

structure

/

/boot

kernel, initrd, bootloader and its config

/root

/home

/bin (binary)

user commands (general commands)

/sbin (system binary)

system commands (administration commands)

/lib (library)

shared libraries & kernel modules

/opt (optional)

third-party applications

/tmp (temporary)

/etc (etcetera)

host configurations files

/dev (device)

/mnt (mount)

peripheral devices

/media

/var (variable)

log server, print server, web server, mail server, cache server, client cache, a few application caches,...

/usr (user)

non-essential executable program struct of usr look like / and important next to /

/proc (process)

window to kernel

/sys (system)

window to kernel

0.1 file

every file have code named inode#

0.2 user

every user have code named UID

0.3 group

every group have code named GID

0.4 processor

every process have code named PID

Commands

ls

ls command use to see all existing file in directory an you can make it optional with any switch

-a

this switch show you all of file in directory even hidden file

-i

show inode of files

-l

this switch show you file with more detail such as (type,user,group,size,modified date)

any type of file:

regular file:-

directory: d

short cut (symbolic link, sym link): l

socket: s

pipe: p

special device-character: c

special device-block: b

you can filter search by *

mean zero to infinity character

?

mean one character

[character]

mean special character

[!character]

mean not special character

[a-z]

mean a range of character

[!a-z]

mean not in range character

arg1,arg2,...

mean exactly same as every argument

pwd

show to you current directory address from root

whoami

show your user

cd

cd use for change directory

-

change between two last address

absolute

cd /fjj/ffs/s/f/f

relative

cd-./dff cd-../dfdff (parent)

rm

delete !rm last rm command run

-r

delete directory with content

-f

no ask question

cp

copy

-r

copy directory

mkdir

make directory

-p

make any directory than not exist mkdir -p/s/sd/d

rmdir

delete directory

clear

clear terminal

mv

move file rename move+rename

file

show type of file

man command

man show you manual of any command and tool to give help

hostname

show hostname

init

init 0

shutdown os

init 6

reboot os

echo

write any thing to any file

echo ' ' >> / /file name
and show variable --> echo &x

echo \$?

if = 0 -> last command excute seccesfully else last command excute failed

echo \$PATH

path of commands

echo \$USER

show user

echo \$UID

user id

echo \$HOME

:

echo \$SHELL

default shell

echo \$OLDPWD

old pwd

vi

use vi to edit of creat text

passwd

change password for users

exit

exit from user

su - name

switch user to name

ctrl (r)+f1,..,f6 or ctrl+alt+f1,..f6

changing terminal

more

in terminal you have no any thing like scroll so by more can see any thing without removing

enter to go to the next line
space to go to the next page

less

like more but you can go up and down again and again and exit with q

nl

count and writh lines

pipe: |

give result of before function and get to next function

cat new.txt | nl | less

semicolon: ;

if gone between to command commands are do like always

ampersand: &&

if a command run successfully them run next command

vertical bar: ||

like or do one of command

```
#(echo in subshell;exit 4)&& echo OK || echo bad exit
in subshell
bad exit
```

touch

make file

```
touch a1 a2 a3 b1 b2 b3 c1 c2 c3
touch a,b,ca,2,3 'wildcard'
```

sort

sort line of file (cat/tac)

which command

tell me which path run ‘command’

-a

tell me all address than run this command

whereis command

give me all path that have ‘command’

info command

information:

useradd/adduser

add regular user
hostname >>/>
date >>/>
dmesg >>/>

userdel

delete user

groupadd

add group

cat

show file text

-n

like cat file | nl

alias

save long command to variable

unalias

delete alias

meta character

*

?

[character]

[!character]

[a-z]

[!a-z]

arg1,arg2,...

df

show storage partition

-h

show storage partition

-hT

show type of partition

-i

show inodo if partitions

lsblk

show hard devision

fdisk

make partition

mkfs

formating a partition

mount

mount a directory to hard

umount

un mount a directory

-a

mount every partition in fstab file that added new

history

show command history !5 run fifth command from top !-5 run fufth command from down !!/-1 run last command !p last command that start with p

 history -d 149 delet line 149

 history -c clear all history

 history -w after -c

tune2fs

about partition

-l

make list propertis of a partition

grep

filter a text by a keyword

mkswap

make partition swap after choosing filesystem linux swap

 mkswap /dev/name

swapon

make swap on

 swapon /dev/name

swapoff

make swap of

uname -a

kernel version

du -csh /addres

list disk usage of addres physicaly

chmod

change permission
with cahr num of — reference -----
u — g — o
——a——
chmode o+w file name

