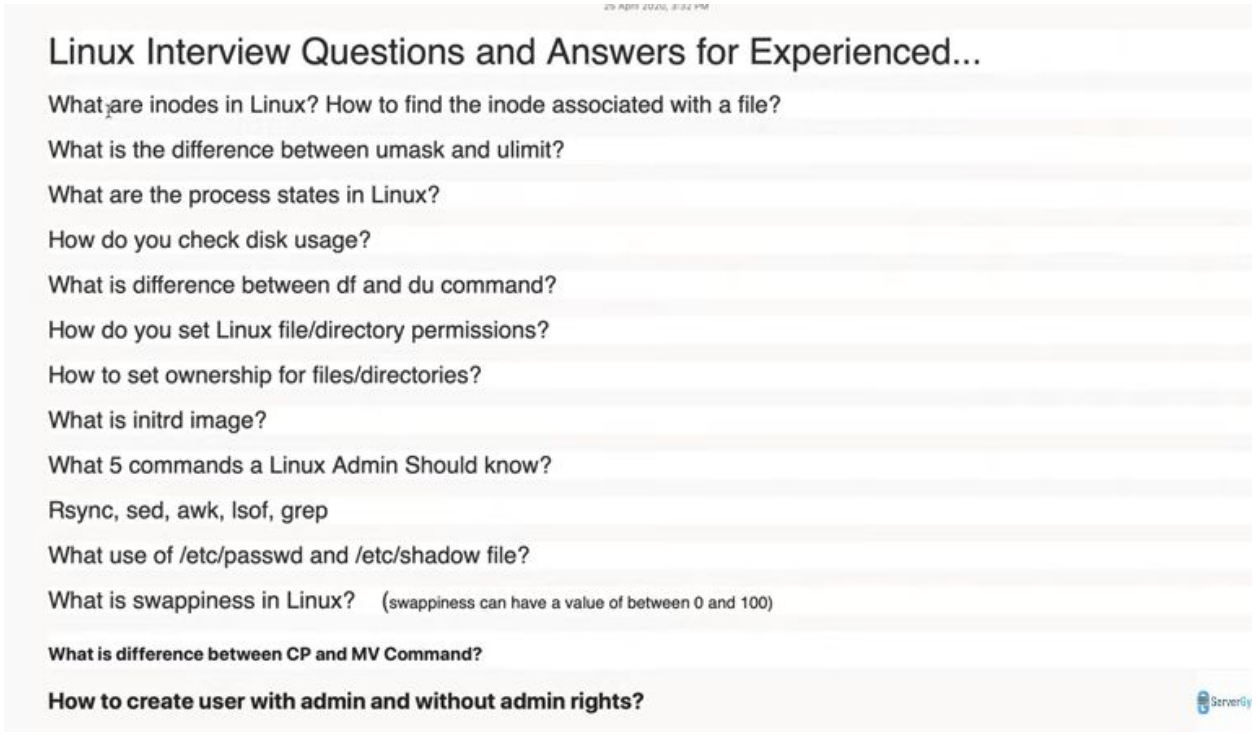


Inode is the random number also it contains two things Data and data of data ,an inode contains a lot of things like file size,permission,data and other details except filename if inode number deleted file name also delete automatically because filename indexing to the inode random number.

```
root@ip-172-31-47-67:/home/ec2-user
[root@ip-172-31-47-67 ec2-user]# ll
total 8
drwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
drwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
[root@ip-172-31-47-67 ec2-user]# ll -li
total 8
159017 drwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
158948 drwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
[root@ip-172-31-47-67 ec2-user]# touch suraj.txt
[root@ip-172-31-47-67 ec2-user]# ll -li suraj.txt
22007 -rw-r--r-- 1 root root 0 Apr 26 09:14 suraj.txt
[root@ip-172-31-47-67 ec2-user]#
```

Umask and ulimit

Umask is related to file and directory permission

umask 000 means full permission and umask 777 means we are revoking the full permission

By Default 0022

```
[root@ip-172-31-47-67 ec2-user]# umask
0022
[root@ip-172-31-47-67 ec2-user]# ulimit
unlimited
[root@ip-172-31-47-67 ec2-user]#
```

t

•When we create any file using touch, cat or vi commands they get created with default file permissions as stored in umask **(User file creation mask).**

•umask is a 4 digit octal number which tells Unix which of the three permissions are to be denied rather than granted.Umask will decide that what should be the default permissions for a file and directory when it is created **•The default umask value is 0022**

Calculation of default permissions for file and directory, basing upon the umask value

