticky bit.

How to remove

# chmod 0-t folder

ll -d folder → To check

Note:-  
tmp - default file system which already have attribute.  
sticky bit.

ACL :- access control list

This permission apply particular file and folder to be read, write  
and execute by particular user or group.

Syntax:-

# setfacl -m u:username:perm file/folder  
↳ file.      ↳ mode

# setfacl -m g:groupname:perm file/folder

Apply acl permission to particular user.

user → make file abc.

e.g:-

setfacl -m u:maw:rw abc

setfacl -m u:maw:rwx abc

↳ mode

+ = 'indicate act'

11 labc.

# getFact | file/folder  $\Rightarrow$  info.

- other user by default read file. (new user).

Apply act permission to any group.

# SetFact -w g:admin:rw labc  
↳ group name.

getFact labc

Apply act to other user as help with number 11

# SetFact -w o:--- labc.  
↳ user.

How to remove act from particular user.

# SetFact -x u:nam: labc

# SetFact -x g:admin: labc.

To remove all act from particular file.

# SetFact -b (o\*) labc

# SetFact --remove-all labc

11 labc

mkdir /test

ll -d /test

chgrp admin /test

ll -d /test

root	admin
chmod	2775

ll -d /test

ll -d /test

root admin	ls
cd /test	ll

mkdir test1	ll
-------------	----

mkdir test2	ll
-------------	----

root admin	ls
cd test2	ll

ls

mkdir test3

ll

o/p: root admin.

go inside test folder: # mkdir -P test1/test2/test3/test4.

# cd test1/test2/test3/test4.

Note: if you want to check main folder then go inside.  
 always make folder inside /Project/Project1/Project2/Projects

Question  
 touch {1001..10000}  
 bash: fork: cannot allocate memory

# cd  
 rm -rf shweta  
 fork can't allocate memory

Whenever reboot the server if we get root received below error

# Give root Passwd for maintenance  
 (or control+d to continue)

Solution: In this case should place the root Passwd  
 then change the runlevel  
 df -h /  
 fsck -y /dev/sda2

X-TS repair /dev/sda2  
 reboot

3/08/19

ls -laur

df --Type

df -H

df -TH

df -h

To download Package o.fline.

# df

# cd /mnt/mediavroot/RHEL-7.4 Server. x86\_64

# ls

# Package

# cd Packages

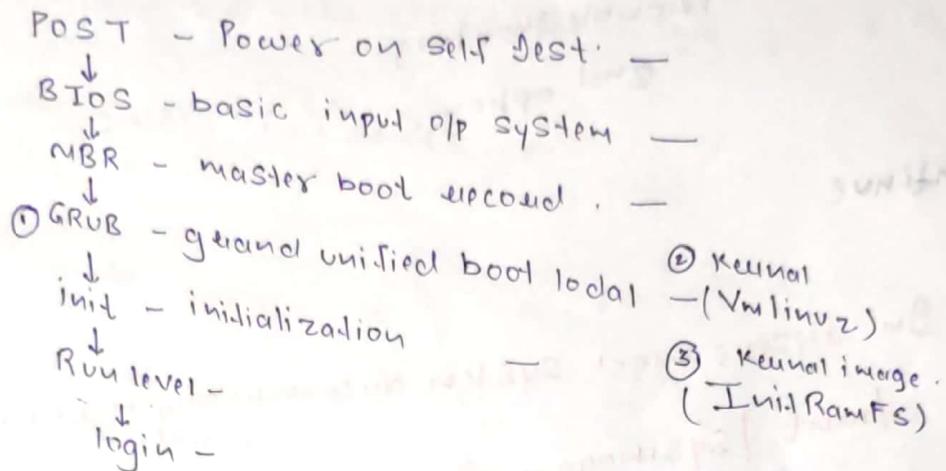
# ls

#

19/04/2019

## Troubleshooting

### Booting Process:-



Red hat 5 = LILO  
RHEL 6 = grub  
RHEV = grub2

### How to repair Kernel?

#### 1] To \*create Kernel error

```
- go inside boot folder # cd /boot  
- # um -uf vmlinuz-*  
# ls  
# ueboot - To check
```

#### 2] How to repair Kernel?

① Power off NIC

② insert bootable media and boot from media.

Power — Power on to ~~Normal~~ [BIOS Help]

- To go in rescue mode Press Esc button }  
boot: linux rescue. } all

RHEL 7 — Troubleshooting and Test  
2nd options. (press F2) → 2nd  
Continue. → Continue and F10 → ①

Note:-  
In rescue mode system automatically mount under /mnt/sysimage.  
In emergency mode system automatically mount under /sysroot.

- # chroot
- # mount /mnt/sysimage.
- # mount -o remount rw /mnt/
- # mount /dev/sr0 /mnt/
- # cd /mnt/Packages.
- # ls.
- # rpm -ivh Kernel-5.10.0-123.e17.x86\_64.rpm --force
- exit
- exit
- boot system from local drive.

## How to repair Kernel image.

### ① To get error

go inside boot folder and remove.

# initramfs-3.10.0-123.el7.x86\_64.ing

- # rm -rf initramfs-\*.

### ② How to repair

① Power off mc.

② insert bootable media and go in rescue mode

③ chroot.

④ mount

/mnt/sysimage.

⑤ mount -o bind /dev/mem /mnt/sysimage

cd /boot.

⑥ mkinitrd

initramfs-\$(uname -r).img

\$ - To call any variable.

⑦ exit.

⑧ exit

⑨

boot system from local drive.

## How to repair GRUB [in local host]

### ① To get error

go inside boot folder # cd /boot

and remove grub 2 # rm -rf grub 2  
# reboot

② To remove error.

① Power off mic.

② Insert bootable media and go into rescue mode.

③ # chroot /mnt/sysimage

④ # mount -o remount rw /

⑤ # grub2-install /dev/sda1

⑥ # grub2-mkconfig -o /etc/grub2.cfg

⑦ exit

⑧ exit

⑨ boot system from local drive.

How to repair GRUB in Red Hat 6

① To get error - same

② To remove error

- Power off mic

- insert bootable media

install or upgrade an existing system.

- Skip

- choose your language

- Basic storage device

+ Upgrade an existing installation

- create new boot loader configuration.

## How to resolve cutul-D

Note:- cutul-D error always comes from fstab file or  
file system may be corrupt.

This error always because of ~~extended~~ Partitions.

### To get error

- change write Parameter in fstab file when reboot.

### To remove error

- 
- give root Password to go in maintenance mode.
- #mount -o remount rw /.
- # vi /etc/fstab.
- correct the Parameters save and exit
- reboot.

## How to check file system - [in ext file system]

# e2fsck -f /dev/sda1

### How to repair

fscik -f /dev/sda1

check file system in xfs -

# xfs\_growfs /dev/sda1

To repair file system .

xfs\_repair /dev/sda1

# reboot

Note :-

If it is showing troubleshooting after rebooting if it booting from local drive. Then go to C.D and Power on and disconnect C.D.

(OS)

go to BIOS file and change Priority to Hard disk instead of CD-ROM.

## Types of Partition technique.

- (a) Swap
- (b) LVM
- (c) RAID.

## Hex/ID's of Partitions :-

Primary :-	Hex - 83
Extended :-	Hex - 85
Logical :-	Hex - 86
Swap :-	Hex - 85
LVM :-	Hex - 82
RAID :-	Hex - fe

To check Partition tables :- fdisk - l.

How to create Partitions :-

fdisk  
l (hex|dec)

y :- To create new Partitions. Hardisk name

d :- delete Partition.

w :- save and exit from Partition.

q :- quit w/o save.

P :- Print Partition Table.

Note:- logic Partition always start from no. 5.

## To create Partitions.

- ① go to Partition [fdisk /dev/sda]
- ② Press y
- ③ Then choose Partition style [msdos]
- ④ choose Partition no: [1 - 4]
- ⑤ Select first sector
- ⑥ Select last sector
- ⑦ w:- save and quit.

Note:- any thing change in Partition Table system Kernel not be update the changes.

To update Partition Table reboot your PC or use Partprobe command.

- ① Partprobe /dev/sda
  - ② kpartx /dev/sda
- Partx -a /dev/sda

Format or assign the file System.

# mkfs.xfs /dev/sda1

To check the file System type and UUID

# blkid

Create mount Point and mount the disk

① `mkfs -t ext4 /dev/sda1`

② `mount /dev/sda1 /mnt`

Vim /etc/fstab

wq!

`/dev/sda1 /mnt ext4 defaults 0 0`

wq!

To verify → mount -o

To check multiple & temporarily mount

# vim /etc/fstab

How to remove Partition

# umount /mnt

# Vim /etc/fstab

# dd if= /dev/sda1 of=/dev/null

wq!

fdisk /dev/sda

Parted d.

choose Partition no.

wq!

## Swap

This Partition technique used to create Virtual memory. We can create and delete Swap Partition in run time. To create Swap twice of Physical memory.

Types of methods. To create Swap  
There are 2 methods

① Partition method

② File method.