chown

change owner

-r

do to all child file

:

chgrp = chmod :

chgrp

change group

newgrp

change principle group

stat file

status of file

umask

set default permission but woeek inversly

find

find [addres] -[option] [variable]
find / -name '*mp3'
find / -user ali
find / -qroup it
find / -perm 0400
find / -size +10M
find / -size -500M
find / -mtime -7
find / -atime -2

```
find / -ctime -14
find / -mmin -60
find / -amin -60
find / -cmin -30
find / -size +10M -size -50M
    find / -mtime +7 -mtime -14
    find / -amin +30 -amin -60
find / -type d -name test in double coutation
    find / -type f -name
find /tmp -name name -user ali -group it -perm 0400 -size +40M
    2> /dev/nul in end command not show you error
    exec rm -f at the end of file delete all founded or any command
    find / -lname for sym link
    find / -samefile for link
    find / -inum number for link by inod
```

expr

do math equation

bash

open new bash

ps

show maked bash

mail

make email and can send to another user and can be read by mail commands
male ali: mail to ali

reset

reset the terminal and fix some bugs

gzip

zip the file
-d || gunzip to unzipping
show with gzip

bzip2

compress better usually
-d || bunzip2 to unzipping
show with bzipcat

tar (tape archiver)

-f filename (file)
-c (creat)
-x (extract)
-t (test)
-C path (destination)
-v (verbose)
tar -cf ./gooni.tar ./m*
-z (gzip, gunzip)
-j (bzip2, bunzip2)
tar -czf gooni.tar.gz filename
tar -zxf gooni.tar.gzcat
tar -cjf gooni.tar.bz2 filename
tar -jxf gooni.tar.bz2

time command

show time to execute totally a command

wget link

download from link

sleep

sleep 5
delay for five second

seq

seq 1 10
write one to ten in order

any thing

/etc/group

list of all group

/proc/swaps

list of swaps

/proc/meminfo

list of memory

/proc/cpuinfo

information of cpu

/proc/version

version of linux

/etc/passwd

name of all user maked user exist an 1000 to up

/etc/fstab

file of partition mount

/dev

partition

/dev/null look like black hole

/dev/hda,b,c,... IDE (PATA)

/dev/sda,b,c,... (SCSI)

/dev/sda,b,c,... (SATA)

/dev/sda,b,c,... cool disk

file of variable

.bash-profile underline instead minus

/.profile

/.bashrc

/.bash-logout

vi app

basic text editor in any linux

i

go to the insert mode

I

like i just go to the first of line

shift+r

go to replace mode repalce new to old char

esc key

back to basic mode

:

go to command line

q/q! => quite from vi
w/w! => save text /fours save
w /addres name=> save as
n/n! => open next file
e/e! /addres name=> open file in addres/open force
r /addres name=> write file in this file
x/ZZ => save and quite
every bash command => ...
set nu => set nummber to any line
nummber => go to line number

v

go to visual mode

o

open new line and go to insert mode

O

open new line before curser and go to insert mode

hjkl

left down up right

$$3j = j+j+j$$

H,L,gg,G

H go to first line of page

L go to last line of page

gg go to first of file

G go to last line of file

w,b

w go to next word

b go to before word

Ô \$

Ô go to first of first word of line

0 go to first of line

\$ go to last of line

ctrl+f,ctrl+b

f go to forward page

b go to back page

x,X

x delete from front of cursor

X delete from back of cursor

s,S

s delete one char and go to insert mode

S delete one line and go to insert mode

dd

cut total line

7dd cut 7 line

d num jahat

cut number type jahat

c

like d them go to insert mode

cc

like dd then go to insert mode

y

copy to clip board

yy

copy total line to clip board

p,P

p past to right of curser

P past to left of curser

search

/word

?word

n down

N up

u,ctrl+r,.

undo

redo

repatate last command

partitioning

cable connection

partitioning fdisk

chossing filesystem

format mkfs

mount mount!=unmount

to view df -h

partitioning method

1- MBR Schene (MSDOS Style)