Note: For a file by default it cannot have the execute permission, so the maximum full permission for a file at the time of creation can be **666** (i.e. 777 -111 = 666), whereas a directory can have full permissions i.e. **777**

```
[root@ip-172-31-47-67 ec2-user]# umask 000
[root@ip-172-31-47-67 ec2-user]# touch xyz.txt
[root@ip-172-31-47-67 ec2-user]# ll xyz.txt
-rw-rw-rw- 1 root root 0 Apr 26 09:28 xyz.txt
[root@ip-172-31-47-67 ec2-user]# mkdir test
[root@ip-172-31-47-67 ec2-user]# ll test
total 0
[root@ip-172-31-47-67 ec2-user]# ls -l
total 12
drwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
drwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
-rw-r--r-- 1 root     root        0 Apr 26 09:14 suraj.txt
drwxrwxrwx 2 root     root     4096 Apr 26 09:29 test
-rw-rw-rw- 1 root     root        0 Apr 26 09:28 xyz.txt
[root@ip-172-31-47-67 ec2-user]# umask 777
[root@ip-172-31-47-67 ec2-user]# ls -l
total 12
drwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
drwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
-rw-r--r-- 1 root     root        0 Apr 26 09:14 suraj.txt
drwxrwxrwx 2 root     root     4096 Apr 26 09:29 test
-rw-rw-rw- 1 root     root        0 Apr 26 09:28 xyz.txt
[root@ip-172-31-47-67 ec2-user]# mkdir test2
[root@ip-172-31-47-67 ec2-user]# ls -l
total 16
drwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
drwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
-rw-r--r-- 1 root     root        0 Apr 26 09:14 suraj.txt
drwxrwxrwx 2 root     root     4096 Apr 26 09:29 test
d--------- 2 root     root     4096 Apr 26 09:29 test2
-rw-rw-rw- 1 root     root        0 Apr 26 09:28 xyz.txt
[root@ip-172-31-47-67 ec2-user]#
```

Ulimit is depend up on no of open file with user specify limit

vi /etc/sysctl.conf

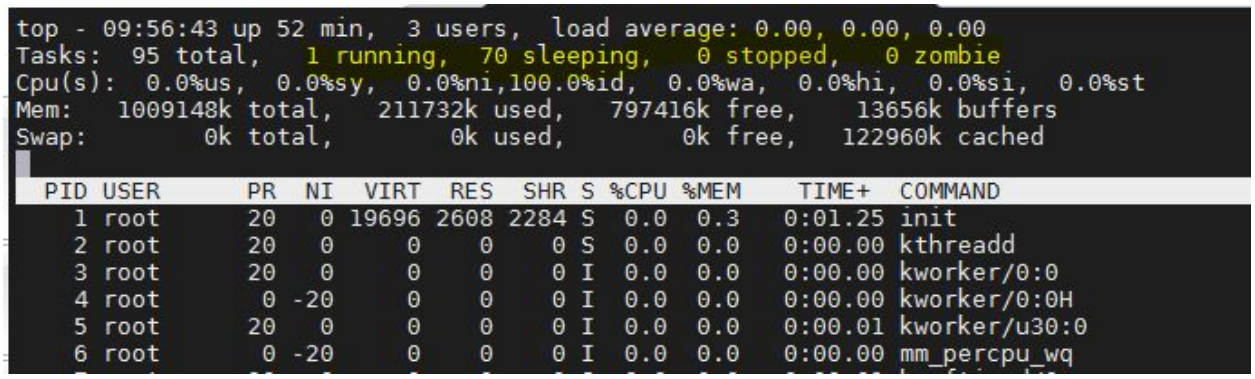
vi /etc/security/limits.conf (soft and hard limit specify to user or group ,we can define domain,type,item,value)

)

```
kernel.shmall = 4294967296
[root@ip-172-31-47-67 ec2-user]# cat /etc/security/limits.conf
# /etc/security/limits.conf
#
#This file sets the resource limits for the users logged in via PAM.
#It does not affect resource limits of the system services.
#
#Also note that configuration files in /etc/security/limits.d directory,
#which are read in alphabetical order, override the settings in this
#file in case the domain is the same or more specific.
#That means for example that setting a limit for wildcard domain here
#can be overriden with a wildcard setting in a config file in the
#subdirectory, but a user specific setting here can be overriden only
#with a user specific setting in the subdirectory.
#
#Each line describes a limit for a user in the form:
#
#<domain>        <type>  <item>  <value>
#
#Where:
#<domain> can be:
#        - a user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
#        - the wildcard %, can be also used with %group syntax,
#                 for maxlogin limit
#
#<type> can have the two values:
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#        - core - limits the core file size (KB)
#        - data - max data size (KB)
#        - fsize - maximum filesize (KB)
#        - memlock - max locked-in-memory address space (KB)
#        - nofile - max number of open file descriptors
#        - rss - max resident set size (KB)
#        - stack - max stack size (KB)
#        - cpu - max CPU time (MIN)
#        - nproc - max number of processes
#        - as - address space limit (KB)
#        - maxlogins - max number of logins for this user
#        - maxsyslogins - max number of logins on the system
#        - priority - the priority to run user process with
#        - locks - max number of file locks the user can hold
#        - sigpending - max number of pending signals
#        - msgqueue - max memory used by POSIX message queues (bytes)
#        - nice - max nice priority allowed to raise to values: [-20, 19]
#        - rtprio - max realtime priority
#
#<domain>      <type>  <item>         <value>
#

#*               soft    core            0
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#@student        -       maxlogins       4

# End of file
```

What are the process states in linux?