### Partition method :-

- 1 - Create Partition twice of Physical memory.
- 2 - Save Partition table and update Partition table.
- 3 - To check Swap status

# swapon -s  
(08)

# cat /proc/swaps

- \* To check size in human readable

→ first create Partition  
Create Swap

# swapon -v

free -h

# Primary | extended Swap Size :- double of Ram

# mkswap /dev/sda5

- To activate Swap Partition:-

swapon /dev/sda5

To check:-

swapon -s

swapon -v

free -h

free -ht

Result will come out after swapon.

To update or save  
\* To save Swap Partition Permanently

mount pt  
file system } is swap ] interview  
of swap

# vim /etc/fstab

write

# /dev/sda5 swap swap defaults 0 0

\* wa!

To check: df

\* To verify  
\* How to remove

mount -o

# swapoff /dev/sda5

\* How to deactivate Swap

# swapoff /dev/sda5  
(or) — Particular

# swap off -o — for all

\* Remove Parameters from fstab file.

# vim /etc/fstab

\* Remove Partition from Partition Table.

# fdisk /dev/sda

Delete 5th Partition which is swap Partition.

## \* Create Swap via file method.

# touch abc.

# dd if=/dev/zero of=/abc bs=1M count=1  
 ↓  
 → Go into / and check  
 ls

## \* Create Swap :-

# mkswap /abc.

\* To activate # swapon /abc.

w/o chmod swapon will error 644

## \* To Save Permanent

# vim /etc/fstab

# /abc swap swap defaults 0 0  
 # was!

~~# swapon /abc~~

# mount -a

To remove

# swapoff /abc

# vim /etc/fstab

# rm -rf /abc

To know memory # cat /proc/meminfo | more.

26/08/2019

## Networking

PC's and Printers connected b/w each other but cannot transfer the data.

PC's and Printers or any network device connected b/w each other and transfer the data.

### Types of address

There are 2 types of address

- ① Physical address
- ② logical address

① Physical address:- This type of address we cannot change.

Types:-

- ① Relatively physical [ MAC addr → media access control (48bit) ]
- ② Point address (16 bit)

② logical address:- These type of address we can change.

Types of logical address

- ① IPv4 32bit
- ② IPv6 128bit

① IPv4 :- This is a class full IP defining class discovery  
and developed by IANA  
(internet assign number authority)

### Types of class in IPv4

There are 5 types of classes.

Types range

A

0 - 126

B

128 - 191

C

192 - 223

D

224 - 239

E

240 - 255

127 reserved for loop back

loop back ip reserved for self testing, by the help of this ip we communicate other host.

check :- ifconfig.

APIPA - automatic private IP addressing

range :- 169. . . . .

Why IP address assign like this 0.0.0.0?

⇒ because IANA assign it in octet format.

8	8	8	8
255	255	255	255

What is Subnet or net-mask.

Sub-net mask define how many bits are on or off in your network.

By default class A Subnet mask is  $255.0.0.0 /8$

↓      ↓  
Subnet / net mask      CIDR  
↓  
Class A inter domain routing.

Class B :-  $255.255.0.0 /16$

Class C :-  $255.255.255.0 /24$

Class D :- broadcast multicast

Class E :- research and development

$\begin{array}{r} 255 \ 255 \ 255 \\ \underline{\underline{10 \ 0 \ 0 \ 0}} \end{array} /8$  - 1 bit on

$\underline{\underline{10 \ 0 \ 0 \ 0}} /16$  - 2 bits on,  $-10.255.255.254$ .

$10.0.0.0 /15$

$255.111110.0.0$

$255.\underline{254}.0.0$

$128 \ 64 \ 32 \ 16 \ 8 \ 4 \ 2 \ 1$   
 $\begin{array}{r} 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \\ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \\ \hline 254 \end{array}$

$255.255.128.0 /17$   
 $\underline{\underline{8-32}}$        $\underline{\underline{8+1}}$

$10.0.0.0$  - Network ID

$10.0.0.1 \rightarrow$  IP assign.

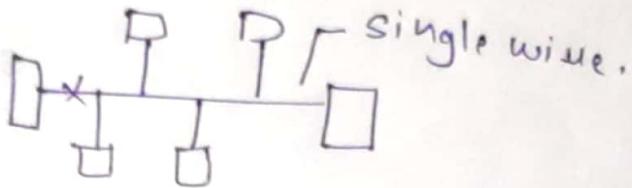
$10.0.0.0255 \rightarrow$  BID

# What is Topology?

It's a process that define the physical architecture of network.

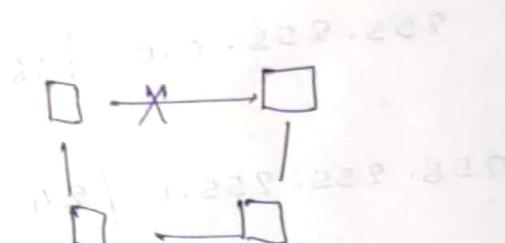
## Types of Topology?

### ① Bus Topology

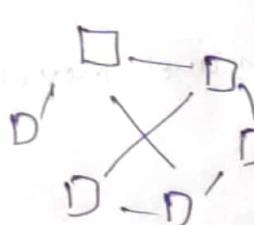


### ② Ring Topology :-

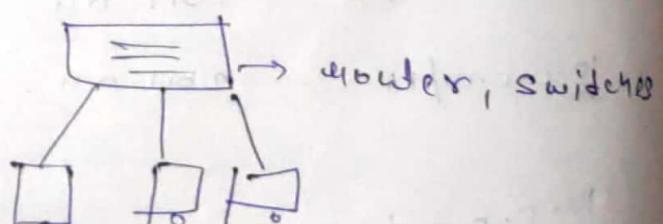
(Packet lost)



### ③ Mesh Topology



### ④ Star Topology



### ⑤ Hybrid topology

(Star + bus)

192.168.1.10

## Types of Duplexing

OSI Model  
PSL Model

- ① Simplex - we can only receive but cannot send.  
(Micro, FM, TV)
- ② Half duplex :- we can send and receive Packets but not at a time.  
(Walkie-Talkie, Hub)
- ③ Full duplex :- we can send and receive Packets at a time.  
(Mobile, switches, routers).

## How to assign IP in red hat?

There are 3 method to assign IP

- ① NNTUI (Network manager terminal user interface)
- ② NMCLI (Network manager command line interface)
- ③ File method (etc/sysconfig/network-scripts)

Check IP and interface name.

# ifconfig (or) # ip a (or) ip addr

To check interface speed.

# ethtool eth0 1000000000 <interface name>

To check interface status.

# mii-tool interface name.

1) Assign IP via NMUI → # nmui → e → edit → add →  
ethernet

Activate or connection if not showing change  
(or)

ipup name

ipdown name

Possible names: any

device: lan card name.

manual → show → add → ok → quit.

To change ip configuration.

# ipdown name } only for nmcli

# ipup interface name.

Assign IP via nmcli command

# nmcli connection add con-name static ifname interface

Yes type ethernet ip4 192.168.0.1/24 gw4 192.168.0.1/24

↓  
172.168.25.0/24 (mediator)

To check connection.

# nmcli connection show (or) nmcli con show  
or

# nmcli con

To up and down connection via nmcli command.

# nmcli connection up connection name  
(or)  
{statics}

# nmcli connection down static.

How to modify IP via nmcli command.

# nmcli connection modify static ipv4.addresses 192.168.0.20/24 ipv4.method

checknmcli connection up static.

How to delete connection.

nmcli connection delete static.

checknmcli connection show.

Assign IP via file method. [6, 7, 8]

# cd /etc/sysconfig/network-scripts.

# ls # vim ifcfg-eth0.

# cp ifcfg-eth0 ifcfg-eth0.

# ls yes (anyname) (anyname)

# vim ifcfg-eth0

DEVICE - eth0 --

IP Addr -

Net mask - 255.255.255.0.

Onboot - yes.

Name - eth0

Wq.

# systemct start network.

# ifconfig → To check

How to set hostname or node name.

# hostname → To check hostname

(or)

uname -n

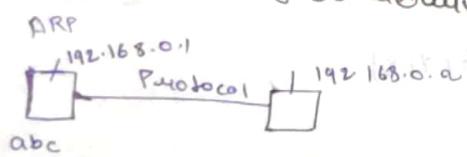
To change → # hostnamectl set-hostname Server1.example.com

To update terminal :- # bash  
(or)  
# exit

\* Hostname save inside # cat /etc/hostname

PING - Packet Internet George

→ To verify the time do which packet or system active or not.



ARP TCP UDP → Types of Protocol

To resolve via name w/o DNS Service.

vim /etc/hosts

write # 192.168.0.60 Server2.example.com google  
www!

↓ alias

DIG: daemon internet groups  
→ To verify dns server service.

# nslookup - To check ip and hostname from dns server  
# nslookup Servername.

# hostname -d → To check domain name.

fqdn → Fully qualified domain name.

How to assign IP in netcfg 6.