Master Boot Record —> 512B

2- GPT Scheme

GUID Partition Table

MBR

max 4

if primary = max 4 extended=n/a logical=n/a if primary = 3 extended= max 1 logical= max 11 extended partition cant store data and contain logical partition

filesystem

native — ext2,3,4,btrfs,reiserfs

non-native if

 with modules — XFS,ZFS

 withouen module — APFS,NTFS

cross-platfor — FAT12,16,32,iso9660,CDFS (joliet)

small partition <= 2TB < large partition

virtual memory

windos page file

linux swap

 with LRU algorithm (least Recently Used)

free -h

show your swap

dd if=/dev/zero of=/root/myswap bs=500M count=1

make 500M free of / partition and named myswap

 then with mkswap /root/myswap and swapon /root/myswap add it to main swam

link

hard link / link

make with ln filename linkname

 like backup

 look like pointer to inode

 not work in diffrent partititon

symbolic link / sym link

make with ln -s filename linkname

 this link look like shortcut

variable

system var: usually capital

two module

local var — v = any
environment var — export v = any
variable in linux:
question sign (last command)
PATH (addresses of commands)
USER (user name that login)
HOME (address of home)
SHELL (address of bash)
PWD (save address of current directory)
OLDPWD () work with cd -
HISTSIZE (500 last command)
MAIL (address of file than save email of user)
HOSTNAME
LS (underscore sign) COLORS
\$ current shell PID
PPID current shell parent PID
PS1 file of text than in terminal showed before every commands

ps1 code:

u user
h computer name
H hostname
d date
t time
w total current address
W last current directory
n new line
\$ user type sign
e color code
.....
env list of total environment variable

user defined var: usually small

Man Pages:

- 1.user commands (general commands)
- 2.system calls
- 3.library class
- 4.
- 5.config files
- 6.games 7.miscellaneous
- 8.system commands (administration command)

9.kernel routines
all in /usr/share/man/...
whatis fdisk
apropos partition
fdisk –help (with all commands)

text processing

work with delimiter
set delimiter
cut -d double quotation and delimiter -f 1 to -3 /etc/passwd ; u3 cut -d double quotation and one char -f 1,3 /etc/passwd
-f field
head file
head default=10 line
head -5 file name
tail like head
tac or head -n
expand command change tab to space default 8 and you can use -t 5 to five space
unexpand change space to tab
od -tc/tc file name show tab or space and total char
sort
-r reverse
-n sort numeric
-k 2 with field 2
wc line/word/char number
-l -w -m -c -byte
uniq filename del repeated line
-d print repeated line
-D print repeated line and count of repeated
-c count of repeat
join file1 file2 one column must be same as another file
join -1 3 -2 4 file1 file2 join with another column 3 in file one and 4 in file two
paste write file one them filetwo in row
-d and double quotation can use delimiter
split -num filename name of new file
default 1000line
split -b 4.7G file name file
cat file1 file2 show file2 after file1
rev reverse in every line
tac revers in total of file
tr a-z A-Z if a them A just standard entry
receive operator ;
xargs in standard entry and write all of file in one line

ls /home 1;filename 2;filename/&1 pipe one
 tee command like three way on input two out put that on of always file and
 another is terminal of pipe
 tee -a append text
 grep anything
 grep -v none have
 grep -i case insensitive
 grep -n line number
 or sign char at the first of line bee char
 & char at the last of line be char
 jword just word total in countation
 [abcd] [a-b]
 or sign in brace mean not these char
 .show lines than not null or just enter

Processes

spawn
 -PID
 -lifetime normal exit or abnormal exit
 -UID
 -GID
 -Parent Processes
 -workingdirectory
 -environment
 -...
 ps show process
 -A (all)
 -e (all)
 -a (attached processes)
 -f (forest mode) ps tree -h/-p
 -w (wide output format)
 -l (long format)
 -u (user format)
 -x (background processes)
 -C command (special commands)
 -U username (User command)
 most useful
 ps -aux
 ps -ef
 ps -el
 top like taskmanager and put space lead to refresh bar (default 3s)
 uptime show some details like time uptime upusers load avg
 d change delay
 k kill a process
 kill -l list of signals

```
SIGHUP reload 1
SIGINT interrupt,cancle 2 ctrl+c
SIGKILL kill 9
SIGTERM terminate 15
SIGCONT continue,unfreeze,unpause 18
SIGTSTP stop,freeze,pause 20 ctrl+z
kill -15 PID#
kill PID# default -15
kill -9 PID PID PID PID PID
killal vi
NI (nice of process) priority of process between -20 to +19 and +19 wors
priority and -20 is the best just super user can lower priority
nice -4 vi myfile
nice -vi myfile
renice in during the process change priority
renice 9 PID
renice -9 PID
tail -f show last of file and live it
du -csh /var
du -cs /var
du -sh /var
du -ch /var
jobs -l running command
fg num run one of those to foregrand
bg like fg but run in back ground
& at the last of command lead to command run in background
nohub anycommand & keep running after logout
```