1. Running / Sleeping both are same
2. Stopped
3. Zombie
4. Waiting

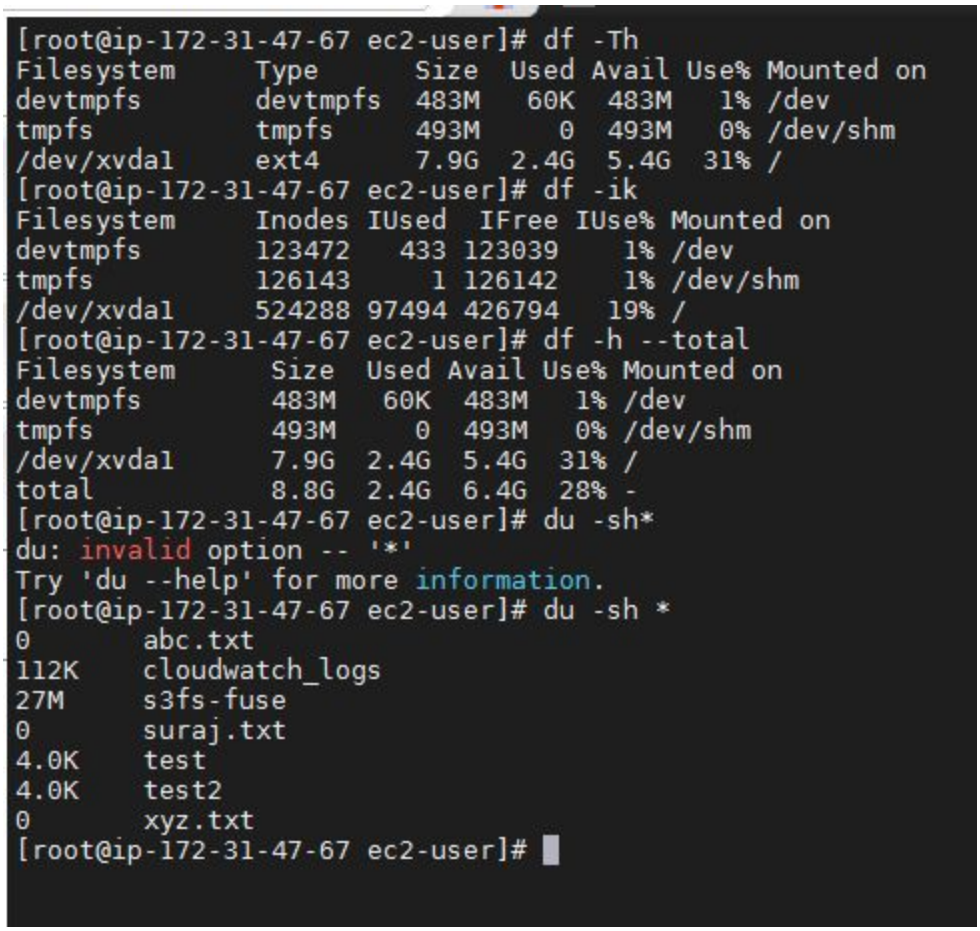


How do you check disk usage? And what is the difference between df and du?

df -Th (T shows the file system type)

df -ik (i stands for no of inodes)

du -sh * (to see the specific folder usage like how many files and data stored)



How do you set linux file and directory permissions?

chmod 777 (full permission)

Absolute Method (numbers)

In Absolute method we use numbers instead of using symbols i.e.

•Read=4

•Write=2

•Execute=1

Assigning different permissions to the file (user=rwx, group=rw and others=r)

#chmod 764 ktfile (where 7 means rwx i.e. 4+2+1, rw=6 i.e. 4+2 and 1 indicates x)

Assigning full permission to the file i.e. rwx to all

#chmod 777 ktfile

Removing all permissions from others

•#chmod 770 ktfile (where **0** indicates **no** permissions)

```
root@ip-172-31-47-67 ec2-user]# ls -l p1.txt
rw-r--r-- 1 root root 0 Apr 26 10:07 p1.txt
root@ip-172-31-47-67 ec2-user]# chmod 777 p1.txt
root@ip-172-31-47-67 ec2-user]# ls -l p1.txt
rwxrwxrwx 1 root root 0 Apr 26 10:07 p1.txt
root@ip-172-31-47-67 ec2-user]# mkdir p2
root@ip-172-31-47-67 ec2-user]# ls -l
otal 20
rw-r--r-- 1 root     root        0 Apr 26 09:35 abc.txt
rwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
rwxrwxrwx 1 root     root        0 Apr 26 10:07 p1.txt
rwxr-xr-x 2 root     root     4096 Apr 26 10:09 p2
rwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
rw-r--r-- 1 root     root        0 Apr 26 09:14 suraj.txt
rwxrwxrwx 2 root     root     4096 Apr 26 09:29 test
--------- 2 root     root     4096 Apr 26 09:29 test2
rw-rw-rw- 1 root     root        0 Apr 26 09:28 xyz.txt
root@ip-172-31-47-67 ec2-user]# chmod 777 p2
root@ip-172-31-47-67 ec2-user]# ls -l
otal 20
rw-r--r-- 1 root     root        0 Apr 26 09:35 abc.txt
rwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
rwxrwxrwx 1 root     root        0 Apr 26 10:07 p1.txt
rwxrwxrwx 2 root     root     4096 Apr 26 10:09 p2
rwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
rw-r--r-- 1 root     root        0 Apr 26 09:14 suraj.txt
rwxrwxrwx 2 root     root     4096 Apr 26 09:29 test
--------- 2 root     root     4096 Apr 26 09:29 test2
rw-rw-rw- 1 root     root        0 Apr 26 09:28 xyz.txt
root@ip-172-31-47-67 ec2-user]#
```