There are 2 method to assign IP

- ① Command method
- ② File method [Same]

① Command method.

# Setup

- Select network config.  
↓
- Device config  
↓
- Choose interface name

Space - To check uncheck.

NAME :- eth0

OK

Save and quit  
quit.

# ifup eth0 (as) Service network restart

## How to set hostname.

To check :- hostname.

To change :- hostname server1.example.com - Temporarily.

To Save Permanent.

# vim /etc/sysconfig/network.

change it. HOSTNAME=

# bash.

nmcli con add con-name manisha ifname eth0 type ethernet autocom

Yes ip4 172.168.25.0/24

# Firewall

3/09/19

- So this service use to secure system over the net.
- we can apply rules like src except, dst and forward.
- apply rule via host, network, protocol and with port no. and Service name.
- It works on zone technique.

## Types of zones

- ① Home zone.  
reject all incoming traffic only allow ssh, http, samba, mDNS, ipi-client.
- ② Block zone.  
reject all incoming traffic.
- ③ Drop zone.  
reject all incoming traffic, do not even respond with icmp protocol.
- ④ Trusted zone  
allow all incoming traffic.
- ⑤ Permit zone  
reject all incoming traffic only allow ssh and drop and this is default zone activate or running in system.

## How to set hostname.

To check :- hostname.

To change :- hostname server.example.com - Temporally.

To Save Permanent.

# vim /etc/sysconfig/network

change it. HOSTNAME:-

# bash.

nmcli con add con-name manisha ifname eth0 type ethernet autocong  
Yes ip4 192.168.25.0/24

# Firewall

3/09/19

- So this service use to secure system over the net.
- we can apply rules like accept, reject and forward.
- apply rule via host, network, protocol and with port no. and service name.
- It works on zone technique.

## Types of zones

- ① Home zone.  
reject all incoming traffic only allow ssh, dhttp, Samba, mDNS, ippi-client.
- ② Block zone.  
reject all incoming traffic.
- ③ Drop zone.  
reject all incoming traffic, do not even respond with icmp protocol.
- ④ Trusted zone  
allow all incoming traffic.
- ⑤ Permit zone  
reject all incoming traffic only allow ssh and dhttp and this is the default zone activate or running in system.

## How to manage Firewall.

There are 3 method to manage Firewall via

① GUI

— # firewall-config

② CLI

— # firewall-cmd

③ file method

— # /etc/firewalld / firewall.conf

### Requirement to configure Firewall

- Set hostname and ip and check Firewall Package install or not. and check service should be active or not.

# systemctl status firewalld.

# systemctl restart firewalld.

### To check default zone,

# firewall-cmd

-- get-default-zone

### To check active zone.

# firewall-cmd

-- get-active-zones

### To check zone list

# firewall-cmd

-- get-zones

### To check Services

# firewall-cmd

-- get-services

To check default zone information,

# firewall-cmd --list-all

To check Particular zone list,

# firewall-cmd --list-all

To check all zone information,

# firewall-cmd --list-all-zones

To set your default zone,

firewall-cmd --set-default-zone=home

To add or remove allays first reload [any changes made]

firewall-cmd --reload

How to add and remove services in default zone.

Permanent

# firewall-cmd --permanent --remove-service=ss4

firewall-cmd --reload

To remove service on any Particular zone

# firewall-cmd --permanent --remove-service=ss4 --zone=Public

# firewall-cmd --reload.

In run time remove service on default zone

# firewall-cmd --remove-service=sshd

To add Service Permanent

# firewall-cmd --permanent --add-service=sshd  
# firewall-cmd --reload.

How to add and remove ports  
[default zone]

# firewall-cmd --permanent --add-port=22/tcp  
in particular zone.

How to add and remove interface.

Step 1:- add physical or virtual interface in system and then  
add them add in firewall zone.

# firewall-cmd --permanent --add-interface=en0  
# firewall-cmd --zone.

--reload.

How to add and remove Source filter :-

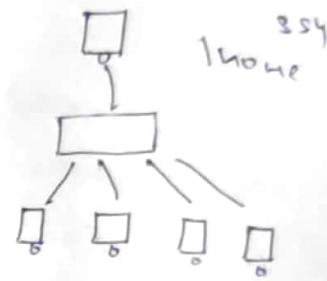
Particular IP

# firewall-cmd --permanent --add-source=192.168.0.20/24

Particular IP

# firewall-cmd --permanent --add-source=192.168.0.0/24

How to apply rich rule.



# firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=192.168.0.4/24 service name=ssh reject'

Service

Name = ssh reject

How to forward any Port.

First check about Port availability

# netstat -anulp | grep 8961

J - listen

P - Protocol

LO - Port=8961

# firewall-cmd --permanent --add-rich-rule='rule family=ipv4 protocol=tcp to-port=8961 port=8961'

4/09/19

## iptables

This is like a software Firewall to secure system over the net.  
It's less secure than Firewall.

Requirement to configure iptables.

- ① Set hostname and ip and check iptables package install or not.

Syntax to execute iptables

```
# iptables -I/A/D/R/F/L [chain] --SPOUT [INPUT/OUTPUT/FORWARD]
-P [tcp/udp/icmp] --SPOUT --CPOINT -s -d -j [ACCEPT/REJECT/DROP]
--ACTION
```

I → insert  
A → append  
D → delete  
R → replace  
F → flush  
L → listen  
-P → Protocol

--SPOUT → Source Port address

--CPOINT → destination Port address

-s → source ip addr

-d → destination ip addr

-j → jump

② Check Package installed or not : # rpm -qo ipatables.

③ Check System should be upstart or Acitive.

# systemctl status ipables

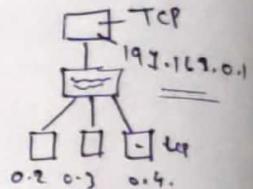
# systemctl enable ipables

# systemctl start ipables

To block all network via Protocol.  
icmp → Protocol.

# iptables -I INPUT -p icmp -j REJECT } for all nw.  
# ping

To block or deny Particular host.



# iptables -I INPUT -p tcp -s 192.168.0.3/24 -j REJECT

# iptables -I INPUT -p tcp -s 192.168.0.3/24 -d 192.168.0.5/24 -j REJECT

To deny entire network

# iptables -I INPUT -p tcp -s 192.168.0.0/24

-j REJECT.

To allow and deny via Port no.

# iptables -I input -p tcp --sport 22 --dport 25  
-j REJECT

To check iptables rules.

# iptables -L

To check Particular chain list.

# iptables -L INPUT

# iptables -L OUTPUT

# iptables -L FORWARD

To remove Particular rule from Particular chain.

To Set line no.

# iptables -L INPUT  
-L Line-number

Vim /etc/sysconfig/iptables -i file

# iptables -D INPUT 4  
-L delete

To remove all rule from all Particular chain.

# iptables -F INPUT

To remove all rule from all chain.

# iptables -L

To save iptables rules

# service iptables save

tcp-wrappers

[Very less frequent].

This service also used to secure system over the network.  
we can allow and deny any service over Particular user  
or all user.

It works over 2 files.

- ① # /etc/hosts.deny
- ② # /etc/hosts.allow

It's less secure than Firewall and iptables.

¶ To deny any services

# vim /etc/hosts.deny  
write

SSH: 192.168.0.4/24

SSH: desktop 2.example.com

SSH: 192.168.0.0/24

SSH : \* . example.com

SSH : \*

SSH, FTP, HTTP : 192.168.0.10/24

SSH : all except 192.168.0.50/24

## Process management

In this technique we are going to manage system process on local and remote file.

We can manage application resources, CPU utilization, memory, and disk network and disk utilization.

To check Process tree. # ps -tree

To check PID of any Process # pidof system

To check user Process # ps

Note:-

pts represents user login in graphical mode  
tly2 represents user login in CUI mode. 10 - terminal one  
12

tly6 - terminal 6 & login.

To check user login # who

# w

# Pinky

# finger

To check all Process including CPU memory and disk utilization.

# ps -aux

a - all

u - user

x - extra full command

Header field in ps-aux.

USER	PID	virtual memory			STAT	START	TIME		
		%CPU	%MEM	VSIZE				RSS	TTY
root	1	0.0	0.6	53940	6944	?	Ss	08:26	0.06

/usr/lib/systemd/system --switched

VSIZE - virtual memory used by process

RSS - Physical memory used by process

TTY - Terminal

STAT - Status

Ss - Background running

# ps aux

To check child Process of any Parent

# ps -efH

efH - extra full command in human readable.

To check user Process [PID]

# ps aux

# ps -aux 1 group

To check Process name via PID

# ps -aux | grep -w 51924

w - what

How to kill any Process.

Types of Signals.

Signal 15 / TERM - This signal used to terminate any process.

Signal 9 / KILL - This signal used to kill any process forcefully.