useradd

```
swithc
-d new home dir addres
-m make address than is up in disk
-g name of principle user group
-G name of subordiner user qroup
-s address of excuring default shell
-u user UID
-c command of discription
usermod -L name
usermod -U name
passwd -l name
passwd -u name
cshs to chang shell
```

login

```
1
    su - ali login mode
    su ali non-login mode
    /etc/skel/ files are copied to any when an account is made
    /.bash (underline) profile 1 3 no execute in none login mode
    /.bashrc 2 2
    /etc/bashrc 3 1
    number is order of read and do
    .....
    /.bash (underline) logout
    su/su -empty switch user to root
    visudo like vi /etc/sudoer
    visudo of vi /etc/sudoer in this file can change accessibility of another user
    and user than in sudoer file can be like root and log be save its activity
    in this file % before name mean its group not user
    in some linux root have no password with sudo su - root and then change
    root password
    useradd -u 500 newusr if before exists an user with UID 500 and we delete
    it and want to get this user to new user use this command
    userdel -r name delete user and home directory
    groupdel name
    pwunconv deactivate shadowing grpunconv
    pwconv activate shadowing grpunconv
```

boot initialisation and shutdown

BIOS

(Basic input/output System)

- hardware clock (CMOS battery)
- software clock
- CHS (sylinder/head/sector) LBA (logical block addressing)

EFI

UEFI

MBR

(master boot record)

512 B

- 446 B (bootloader information)
- 64 (partition table information)
- 2B (MBR validation check)

most famous bootloader in linux

1. LILO (linux loader) lilo /etc/lilo.conf
2. Grand unified bootloader (GRUB legacy) grub /boot/grub/menu.lst /boot/grub/grub.conf /etc/grub.conf
3. GRUB2 grub /boot/grub/grub.cfg /boot/grub2/grub.cfg /etc/...

initrd is a file than kernel need to it to prevent detectiv loop

```

bootloader
kernel
init
runlevel
    init and telinit to change runlevel
    init 0 shotdwon
    inti 1 single user mode
    init 2 multiuser -nfs -x11
    inti 3 multiuser +nfs -x11
    init 4 unused
    init 5 multiuser +nfs +x11
    init 6 reboot
    we cant use init 0 or 6 in default
    usualy default is 5 or 3
/etc/inittab
    runlevel command show before and now runlevel N mean shud down and s
mean single user mode
    unused runlevel work like before runlevel init 4 = init 3
    startx up graphic sevise manual withot use init 5
    service web ssh database dns proxy/cache
    applications apache openssh-server vsftb mysql bind squid
    daemon httpd sshd vsftpd mysqld named squid
    name of script like daemon
    /etc/init.d/sshd stop—start—status—restart—reload—
    /etc/rc0.d
    /etc/rc1.d
    /etc/rc2.d
    /etc/rc3.d
    /etc/rc4.d
    /etc/rc5.d
    /etc/rc6.d
    Snnsshd to start
    Knnsshd to stop
    for start s00 to s99 in priority in /etc/rcc
    also for end
redhat base:
1. LSB: /etc/init.d/sshd stop—start—status—restart—reload—...
2. service sshd stop—...
3. chkconfig
4. systemstl
debian base
1. LSB
2. service
3. update-rc.d
4. systemctl
example for 3