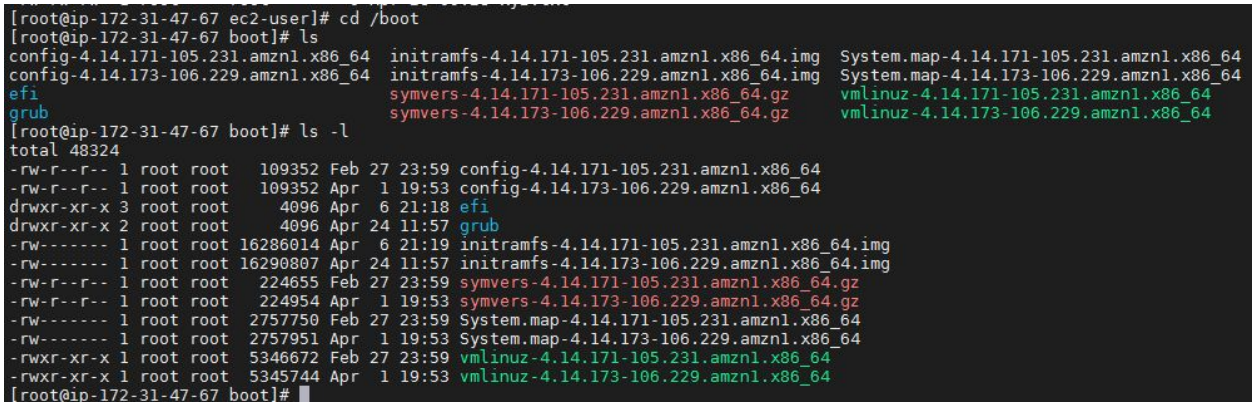
How to set ownership of file and directory?

chown username:groupname filename

```
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
ec2-user:x:500:500:EC2 Default User:/home/ec2-user:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
[root@ip-172-31-47-67 ec2-user]# ls -l p1.txt
-rwxrwxrwx 1 root root 0 Apr 26 10:07 p1.txt
[root@ip-172-31-47-67 ec2-user]# chown ec2-user:ec2-user p1.txt
[root@ip-172-31-47-67 ec2-user]# ls -l p1.txt
-rwxrwxrwx 1 ec2-user ec2-user 0 Apr 26 10:07 p1.txt
[root@ip-172-31-47-67 ec2-user]# chown ec2-user:ec2-user p2
[root@ip-172-31-47-67 ec2-user]# ls -l
total 20
-rw-r--r-- 1 root     root        0 Apr 26 09:35 abc.txt
drwxrwxr-x 3 ec2-user ec2-user 4096 Apr 25 11:42 cloudwatch_logs
-rwxrwxrwx 1 ec2-user ec2-user    0 Apr 26 10:07 p1.txt
drwxrwxrwx 2 ec2-user ec2-user 4096 Apr 26 10:09 p2
drwxr-xr-x 8 root     root     4096 Apr 24 17:28 s3fs-fuse
-rw-r--r-- 1 root     root        0 Apr 26 09:14 suraj.txt
drwxrwxrwx 2 root     root     4096 Apr 26 09:29 test
d--------- 2 root     root     4096 Apr 26 09:29 test2
-rw-rw-rw- 1 root     root        0 Apr 26 09:28 xyz.txt
[root@ip-172-31-47-67 ec2-user]#
```

What is the initrd image?

cd /boot Initial ram disk file system which hold info about your drivers and devices



5 command linux admin should know ?

rsync

sed

awk

lsof

grep

What use of /etc/passwd and /etc/shadow file in linux?

cat /etc/passwd - stores all the info of users and details

cat /etc/shadow - store all user password info in encrypted

```
[root@ip-172-31-47-67 ~]# useradd suraj
[root@ip-172-31-47-67 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
ec2-user:x:500:500:EC2 Default User:/home/ec2-user:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
suraj:x:501:501::/home/suraj:/bin/bash
```

```
[root@ip-172-31-47-67 ~]# passwd suraj
Changing password for user suraj.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-47-67 ~]# cat /etc/shadow
root:*LOCK*:14600::::::
bin:*:16323:0:99999:7:::
daemon:*:16323:0:99999:7:::
adm:*:16323:0:99999:7:::
lp:*:16323:0:99999:7:::
sync:*:16323:0:99999:7:::
shutdown:*:16323:0:99999:7:::
halt:*:16323:0:99999:7:::
mail:*:16323:0:99999:7:::
uucp:*:16323:0:99999:7:::
operator:*:16323:0:99999:7:::
games:*:16323:0:99999:7:::
gopher:*:16323:0:99999:7:::
ftp:*:16323:0:99999:7:::
nobody:*:16323:0:99999:7:::
rpc:!!:18358:0:99999:7:::
ntp:!!:18358::::::
saslauth:!!:18358::::::
mailnull:!!:18358::::::
smmsp:!!:18358::::::
rpcuser:!!:18358::::::
nfsnobody:!!:18358::::::
sshd:!!:18358::::::
dbus:!!:18358::::::
ec2-user:!!:18376:0:99999:7:::
apache:!!:18376::::::
mysql:!!:18377::::::
suraj:$6$mGSBaEAF$VxDuAQuw7lG.ykAxZHvWjUNlMktWmZOt/H0I9f27h55uPwvsnfR1k5pKX.WUyYGdDZcKV1liD18CtLIDbu1J./:18378:0:99999:7:::
[root@ip-172-31-47-67 ~]#
```