Signal 1 / HUP - This signal used to store command off.

e.g.: Signal 15 / TERM

# ping  
# pinger 192.168.0.10

# pidof PING

# kill -15 51952

# kill -TERM 51953

e.g.: Signal 9 / KILL -

# su - save  
# pgrep -u save  
# kill -9 52019

Kill -KILL 52019

Kill -KILL 52019

e.g.:

# nohup ping 127.0.0.1

# tail -f nohup.out

This comm. used to create file with name of nohup.out

5/09/19

- \* How to run any Process in background.

```
# nohup Ping 127.0.0.1 &
```

- \* To check background Process.

```
# bg
```

- \* To check Process name in background.

```
# jobs
```

- \* Run Process in foreground

```
# fg 2
```

- \* How to manage system Process.

There are 2 method to manage

① GUI

② CLI

- To manage via GUI

```
# gnome-system-monitor
```

- To manage via CLI

```
# top
```

PR

- Priority

NI - nice value.

SHR - Shared memory

VIRT - Virtual memory.

Note: To check in colour Press Z.

To change delay time. [by default 3 sec]

Process S → change delay → enter.  
(X)  
(D)

C → First Process [check highest resource utilization]  
S - background.

\* To kill any process through top.

# Ping 127.0.0.1.

# Pidof Ping.

Process K → choose PID → enter → choose signal (15) → enter.

\* To kill any user process.

by: Ram → Ping

Process U → choose user → enter → Kill by above method.

\* How to check and change nice value of any process  
-0 do -20 → range of nice value.

To check nice value.

# Ps -eo comm,nio,%C.P.U,%Mem,Pid

| group shell  
optional.

\* How to change nice value.

# renice -10 2054

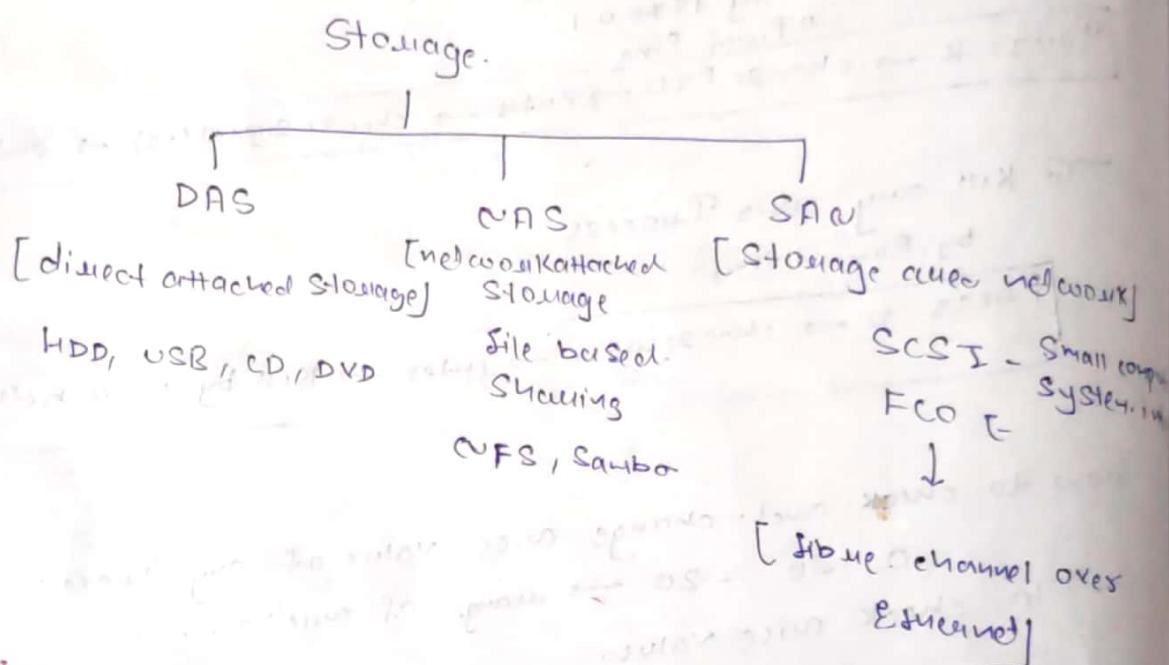
Run again above command. To change.

# Ps -ef | grep -i func. +

## NFS Server.

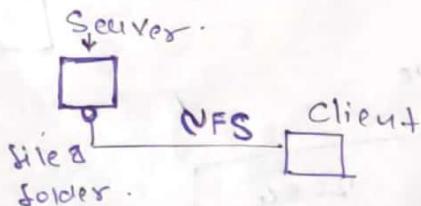
NFS - network file system

This service used to share file and folders over the network.  
It works offline mode and communicate with same operating system.



Note:-

NFS is unsecure by default but we can secure via Kerberos. Kerberos.



Requirement to configure NFS.

- ① Set hostname, set up and create group and user.
- ② Package install

# nfs\*

Daemon - nfs-server - RH 7  
nfs - RH 6

configuration file → /etc/exports.

③ Check Package available or not other installed it.

# rpm -qo nfs\*

④ Create folder.

# mkdir /read /write  
Change Permission # chmod 777 /write

# vim /etc/exports

write :-

/read      ↗ client IP  
/read      192.168.0.3/24(40) -  
/read      desktop.example.com(40) -  
/read      192.168.0.0/24(40) - Particular h/w.  
/read      \*.\*.example.com(40) - client IP.  
/read      \*(40) - domain name.  
/read      all [A,B,C]  
/write     \*(ecos)  
/write     \*(rw)

To verify and refresh exports file

# exportfs -r

# exportfs -av

# systemctl restart nfs-server

# systemctl enable nfs-server

# firewall-cmd

--permanent --add-service=nfs

# firewall-cmd --reload

Server IP: 172.25.5.14 | 24

## On client side:-

Client IP: 172.25.5.10 | 24

Gateway: 172.25.254.254  
DNS Server: 11

- ① Set hostname and ip and check communication between server and client.

- ② To access NFS share folder to mount NFS Server.

# mkfs -t ext4 /dev/sda1

- ③ mount it

# mount

# mount

# df

→ Server IP

192.168.0.1:/read /dev/sda1

192.168.0.1:/write /dev/sda1

= TH

check: { cd /dev/sda1 → ls -labc  
cd /dev/sda1 → ls -f abc

- ④ To mount Permanent:

# vi /etc/fstab

write: - 192.168.0.1:/read /dev/sda1 nfs defaults 0 0

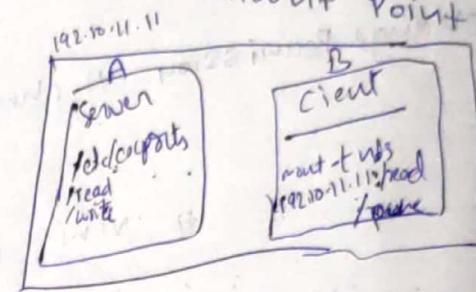
192.168.0.1:/write /dev/sda1 nfs defaults 0 0

wow!

- ⑤

# mount -o

# df -Th



on server side  
share nfs folder with unique user id and group id.

# useradd admin  
# groupadd admin  
# id admin.  
# group addadmin local group  
# vim /etc/export

wide :-  
lread  
lwrite  
# exports

To check su - man in Server  
cd /wide  
touch abc.  
Client Side :-  
How to remove.  
① umount  
② vim /etc/fstab - remove  
# off

## ④ Server Side

# vim /etc/export  
remove everything  
# systemctl stop nfs-server  
# systemctl disable nfs-server  
# Firewall-cmd --permanent --remove-service=nfs  
# Firewall-cmd --upload

## Samba

Vim /etc/samba/sub.conf.example.

- \* This service used to share file and folder over the net.  
It works both online and offline mode.  
It communicate with same and different both operating system

### Requirement To configure Samba

- ① Set hostname, ip and update yum.

Package Name :- Samba\*

Server:-

Daemon:- smbd [Samba msg block].

Configuration file:- /etc/samba/Sub.conf

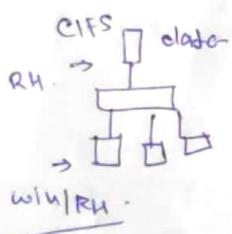
log file

: /var/log/samba/Sub.log

Port no:-

137 and 138 for UDP

139 445 for TCP



### Server Side

- ① Set hostname, createIP and install this Package.

# yum install Samba\* -y.

- ② Create folder shared via Samba.

# mkdirs /data

- ③ Create user & apply Password for authentication.

# useradd s1am

# Subpassword -a s1am.

④ Create config file # vim /etc/samba/sub.conf.

go about line no. 94, 95

Interfaces means allow samba share folder to Particular host  
and host allow Parameter define allow Particular user.

interfaces = 10 eth0 192.25.18.11  
host allow = 127.192.168.0.3/24 192.25.18.10  
127.192.168.0.10/24.  
127.192.25.6.

Same file go to bottom and copy line from 814 to 820.  
and Paste there only.

\* Paste there

only. [network] — share name.  
comment

Path = first samba.

Public = /data

available = no

printable = no

valid users = s1am mavi sraj @hr.

\* write list = +hr → optional.