```

```
update-rc.d crond default
update-rc -f dovecot remove
update-rc -f dovecot stop 24 2 3 4 5
```

service managment

```
-System V (SssysVInit) -i init (centoOS 5, older)
    service sshd stop
    chkconfig — update-rc.d
    init 0
-upstart -i init (CentoOS 6)
    initctl stop sshd
    chkconfig — update-rc.d
    init 0
-systemd -i (CentOS 7, newer)
    systemctl stop sshd —i at moment
    systemctl start sshd —i at moment
    systemctl disable sshd -i next boot and always
    systemctl enable sshd—i next boot and always
    systemctl poweroff
    -shutdown command
    shutdown -h now
    shutdown -h 120
    shutdown -r 10
    -h (shutdown, halt)
    -r (reboot)
    -c (cancel)
    -f (fast boot)
    -F (force filesystem check)
```

package managment

1. redhat rpm *.rpm
 2. debian dpkg *.deb
- a-b.c.d-e.f.rpm
a=package name
b=version
c=major release (major revision)
d=minor release (minor revision)
e=build number
f=arch. -i x89, i386, i486, i586, i686 -i 32bit -i x86underline64, amd64 -i 64bit
-i sparc,
-i PowrPC,
-i arm,
-i ...,

```

-i all, noarc (suit for any device)
rpm
  -i (install)
  -u (update)
  -U (install/update)
  -v (verbose)
  -h (hash)
  -e (erase)
  -q (query)
  -a (list all package names installed on this system)
  -f (file)
  -l (list all package files)
  -c (list all package config files)
  which chmod
    rpm -qf /usr/bin/chmod
dpkg
  -i (install) = rmp -i
  -r (remove) = rmp -e
  -s (status, query) = rmp -q
  -S (search) = rmp -qf
  -l (list all installed package) = rmp -qa
  -L (list all package files) = rmp -ql
wrapper
  1.yum (redhat base)
  2.apt (debian base)
yum
  (yellowdog updater modified)
  /etc/yum.conf
  /etc/yum.repos.d/—.repos
  yum update
  yum update appname
  yum install appname
  yum remove appname apt (advanced package tools)
  /etc/apt/sources.list
  /etc/apt/sources.list.d/official-package-repositories.list
  apt -get update
  apt -get upgrade
  apt -get upgrade appname
  apt -get install appname
  apt -get remove appname
  -get is optional

```

shell:

sh, csh, ksh, tcsh, zsh, ... bash, ...

you shold write your command in a text and run it with bash command

```

echo clear
bash a
run file as alone command most use address
addres/a to run
or
vi .bashunderlineprofile
and change PATH (add address of this file)
better named file than have .sh at end
# to comment
#!/shibang addres runner of command so #! /bin/bash
which top
ls -l /usr/bin/top
ls -l 'which top'
ls -l $(which top)
these command are equal to each other
automatic run in linux in cron service
crontab
-l list
-r remover
-e edit
min hrs dom moy dow cmd these column ser the time of script
15 8 * * * /root/class/myscript.sh these line run than exploitat every day
in 8:15
15 8-10 * * * /root/class/myscript.sh
15 8,17 * * * /root/class/myscript.sh
how work with crone
cronetab -e
write = 53 10 * * * /root/class.myscript.shadowing

```

networt

OSI

client server 1.Application A 2.Presentation P 3.Session S 4.Transport T 5.Network N 6.Data link D 7.Phisical P
physical layer

Wireless wlan0

Ethernet eth0

priority with Ethernet

naming approaches

1-Hostname = computerPunderline name.domainunderline name

www.google.com

mail.yahoo.com

kashani.lpir.org

(org, com, ir) TLD (top level domain)

(google, yahoo, lpir) SLD (second level domain)

www, mail sub-domain name

change hostname in /etc/hostname

```

2-Physycal addr (mac addr)
dhclient (IP, Gateway, DNS)
3-IP Addr
ifconfig eth0 192.168.10.11
default netmasks
-; A:255.0.0.0
-; B:255.255.0.0
-; C:255.255.255.0
ifconfig eth0 192.168.10.11 netmask
1111111.11111111.11111111.11111111.00000000
debian base: /etc/network/interface
redhat base: /etc/sysconfig/network-scripts/ifcfg-eth0
command
ifconfig
ip addr show — ip a
...
ifconfig eth0 192.168.10.11
ip addr add 192.168.10.11 dev eth0
...
ifconfig eth0 down — ifdown eth0
ip link set eth0 down
...
ifconfig eth0 up — ifup eth0
ip link set eth0 up
...
route -n
ip route show — ip r
...
route add default gw 192.168.10.1
ip route add default via 192.168.10.1
ssh (22)
client ——; server A ——; server B
openssh-clients openssh-server (22) openssh-clients openssh-server (22)
1.remote console
ssh username@IP
2.secure copy
scp usesrname@IP:path username@IP:path
for each user that i write in command in terminal can write no username
and just write address

```