What is swappiness in linux? (can have value between 0 to 100)

Sending the process from ram to swap whenever a new process is coming then the old process sends to ram.

What is the difference between cp and mv?

cp for copy and mv (inode number doesn't change until the partition disk is the same) for rename or move a file or directory.

```
[root@ip-172-31-47-67 ~]# ls
demo1.txt
[root@ip-172-31-47-67 ~]# cat demo1.txt
hiiiiiiiiii
hello
[root@ip-172-31-47-67 ~]# cp demo1.txt demo2.txt
[root@ip-172-31-47-67 ~]# ls
demo1.txt  demo2.txt
[root@ip-172-31-47-67 ~]# cat demo2.txt
hiiiiiiiiii
hello
[root@ip-172-31-47-67 ~]# mv demo2.txt demo3.txt
[root@ip-172-31-47-67 ~]# ls
demo1.txt  demo3.txt
[root@ip-172-31-47-67 ~]# ll
total 8
-rw-r--r-- 1 root root 19 Apr 26 10:36 demo1.txt
-rw-r--r-- 1 root root 19 Apr 26 10:38 demo3.txt
[root@ip-172-31-47-67 ~]# pwd
/root
[root@ip-172-31-47-67 ~]# mkdir test
[root@ip-172-31-47-67 ~]# mv demo3.txt test
[root@ip-172-31-47-67 ~]# cd test
[root@ip-172-31-47-67 test]# ls
demo3.txt
[root@ip-172-31-47-67 test]# cat demo3.txt
hiiiiiiiiii
hello
[root@ip-172-31-47-67 test]# ls -li
total 4
22012 -rw-r--r-- 1 root root 19 Apr 26 10:38 demo3.txt
[root@ip-172-31-47-67 test]# cd ..
[root@ip-172-31-47-67 ~]# ls -li
total 8
 22011 -rw-r--r-- 1 root root   19 Apr 26 10:36 demo1.txt
159411 drwxr-xr-x 2 root root 4096 Apr 26 10:39 test
[root@ip-172-31-47-67 ~]#
```

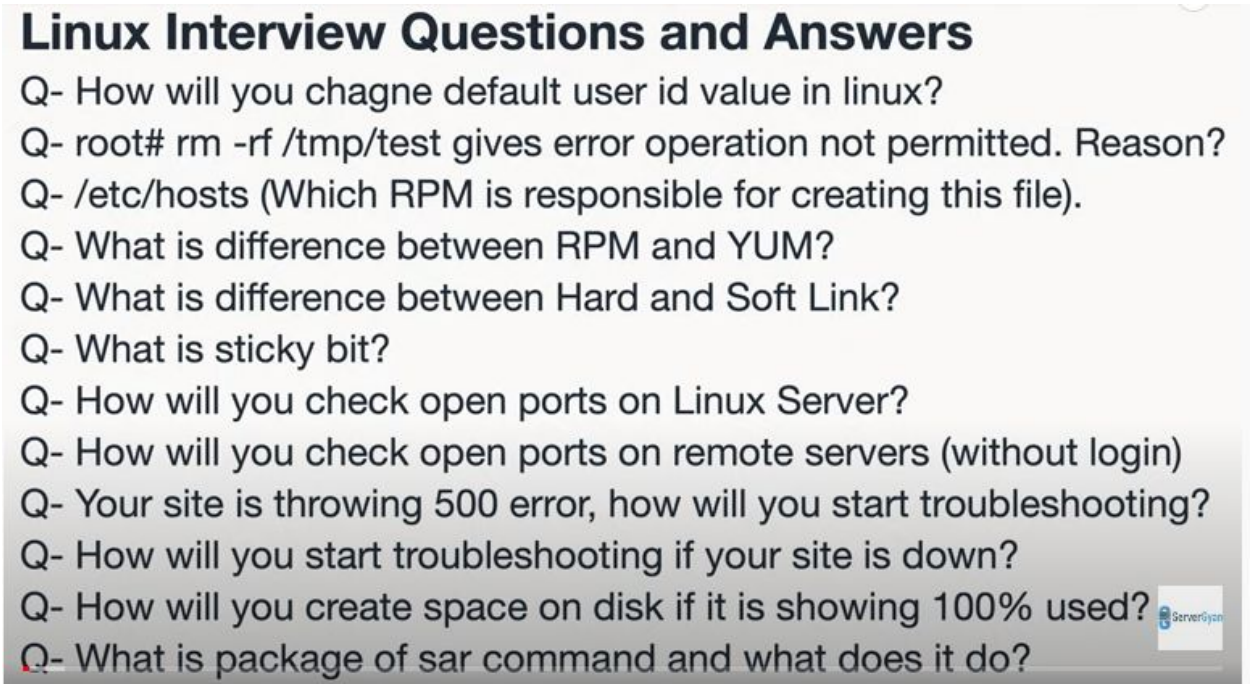
How to create users with admin and without admin rights?