WOW!

Printer → daemon.  
copied

\* To check samba Parameter.

# testparm.

Change SELinux context of Samba shared folder.  
↳ security enhance.

# Chcon -R -t Samba\_Shaue-t /data .  
# ls Recursive. -l dZ /data .

# Systemctl restart smbd

## # Systematization

# Firewall - cmd -- permanent -- add - Service - Start

# Fillowell - end  $\rightarrow$  end of 2007 basin  
 $\rightarrow$  upload out of 2011 basin  
 $\rightarrow$  0.861.891 PPI = 0.861.891

client side

Red Hat Linux

- ① Set host name, ip and yum, and install samba client package.
  - ② And check communication between server and client.

How do access samba shared folder temporarily

- ① # yum install Samba-client -y

② ping 192.168.0.1 [server ip]

③ Subclient //192.168.0.1/network -u user -p password

To check

Scanner have abc {1..10}  $\leftarrow$  make 10 is,  
client is .

## How to mount permanent.

- ① mk blir /Samba
- ② vim /etc/fstab

/192.168.0.1/network /Samba  
L  
server ip

cifs defaults, username = ravi,  
[common interuel] pass = 123 o o.  
file system.

wa!

- ③ mount -o
- ④ df -TH

To check /data is 1s, touch xyz.

## How to give write permission to samba share folder.

On server side :-

- ① # chmod 777 /data
- ② upload config file :- writable = yes.  
# systemctl restart smb

To secure Password:  
[Samba client Password] # vim abc.txt — create file — Type username and password.  
# chmod 600 abc.txt

- ① vim abc.txt  
username = ravi  
password = 123

To encrypt Password.

- ① # glib2-mkpassword-pbkdf2  
give password.
- ② copy password.

③ Paste in vim abc.txt  
Save and quit from this file.

# chmod a+r /root/abc.txt

④ Read fstab file.

1192.168.0.1/network /samba Re cifs defaults,1root/abc.txt

How to access samba share folder over windows machine.

① Set ip and check communication between server and client.

Run popup :- ncpa.cpl  
[Windows+R] cmd

② How to access Samba folder Temporary

Open Run :- 1192.168.0.1

Add username password.

To check:-

③ How to map network drive.

Map network drive.

Drive S:

Folder 1192.168.0.1 / network.

✓

## SYSLOG Server

16/09/19

This service used to store services log over the network. we can store application log, service log, user log, and disc log. It work online and offline both mode and communicate with **tcp** and **udp** both protocol.

### Requirement to configure syslog server

① Set hostname, create IP, and installed Package.

```
#  /etc/syslog  
# (58)  
# daemon
```

config file :- /etc/syslog.conf.

Port no:- 514

\* # yum install usyslog\* -y .

mod it → # vim /etc/syslog.conf .

- uncomment line no. 15, 16, 19, 20

- save and quit .

start the service # systemctl start usyslog

# systemctl enable usyslog

# firewall-cmd --permanent --add-port=514/tcp

# firewall-cmd --permanent --add-port=514/udp,

# Firewall - cmd

-- disable

# Firewall - cmd

-- list-all

### Client side :-

- ① Set hostname, IP and create yum and install package.

# msyslog.

# yum install msyslog\* -y.

- ② And check communication between Server and client.

- ③ And edit config file vim /etc/msyslog.conf

for Particular Service.

authpriv.\*

@ 192.168.0.1  
↳ Serverip

/var/log/secure.

mail.\*

@ 192.168.0.1

/var/log/maillog

for all Services.

\*.\*

@ 192.168.0.1

/var/log/message.

below.

Uncomment it.

\*.\*

@@ monote-host : 514.

} for both Side  
Server and Client

now!

```
# systemctl restart rsyslog
# systemctl enable rsyslog
```

## ntp server

→ Network time Protocol

This service used to synchronise date and time over the network. It works online and offline both mode and communicate with any operating system.

### Requirement:

Package name:- ntp\*

Daemon - ntpd

Config file - /etc/ntp.conf

Port no:- 123

log file - /var/log/ntp.log

### Server Side:

- ① Set IP, hostname, yum, and install Package.

```
# yum install ntp* -y
```

```
# vim /etc/ntp.conf
```

Comment line no: 21 -- 24.

33 :- interface 192.168.0.0 mask 255.255.255.0 nomodify nopeer

wq!

nomodify nopeer

```
# Systemctl restart ntpd  
# Systemctl enable ntpd  
# Firewall-cmd --permanent --add-service=ntp  
# Firewall-cmd --reload  
# Systemctl status ntpd  
# netstat -lunip | grep ntpd.
```

## Client Side.

There are 2 methods.

① graphical

② file method.

① graphical method.

```
# yum install system-config-date -y.
```

# System -config-date.

- checkmark over Synchronise date and time over the network.  
add ntp server: 192.168.0.1 Tab for Synchronise.

- Explore advance option check mark over Speed up initial synchronisation. OK.

```
# Systemctl restart chronyd.
```

```
# Systemctl enable chronyd.
```

```
# Systemctl status chronyd.
```

## ② bind via file method

# vim /etc/chrony.conf

write in bottom.

Server 192.168.0.1 ibusif

↳ Server ip

:wq!

Start the Service.

# systemctl restart chronyd .

# timedatectl {

## DNS Server

NIS Server - not in syllabus

\* Network information

server or system

This service used to centralize user over the network.

This unsecure communicate with same operating system.

Requirement to configure.

① Set hostname, IP or install Package, create yum repository.

# ypserv, #ypbind, #yp-tools

# ypserv - daemon .

by default NIS don't have any Protocol, Port no, config file.  
hence it is unsecure. but we can assign Port no. to secure  
connection.

Check NIS domain name.

Step 1: Set NIS domain name and set id Permision.

g. Create user, apply Password and show user home account.

via 2FS.

4:- Set or create master and slave NIS servers.

5. update database.

```
→ # yum install http:// -y
```

→ to check domain name :- # nsdomainname

→ To create domain name :- `nicdomainname name (example)`

→ To set domain name permanent - # vim /etc/sysconfig/network

Write in bottom  $NISDOMAIN = \text{medium}$

OPTIONAL:- YPSERV\_ARGS = '-P 8081'

way!

To check Port Free or not : #netstat -lunlp | grep 808

# Systemctl restart hypserv

# Systemic enable upsell

→ Create user and apply password.

Create Home account #mkclix | schome

```
# useradd -d /home/user1 user1
```

```
# useradd -d /home/user2 user2
```

→ Apply Password.

→ Show home account via NFS

write:-  
viw /etcexports  
\* (ew) all network.

# exports -r

```
# systemctl restart nfs-server
```

```
# systemctl enable nfs-server
```

```
# systemctl stop firewalld
```

```
# systemctl disable firewalld
```

→ Create master and slave NIS Server.

```
# /usr/lib64/yp/ypinit -m
```

on check your name press y to confirm.

To verify master, to add server in future.

→ on other nis [Slave Server]

```
[user] lib64/yp/ypinit -s server1.example.com
```

→ update database

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

```
# ls
```

```
# make
```

On client side

① Set IP, hostname, create yum and install package.

# ypbind

# yp-tools

and check communication between server and client.

Types of bind method.

How do bind client via NIS Server.

[# yum install ypbind yp-tools -y]

① via CLI

② via GUI

To Bind via CLI # authconfig-tui

Checkmark **via Space \* use NIS**

Next.

Domain :- meal.net

Server :- 192.168.0.1 [Server IP]

OK

To Bind via graphically.

# yum install authconfig-gtk -y

# authconfig-gtk.

# System - config-authentication

## DATABASE NIS

Domain      ~~metu~~

Server      192.168.0.1

Authentication :- Password [nis password]  
apply

To check user bind or not

# getent passwd user,

su - user

How to assign auto-mounting . XXX

# yum install autofs -y

# vim /etc/auto.master  
button

write:-

/home      /etc/auto.misc

# vim /etc/auto.misc

write:- user1

    -rw,soft,intr  
    was!      L  
                soft mounting: 192.168.0.1:/home/user1.

# systemctl

    upstart

    autofs

# systemctl

    enable

    autofs

To login all user

# vim /etc/auto.misc

# \* -rw,soft,intr  
# auto! 192.168.0.1:/uhome/g

restart again.

# systemctl restart autofs.

To, su - user1

check su - user2

Note: add or remove any user just database you update.

useradd -d /uhome/user4 user4  
update database.

## DHCP [Dynamic Host Configuration Protocol]

This service used to assign IP automatically over the network. It works online and offline both mode, and communicate with any operating system. It work on DORA Process.

[Discover often meant acknowledgement] - DORA

### Requirement

\* Set hostname, create IP and YUM.

# dhcpc\*

Daemon :- dhcpcd

Port no:- 67

config file :- /etc/dhcpc/dhcpcd.conf

sample file :- /usr/share/doc/dhcpcd-\*/\*dhcpcd.conf.example.  
↳ R.H.7

/usr/share/doc/dhcpcd-\*/\*dhcpcd.conf.example.  
↳ R.H.6.

log file :- /var/lib/dhcpcd/dhcpcdleases.

on Server Side.

- ① Set IP, hostname and install Package.
- ② edit the sample file.

# vim /usr/shaun/doc/dhcp-4.2.5/dhcpd.conf.example.

copy line no. 47 to 55 [Subnet to ]

⑤ Read config file # vim /etc/dhcp/dhcpd.conf  
and Paste.

Assign all IP to network.

Subnet 192.168.0.0 netmask 255.255.255.0 {  
range 192.168.0.2 192.168.0.100;

# ——

# ——

option routers 192.168.0.1; → Systemip

option broadcast-address 192.168.0.255

default

cau!

# systemctl restart dhcpcd

# systemctl enable dhcpcd

# systemctl status dhcpcd

# Firewall-cmd --permanent --add-service=dhcpcp

# Firewall-cmd --reload

## Client Side

How to bind or access IP via dhcp Server.

There are 2 method ① Command line.  
② file method.

① Command line # dhclient

# ifconfig

Go to server and open config file. To check

## ② File method.

assign ip  
ifconfig.

# cd /etc/sysconfig/network-scripts/

# viw ifcfg-eth0

# → bootproto=dhcp

delete ip [which is already assign] and subnet mask.  
waw!

# systemctl restart network.

# ifconfig.

How to bind ip via mac.address?

## On Server Side

### ① edit sample file.

copy line no:- 45 to 78

(hostdevnum = 3)

### ② edit config file.

Paste in bottom.

write:- - host desktop {

- give address 192.168.0.250; }

waw!

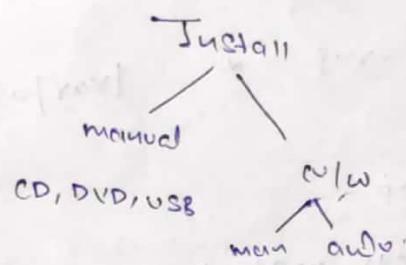
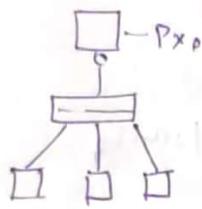
restart the service [dhcpc]

on client side :

# client

Kickstart/pxe servers (WDS in windows)  
↳ Pure executable environment

19/09/19



Requirement to configure.

- ① Set IP, hostname and create yum.

Package :- Ftp/Httpd dhcpc xinetd tftp syslinux

Configure kickstart servers manually.

Ftp/Httpd - To share installation media [img]  
dhcpc - To assign ip automatically.

xinetd - It's a daemon to control tftp server

tftp - Trivial File Transfer Protocol.

\* To boot diskless machine.

syslinux - It's a theme to run background.

# You install httpd\* dnsmasq\* xinetd\* tftp\* Syslinux\* -y

## ① Configure Http Server

- Create document root # mklir [var/www/html] where [Folder name]
- copy the installation media inside this document root  
# mount /dev/sda1 /mnt  
- # cp -rvf /mnt/\* [var/www/html]/www/
- Star the service.  
# systemctl start httpd  
# systemctl enable httpd

Testing:- Open browser # Firefox 8  
Add address: 192.168.0.11 www/

## ② Configure dnsmasq server.

In config file . add.  
# add no-dhcp-interface;  
# allow booting;  
# allow bootp;  
Subnet 192.168.0.0

;

;

;

max

} filename "pxelinux.0";

start the clued server.

### ③ configure tftp

# vim /etc/xinetd.d/tftp - config file.

disable = no

ctrl!

start the service.

# systemctl disable firewalld - optional.

configure tftp boot folder.

- ① copy theme [menu.c32] and pxelinux.cfg under tftpboot folder.

- ② cp /usr/share/syslinux/menu.c32 /var/lib/tftpboot

- ③ cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot

④ # cd /var/lib/tftpboot

- ⑤ make 2 folders # mkdir pxelinux & go inside this folder.

→ cd pxelinux → pxelinux.cfg menu

- copy the kernel and kernel image in pxelinux file

- ⑥ cp /var/www/html/menu/images/pxelinux/vmlinuz /var/lib/tftpboot/

- ⑦ cp /var/www/html/menu/images/pxelinux/vmlinuz /var/lib/tftpboot/

# cd /menu

/initrd.img

/var/lib/tftpboot/  
menu

Asimov

## \* Configure answer file.

```
vim /var/lib/tftpboot/pixelinux.cfg/default.  
timeout 100  
default menu.c32  
menu title #### BOOT MENU ####  
label 1  
menu label ^1) Boot from local  
label 1  
menu label ^2) manual installation file.  
kernel vmlinuz  
append initrd=initrd.img inst. img=http://  
192.168.0.1/mel/ devfs=nomount
```

## \* Configure Kickstart Server automatically.

To configure Kickstart file install

```
# yum install system-config-kickstart  
Once run this command
```

```
# system-config-kickstart → Popup → make some modifications  
# is
```

```
# mkcd /var/www/html/ks  
# cp ks.cfg /var/www/html/ks
```

```
# chmod 0755 /var/www/html/ks/ks.cfg
```

vi /var/lib/firmware/linux-  
cfg/default

- add →

label 3

menu label ^5) ~~W~~ = section 1

Kernel 5) Auto installation

Opposite

Opposed initial school / initialising

inst.ks=4HP://192.168.0.1/

ks/ks.cfg devfs

но нону,

# Systematic

start httpd.

Web server / http / apache

This service is expected to host content over the Web. It works online and offline both mode and communicate with specific and unspecified both protocols.

## Types of Housing

- ① ip based - we can host single site.  
with single IP
  - ② name based - we can host multiple  
site over single IP.

Requirement to configure apache server.

- ① Set hostname, IP, and install yum

Package name :- https://  
classmate :- https://

P config file :- /etc/httpd/conf/httpd.conf

isog660

(OS)

/etc/httpd/conf.d/\*.conf

Port no :- http 80

https 443

log file :- /var/log/httpd/error.log

/var/log/httpd/access.log

document root :- /var/www/html

Note: By default apache read html language and does not support dot html. And for the other language need to install package.

- ② If page name is index.html and store inside the document root so no need to change any thing in config file.  
If any thing change then define this changes in config file of apache server.

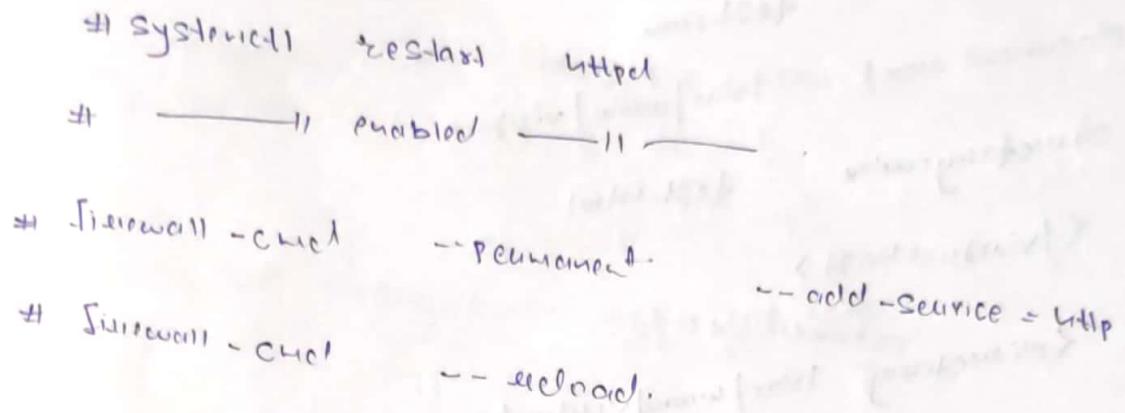
How to host ip based hosting

- ① Install Package and go in the document root

# cd /var/www/html

# vim index.html

Type anything :- This is test  
www.



For testing open browser enter ip name . 192.168.0.1 and check.

For opening with name # vim /etc/host  
→ 192.168.0.1 server1.example.com server1  
↳ fake name .

Run Apache with different Page name and different document root.

① First create document root

# mkdir /var/www/virtual .  
# cd /var/www/virtual .  
# vim test.html

② Edit the config file :-

vim httpd.conf / httpd.conf .

while in bottom:-

```
<virtualhost 192.168.0.1:80>
  ServerAdmin root@Server1.example.com
  ServerName test.com
  DocumentRoot /var/www/virtual
  DirectoryIndex test.html
</virtualhost>
<directory /var/www/virtual>
  require all granted
</directory>
# Systemal restart httpd
# curl -t
```

To check apache syntax : # httpd -t

check page in command line :

```
# curl -o test.html
# curl test.com
# elinks
for this you install elinks
# elinks test.com
```

Run apache in different Port no.

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

change Port no.: 192.168.0.1 : 8961  
Listen 8961  
curl:

Apply this Port changes in selinux manager.