Create user: **useradd suraj or adduser suraj**

Create password: **passwd username or passwd suraj it will ask you enter and retype password**

```
[root@ip-172-31-47-8 tmp]#
[root@ip-172-31-47-8 tmp]# useradd lokendra
[root@ip-172-31-47-8 tmp]# su - lokendra
[lokendra@ip-172-31-47-8 ~]$ sudo ls /etc/shadow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for lokendra:

Sorry, try again.
[sudo] password for lokendra:
[sudo] password for lokendra:
Sorry, try again.
[sudo] password for lokendra:
[sudo] password for lokendra:
^C^C^C^Csudo: 2 incorrect password attempts
[lokendra@ip-172-31-47-8 ~]$ logout
[root@ip-172-31-47-8 tmp]#
```

```
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
suraj   ALL=(ALL)       ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
[root@ip-172-31-47-67 ~]# su - suraj
[suraj@ip-172-31-47-67 ~]$ useradd arun
-bash: /usr/sbin/useradd: Permission denied
[suraj@ip-172-31-47-67 ~]$ logout
[root@ip-172-31-47-67 ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@ip-172-31-47-67 ~]# su - suraj
Last login: Sun Apr 26 10:50:17 UTC 2020 on pts/2
[suraj@ip-172-31-47-67 ~]$ ls
[suraj@ip-172-31-47-67 ~]$
```



How will you change default userid: **vi /etc/login.defs**

```
[root@ip-172-31-47-67 ec2-user]# id tom
uid=502(tom) gid=502(tom) groups=502(tom)
[root@ip-172-31-47-67 ec2-user]# vi /etc/login.defs
[root@ip-172-31-47-67 ec2-user]#
```

```
#
# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define both, MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  500
UID_MAX                60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  500
GID_MAX                60000
```

Rm -rf operation not permitted

```
[root@ip-172-31-42-223 ~]# touch /tmp/test
[root@ip-172-31-42-223 ~]# rm -rf /tmp/test
[root@ip-172-31-42-223 ~]# touch /tmp/test
[root@ip-172-31-42-223 ~]# chattr +i /tmp/test
[root@ip-172-31-42-223 ~]# rm -rf /tmp/test
rm: cannot remove '/tmp/test': Operation not permitted
[root@ip-172-31-42-223 ~]# chattr -i /tmp/test
[root@ip-172-31-42-223 ~]# rm -rf /tmp/test
[root@ip-172-31-42-223 ~]#
```

/etc/hosts which rpm responsible for this file

rpm -qf /etc/hosts

```
[root@ip-172-31-42-223 ~]# ll /etc/hosts
-rw-r--r--. 1 root root 159 Jun 18  2019 /etc/hosts
[root@ip-172-31-42-223 ~]# rpm -qf /etc/hosts
setup-2.12.2-2.el8.noarch
[root@ip-172-31-42-223 ~]# rpm -qf /etc/resolv.conf
file /etc/resolv.conf is not owned by any package
[root@ip-172-31-42-223 ~]# rpm -qf /tmp/test
error: file /tmp/test: No such file or directory
[root@ip-172-31-42-223 ~]# touch /tmp/test
[root@ip-172-31-42-223 ~]# rpm -qf /tmp/test
file /tmp/test is not owned by any package
[root@ip-172-31-42-223 ~]#
```

Difference between rpm and yum

Red hat package manager and YUM (Yellowdog Updater Modified) is an open source command-line as well as graphical based package management tool for RPM (RedHat Package Manager) based Linux systems. It allows users and system administrators to easily install, update, remove or search software packages on a system.