# semodule -l | grep http  
# semodule -I httpd -t http -P tcp 8961  
# semodule -a httpd -t httpd\_t -l httpd

# systemctl restart httpd

To Test :-

domain name: Port no.

# test.com:8961

Open site with user authentication.

Go inside document root create hidden file with name of

# vi .htaccess

AuthName "This is secure site"  
AuthType basic

AuthUserFile "/etc/httpd/.htac"

require valid-user

② Create user and apply password protection on login

```
# htpasswd -c /etc/httpd/new man.  
# cat /etc/httpd/new.
```

③ Add more users

```
# htpasswd -m /etc/httpd/new mani  
# cat /etc/httpd/new.
```

④

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

Server1.example.com

```
<directory /var/www/html>  
allowoverride all  
deny none  
</directory>
```

cug,

⑤

```
# systemctl
```

restart httpd with new id 99?

## Some basic command asked in interview

- ① # diff file1 file2 - To check difference in 2 file.
- ② # diff -q test1 test2 - To check diff in 2 folders.
- ③ # lprm -qo | grep lib\* > lib.txt - 1 Server  
# lprm -qo | grep lib\* > lib2.txt - 2nd Server.  
# SCP lib.txt root@desktop:/root - To Take This file into 2nd server
- # diff lib.txt lib2.txt > result
- # cat result.

"<" - For 1 file

">" - For 2nd file.

How to set environment variable in Linux

/etc/grub2/grub.cfg - when  
/etc/grub.cfg - when

24/09/19

Hostpage with different document root and different language.

```
# cat /var/www/html/index.html
# mkdir -P /srv/java/data
# cat /srv/java/data/index.html
# vim test.html index.php
# yum install php* -y
# vim index.php
- This is PHP Page
```

→ Go inside config file.

```
# vim /etc/httpd/conf.d/vhost.conf
<VirtualHost 192.168.0.1:80>
    ServerAdmin root@Server1.example.com
    ServerName www.php.com
    DocumentRoot /srv/java/data
    DirectoryIndex index.php
</VirtualHost>
<Directory /srv/java/data
    AllowOverride All
</Directory>
```

```
# systemctl -- -- reload
```

# viw /etc/hosts

- 192.168.0.1 php.com

Change SELinux context

# chcon -R -t httpd\_sys\_content\_t /var/java/data

# ls -ldz /var/java/data/  
drwxr-xr-x 2 root root 0 context.

Restart the service httpd.

Host website with secure [https]

Requirement to configure https server.

Package :- # mod\_ssl — for security  
name or # httpd. } install both.

Config file :- /etc/httpd/conf.d/ssl.conf

daemon :- —

Port no:- 443

# yum install mod-ssl\* httpd\* -y

→ generate or create certificate.

# cd /etc/pki/tls/certs

# ls

# make web.crt → public

Fill form.

```
# mv webKey private ..|private.  
cd ..|private/
```

→ edit the config file .ini in /etc/nginx/conf.d/ssl.conf.

100, 10 # change key name and certificate.

```
# Systemctl restart httpsd.  
# systemctl status httpsd.
```

For testing open browser.

Add exception - get certificate.

# Shell Scripting

- Series of command written in Plain Text file

## Types of variables :-

What is variable :-

It's a symbolic name and represent value stored in memory in any command or any shell.

Types:-

- ① SDV - System define variable
- ② UDV - User define variable.

SDV - This type of variable always in capital letter, create and maintained by Linux itself.

UDV - This type of variable always in shell letter, create and maintained by users.

To check :-

#env or #printenv

How to set variable :-

#x=1

#echo \$x

To set permanent

#set x=1

#env

To unset

unset x

## About the Quotations.

- ① " → anything enclosed inside double quotation change  
or shell char except of backslash(\) and \$ (dollar)  
\\ and \$
- e.g.: #echo "Today date is \$(date)"
- ② ' → Anything enclosed inside single quotation print as it.
- #echo 'Today date is \$(date)'
- ⑤ ` → To execute any command.  
(back quote)  
# echo my name is `whoami`

## Arithmetical Operators.

① #expr 2 + 2

#expr 2 - 2

#expr 2 / 2

#expr 2 \\* 2 - for multiplication.

x = 2 y = 4

#echo sum of x and y is `expr \$x + \$y`

## Exit and Status code.

0 means success

1 to 255 means specific error code.

126 means not executable file.

127 means no such command.

128 or > 128 signal.

To check status code. # echo \$?

How do write a script?

① Create a file any name with .sh extension.

# vim new.sh (optional)

Script:-

#!/bin/bash

Clear

echo " welcome to mead naf"

# chmod a+x new.sh

To run the script:- # sh new.sh or # ./new.sh  
# bash new.sh [compulsory param]

Read Statement

use \$ to get input from keyboard and store to variable.

Syntax :- read variable<sub>1</sub>, variable<sub>2</sub>

Script:-

```
echo " Your Name"
read name
echo "Hello $name"
```

**if**

## Condition :-

### ① **if** :-

```

echo "give any input"
read name

if [ $name = "medhat" ]
then
    echo "fedora"
elif [ $name = "fedora" ]
then
    echo "input file not found"
fi

```

## SED - Stream editor

→ This command used to change content from any file who go inside that file.

To delete Particular line.

```
# Sed '3d' test
```

```

# Test
!
medhat
Linux
unix
!
```

To remove Permanent or save it.

```
# Sed -i '3d' test
```

To remove last line.

```
# Sed -i '$d' test
```

\$ → Last line.

To delete from ranges

# Sed '2,4d' test.

To remove line no. 2 and 4.

# Sed '2d;4d' test.

To not delete ranges of the line.

# Sed '2,4!d' test.

To remove or delete line starting with Particular character

# Sed '/^J/d' test.

To remove or delete line ending with Particular char.

Sed '/u\$/d' test.

To remove case sensitive Pattern.

# Sed '/[uv]\$/d' test

# Sed '/^v/v/d' test

To remove blank line.

# Sed '/^\$/d' test.

## Awk Example - I

Awk is a most powerful utilities used in unix o.s. so whenever it come do text file select and Awk command mostly used. Awk comm. used to read file and split the content.

Syntax:- In column:-  
# awk '{print \$2}' test

vim test

O.S. name.

w/o header record:- # awk '\$NR!=1 {print \$2}' test

[Server Side] **Scsi 8 iscsi** [client side]  
[initiated.  
[small computer system interface]

This service used to share block based storage over the network. It works online, offline both mode. It's a secure protocol authenticated with any operating system.

## Requirement:-

- ① set hostname, create IP and yum.

RHEL 7:-

Package name:- targetcli  
daemon :- target

config file:- /etc/target/saveconfig.json

Port no :- 3260

log :- /var/log/dmesg

RHEL 6 :- Package name :- scsi\*.

daemon :- tgtd.

Config file :- /etc/tgt/taugets.conf

Port no and log file same.

On Server Side.

- ① install Package # yum install targetcli -y
- ② create Partition share via scsi
- ③ #targetcli

/> backstores/block create disk /dev/sda4

- ④ create or generate iqn name [ initiator qualifier naming ]  
/> iscsi create iqn.2019-10.com.example:target1 [vany]

- ⑤ To generate key .

/> iscsi/inqn.2019-10.com.example:target1/tgt1/acts create iqn.

2019-10.com.example:cl1

- ⑥ To create luns [logical unit no.]

To map backstore and isci

|> iscsi/igu. 2019-10.com. example: target1/ttgt1/luns create

|backstores|block|disk

⑦ To create portals.

|> iscsi/igu. 2019-10.com. example: target1/ttgt1/portals create  
192.168.0.1 [Server ip]

⑧ To save configuration.

|> saveconfig.

|> exit

To start the service and enable it

Add service in FirewallD status

# firewall-cmd --permanent --add-service=iscsi

# firewall-cmd --reload

On client side

① Set hostname and ip and check iscsi package should be installed.

# rpm -q iscsi

## How to discover luns

```
# iscsiadm -m discovery -t st -p 192.168.0.1  
    ↗ same target.  
    ↘ Target  
    ↘ Type  
    ↘ Portas
```

## How to login

To login Shared disk assign acl permission over client mc.

```
# vim /etc/iscsi/initiatorname.iscsi — need this file.  
Initiatorname = iqn.2019-10.com.example:acl — change and edit.
```

```
# systemctl restart iscsi
```

```
# systemctl restart iscsid.
```

```
# --enable iscsid
```

```
# --enable iscsi
```

```
# iscsiadm -m node -T iqn.2019-10.com.example:target1 -l  
    ↗ mode.  
    ↗ Type.  
    ↗ login
```

To check disk status:

```
# dmesg
```

Create Partition. Format and mount it.

To mount Permanent.

(Sdb1) /test

Inside vim /etc/fstab.

/dev/sdb1 /test ext4 -nodev 0 0

# cd /test - touch abc{1..10}

# dmesg

## How to delete

# umount /test

# vim /etc/fstab - delete

# iscsiadm -m node -T iqn.2019-10.com.example:target



To log out.