yum install httpd

rpm -ivh httpdpackage.rpm

rpm -qPR httpdpackage.rpm

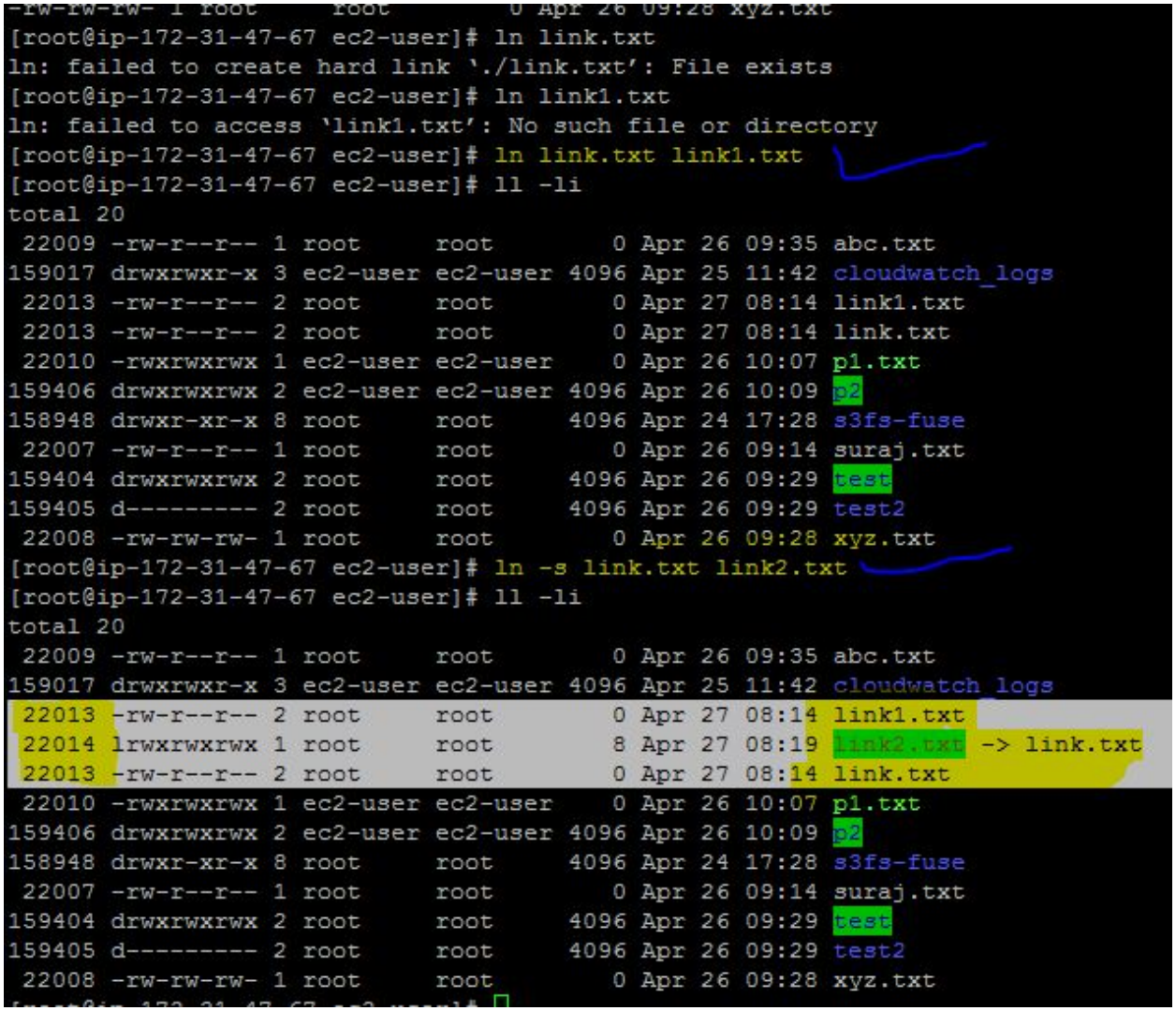
Hard link and soft link:

Creating a soft link: shortcut(indode number change)#

ln –s <source file> <destination>

Creating a Hard link:backup (inode number same with original file):#

ln <source file> <Destination>



Sticky bit in linux

ll / you can see this mean prevent from unwanted deletion

```
[root@ip-172-31-47-67 ec2-user]# ll /
total 108
dr-xr-xr-x  2 root root  4096 Apr 24 17:27 bin
dr-xr-xr-x  4 root root  4096 Apr 24 11:56 boot
drwxr-xr-x  2 root root  4096 Feb 28  2014 cgroup
drwxr-xr-x 16 root root  2740 Apr 27 07:53 dev
drwxr-xr-x 84 root root  4096 Apr 27 07:58 etc
drwxr-xr-x  6 root root  4096 Apr 26 10:45 home
dr-xr-xr-x  7 root root  4096 Apr 24 17:27 lib
dr-xr-xr-x 10 root root 12288 Apr 24 17:27 lib64
drwxr-xr-x  2 root root  4096 Apr  6 21:17 local
drwx------  2 root root 16384 Apr  6 21:17 lost+found
drwxr-xr-x  2 root root  4096 Jan  6  2012 media
drwxr-xr-x  2 root root  4096 Jan  6  2012 mnt
drwxr-xr-x  3 root root  4096 Apr  6 21:18 opt
dr-xr-xr-x 90 root root     0 Apr 27 07:53 proc
dr-xr-x---  4 root root  4096 Apr 26 10:39 root
drwxr-xr-x  3 root root  4096 Apr 24 11:56 run
dr-xr-xr-x  2 root root 12288 Apr 24 17:27 sbin
drwxr-xr-x  2 root root  4096 Jan  6  2012 selinux
drwxr-xr-x  2 root root  4096 Jan  6  2012 srv
dr-xr-xr-x 13 root root     0 Apr 27 07:53 sys
drwxrwxrwt  3 root root  4096 Apr 27 07:53 tmp
drwxr-xr-x 13 root root  4096 Apr  6 21:18 usr
drwxr-xr-x 21 root root  4096 Apr 24 17:29 var
```