# \_\_\_\_\_ ll \_\_\_\_\_ -o delete -fso  
Filesystem

Permanent

## ftp servers

This service used to upload and download content over the ftp server.

It works online and offline both mode.

It's unspecific Protocol. root user can not login by default to ftp server.

Type of Tool or command To upload & download.

① ftp, lftp, sftp, wget, wput, filefox. - by default in linux.

③ winscp filezilla - 3rd Party.

Requirement to configure ftp servers

① Set hostname, ip and create yum.

Package name:- ftp

vsftpd -

daemon - vsftpd.

config file - /etc/vsftpd/vsftpd.conf.

user authentication file → /etc/vsftpd/ftptrusers

/etc/vsftpd/users\_list

Port no:- 20 and 21.

log file :- /var/log/xferlog

document root:- /var/ftp/pub

Note :- When we install Package automatically create user with name of ftp / anonymous , by the help of this user we can only download not upload .  
by the help of normal user we can upload and download both , for upload we need to give the permission .

on Server Side .

① IP, hostname and package

yum install ftp\* vsftpd\* -y

② go into document root # cd /var/ftp/pub /

create 2 folder

# mkdir

download upload .

# touch download /abc {1..10}

# chmod 777 upload .

# systemctl restart vsftpd

# --> enable vsftpd .

```
# firewall-cmd --permanent --add-service=ftp
```

```
# firewall-cmd --reload
```

On client side.

① IP, hostname and yum made and install Package.

```
# yum install -y ftp
```

How to login ftp via ~~normal user~~ anonymous user.

```
# ftp 192.168.0.1
```

↳ Server ip

Name :- anonymous / ftp

Password :-

Login successfully.

ls

```
# cd pub
```

```
# cd download
```

```
# ls
```

How to download.

```
ftp > get abc1
```

```
# ls
```

To download multiple file.

ftp > fgeli > mget abc1 abc2 abc3

To off interactive mode.

ftp > prompt [interactive mode off and on again]

To change downloading Path.

ftp > lcd /tmp

ftp > get abc1

How to login ftp via command also.

On Server Side : - create user and apply Password.  
# useradd man  
# passwd man

On Client Side.

# ftp 192.168.0.1  
man

How to allow root to login via ftp.

On Server Side

1) vim /etc/vsftpd/fpusers - comment root.

2) vim /etc/vsftpd/user\_list - comment root.

"erase root" - comment root.

vim /etc/vsftpd/vsftpd.conf  
 To only allow particular user  
 -allow  
 -deny  
 || or deny.

ftp 192.168.0.1

ftp > bye.

## How to upload

On Server Side.

- ① edit vim /etc/vsftpd/vsftpd.conf
  - Line 29 and 32 uncomment `anonymous_enable=NO`
  - ② allow this changes in selinux booleans
  - ③ `getsebool -a Igneep ftp`
  - ④ `setsebool -P ftptd_anon_write on`
  - ⑤ `setsebool -P ftptd_full_access on`
  - ⑥ `systemctl restart vsftpd`
- } Time Taken

On Client Side.

login via user

ftp > # ls

ftp > # cd upload.

ftp > put test.

To check.

Server side :- cd /var/ftp/pub/upload  
test.

How to change banner

on Server Side

① Edit config file vim /etc/vsftpd/vsftpd.conf

86:- ftpd-banner = welcome do Stp server  
wq!

start the server service.

② On Client Side

ftp 192.168.0.1.  
ftp >

Vim /etc/vsftpd.conf

On Client Side.

1ftp

Login yum install vsftpd -y.

1ftp 192.168.0.1

by default login via anonymous user.

→ How to login Particular user.

```
# lftp user@192.168.0.1
```

```
# cd /var/ftp/pub
```

```
ls
```

## SFTP -

This command also used to download and upload content over the server. It works on RSA Fingerprint. This is a secure protocol. by default most user login via SFTP.

```
# sftp user@192.168.0.1
```

```
# rm -rf /root/.ssh/
```

```
# sftp user@192.168.0.1
```

## wget -

```
# wget ftp://192.168.0.1/pub/download/abc1
```

```
# wput ftp://192.168.0.1/pub/upload/abc2
```

```
{ # file for &  
  ftp://192.168.0.1 }
```

## SCP - Secure copy

This comm. used to copy data from one host to other. It uses protocol and work over RSA fingerprint.

```
# scp -r /data root@192.168.0.2:/tmp
```

on client

```
scp -r root@192.168.0.1:/data /root
```

or

## rsync - remote Synchronization

This comm. used to copy data from one host to other. It copy data in incremental form. It also work over RSA.

Fingerprint

```
rsync -avh /data /root@192.168.0.2:/root
```

```
# rsync -avh root@192.168.0.1:/data /root
```

mysql/mariadb

[RDS]

[Relational database system]

This is a relational database service, that allow the data to store in a organised way. It's open source service, control by mariadb daemon.

Requirement to configure.

① Set hostname, IP and create yum.

Package name:- mariadb

Daemon:- mariadb

Config file:- /etc/my.conf

Port no:- 3306

Protocol:- tcp

Service name:- mysql

On Server Side.

# yum install mariadb\* -y

# Start the Service and aim Firewall.

# systemctl restart mariadb

# ---|| enable ---||---

firewall = mysql.

nest -tulip | grep 8306

configure database password.

# mysql -secure-installation.

Yes all

How to login database.

# mysql -u root -p

To check database.

> show databases;

> use mysql — To go inside database.

To check Tables.

> show tables;

To check content.

> describe Tablename;  
(Severally)

How to create user

> create user name@localhost identified by 'password';

> Select host,

## How to Take backup.

# mysqldump -u root -p mysql > /root/test.dump

To Take all database backup.

# mysqldump -u root --all-databases > /root/test.dump

To store the content

mysqldump -u root -p mysql > /root/test.dump

Inside database

> source

/root/test.dump

## Mail Server

3/10/19

This service is used to send mail from one host to other.  
It works online and offline both mode. It's a service.  
It can communicate with any O.S.

### Types of

#### mailing teams used by mail server

① MTA - mail Transfer agent

This mailing team responsible to send mail from one host to  
other.

Type of MTA :-

- ① Postfix
- ② sendmail
- ③ dovecot
- ④ mucube
- ⑤ squirrel }
- ⑥ zimbra GUI based

② MDA - mail delivery agent

This mailing team responsible to deliver mail from one host to  
other.

Types of MDA.

- ① POP / imap [Post office Protocol]
- ② POP3 / imaps [internet msg authentication protocol]

Diffrn b/w POP/imap or POP3/imap.

POP/imap

POP3/imap.

- ① It works online and offline mode.
- ② It's unsecure protocol.
- ③ Data stored in local storage.  
e.g. outlook
- ④ Port no:- 110  
imap - 143
- ⑤ Data stored over server side.  
e.g. gmail, yahoo.
- ⑥ Secure protocol.
- ⑦ It's secure protocol.
- ⑧ Data stored over server side.  
e.g. gmail, yahoo.

④ Port no:- 995  
imap - 993

④ Port no:- 995  
imap - 993

⑤ MUA

- mail user agent.

This mail terms responsible to select and receive the acknowledgement.

Types of MUA

① CLI (MAIL client)

② GUI (thunderbird) (not in default) and partly

Note:- In version 6 and 7 by default Postfix MTA is configured

In R.H 5 and older version by default sendmail

MTA is configured.

## Requirement to configure Postfix MTA

Set hostname, IP and create yum.

Package name :- Postfix.

daemon :- Postfix

Config file :- /etc/postfix/main.cf

Log file :- /var/log/maillog

Protocol :- Smtp Port no:- 25.

### Server side.

① Set host name, IP and install package.

# yum install postfix -y

② Edit config file.

vim /etc/postfix/main.cf

Line no:- 75 myhostname = server1.example.com  
83 mydomain = example.com  
99 uncomm my origin.  
116 common  
118 uncomm.

allow for all deny only localhost

119 → inet-Protocols = all

264. mynetwork = 192.168.0.0/24, 127.0.0.0/8

wow!

③ # systemctl restart Postfix

# ——|| enable ——|| new alias

④ # firewall-cmd

— permanent — add-service = smtp

# firewall-cmd

— reload,

## How do send mail

# mail

-v

root@Server1.example.com.

EOT

# mail

Send and receive mail via mutt command.

# yum install mutt

# mutt

## LDAP Server

Light weight directory access protocol.

This service used to authenticate user over the network.  
It works online and offline both mode and communicate  
with same and different O.S.

### Requirement to configure LDAP

① Set hostname, IP and yum.

Package name :- openldap

daemon :- slapd

config file :- /etc/slapd.conf

log file :- /var/log/message

or

/var/log/secure.

Port no :- 389.

② # yum install openldap\* -y

③ generate ldap password for authentication.

# slappasswd .

copy password .

③ edit the config file.

cd /etc/openldap/Slapd/cn=config

How to upload a folder  
on client.

Mkdir mohit  
FTP 172.25.8.11

anonymous.

Pwd

cd pub

cd upload.

Put mohit.