How will you check open ports on the linux server? netstat -tunlp

```
[root@ip-172-31-47-67 ec2-user]# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      2327/rpcbind
tcp        0      0 0.0.0.0:46421               0.0.0.0:*                   LISTEN      2350/rpc.statd
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      2533/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      2565/sendmail
tcp        0      0 :::59499                    :::*                        LISTEN      2350/rpc.statd
tcp        0      0 :::111                      :::*                        LISTEN      2327/rpcbind
tcp        0      0 :::22                       :::*                        LISTEN      2533/sshd
udp        0      0 0.0.0.0:111                 0.0.0.0:*                               2327/rpcbind
udp        0      0 172.31.47.67:123            0.0.0.0:*                               2544/ntpd
udp        0      0 127.0.0.1:123               0.0.0.0:*                               2544/ntpd
udp        0      0 0.0.0.0:123                 0.0.0.0:*                               2544/ntpd
udp        0      0 0.0.0.0:806                 0.0.0.0:*                               2327/rpcbind
udp        0      0 127.0.0.1:834               0.0.0.0:*                               2350/rpc.statd
udp        0      0 0.0.0.0:59400               0.0.0.0:*                               2350/rpc.statd
udp        0      0 0.0.0.0:68                  0.0.0.0:*                               2109/dhclient
udp        0      0 :::111                      :::*                                    2327/rpcbind
udp        0      0 :::50468                    :::*                                    2350/rpc.statd
udp        0      0 :::806                      :::*                                    2327/rpcbind
udp        0      0 fe80::3f:3fff:fe0b:73bc:546 :::*                                    2211/dhclient
```

Check open ports on remote servers without login?

yum install nmap -y

nmap -A 8.8.8.8

```
Complete!
[root@ip-172-31-47-67 ec2-user]# nmap -A 8.8.8.8

Starting Nmap 6.40 ( http://nmap.org ) at 2020-04-27 08:33 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0032s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
443/tcp open  https?
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Google Public DNS
| ssl-cert: Subject: commonName=dns.google/organizationName=Google LLC/stateOrProvinceName=California/countryNam
| Not valid before: 2020-04-07T09:35:42+00:00
|_Not valid after:  2020-06-30T09:35:42+00:00
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
mit.cgi :
SF-Port443-TCP:V=6.40%I=7%D=4/27%Time=5EA698D0%P=x86_64-redhat-linux-gnu%r
SF:(HTTPOptions,7,"\x15\x03\x01\0\x02\x02F")%r(SSLSessionReq,7,"\x15\x03\x
SF:01\0\x02\x02F")%r(SSLv23SessionReq,7,"\x15\x03\x01\0\x02\x02F")%r(X11Pr
SF:obe,7,"\x15\x03\x01\0\x02\x02F")%r(vmware-esx,7,"\x15\x03\x01\0\x02\x02
SF:F")%r(RTSPRequest,7,"\x15\x03\x01\0\x02\x02F")%r(RPCCheck,7,"\x15\x03\x
SF:01\0\x02\x02F")%r(DNSVersionBindReq,7,"\x15\x03\x01\0\x02\x02F")%r(DNSS
SF:tatusRequest,7,"\x15\x03\x01\0\x02\x02F")%r(Help,7,"\x15\x03\x01\0\x02\
SF:x02F")%r(Kerberos,7,"\x15\x03\x01\0\x02\x02F")%r(SMBProgNeg,7,"\x15\x03
SF:\x01\0\x02\x02F")%r(LPDString,7,"\x15\x03\x01\0\x02\x02F")%r(LDAPBindRe
SF:q,7,"\x15\x03\x01\0\x02\x02F")%r(SIPOptions,7,"\x15\x03\x01\0\x02\x02F"
SF:)%r(LANDesk-RC,7,"\x15\x03\x01\0\x02\x02F")%r(TerminalServer,7,"\x15\x0
SF:3\x01\0\x02\x02F")%r(NCP,7,"\x15\x03\x01\0\x02\x02F")%r(NotesRPC,7,"\x1
SF:5\x03\x01\0\x02\x02F")%r(WMSRequest,7,"\x15\x03\x01\0\x02\x02F")%r(orac
SF:le-tns,7,"\x15\x03\x01\0\x02\x02F")%r(kumo-server,7,"\x15\x03\x01\0\x02
SF:\x02F");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (89%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   ... 5
6   0.52 ms 100.65.11.161
```

```
[root@ip-172-31-47-67 ec2-user]# nmap 162.255.87.231

Starting Nmap 6.40 ( http://nmap.org ) at 2020-04-27 08:39 UTC
Nmap scan report for 162.255.87.231
Host is up (0.23s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
[root@ip-172-31-47-67 ec2-user]#
```

How to troubleshoot error 500

Db is not responding so check the webserver service ,firewall and security group

How will you start troubleshooting if your site is down?

Same check firewall and running services

How to create space when the disk used 100%?

Either increase the disk space or need to identify using df -Th or du -sh * to remove unwanted storage of data.

What is sar command?

Server activity report: yum install sar -y