Linux Interview Questions

Lavatech Technology

2022

User and Group Administration

1. **What is a user?**
   Ans. In Linux user is one who uses the system.

2. **How many types of users available in Linux?**
   Ans.There are 5 types of users available in Linux.
   - System user (Admin user who control the whole system nothing but root user).
   - Normal user (Created by the Super user. In RHEL - 7 the user id's from 1000 - 60000).
   - System user (Created when application or software installed
   - In RHEL - 7 the System users are Static system user id's from 1 - 200 and (ii) Dynamic system user user id'sfrom 201 - 999).
   - Network user (Nothing but remote user, ie., who are login to the system trough network created
   - Windows Active Directory or in Linux LDAP or NIS).
   - Sudo user (The normal users who are having admin or Super user privileges)

3. **What is user management?**
   Ans.User management means managing user. ie., Creating the users, deleting the users and modifying the users.

4. **What are the important points related to users?**
    - Ans.Users and groups are used to control access to files and resources.
    - Users can login to the system by supplying username and passwords to the system.
    - Every file on the system is owned by a user and associated with a group.
    - Every process has an owner and group affiliation.
    - Every user in the system is assigned a unique user id (uid) and group id (gid).
    - User names and user id are stored in /etc/passwd file.
    - User's passwords are stored in /etc/shadow file in an encrypted form.
    - Users are assigned a home directory and a shell to work with the O/S.
    - Users cannot read, write and execute each other's files without permission.
    - Whenever a user is created a mail box is created automatically in /var/spool/mail location.
    - And some user environmental files like .bash_logout, .bash_profile, .bashrc , ...etc., are also copied from /etc/skell to his/her home directory (/home/<username>).

5. **What are fields available in /etc/passwd file?**
   Ans.<user name> : x : <uid> : <gid> : <comment> : <user's home directory> : <login shell (where 'x' means link to password file ie., /etc/shadow file)

6. **What are fields available in /etc/shadow file?**
   Ans. user name : password : last changed : min. days : max. days : warn days : inactive days : expiry days : reserved for future.

7. **What are the files that are related to user management?**
   - Ans.**/etc/passwd**: Stores user's information like user name, uid, home directory and shell ...etc.,
   - **/etc/shadow**: Stores user's password in encrypted form and other information.
   - **/etc/group**: Stores group's information like group name, gid and other information.
   - **/etc/gshadow**: Stores group's password in encrypted form.
   - **/etc/passwd**: Stores the /etc/passwd file backup copy.
   - **/etc/shadow**: Stores the /etc/shadow file backup copy.
   - **/etc/default/useradd**: Whenever the user created user's default settings taken from this file.
   - **/etc/login.defs**: user's login defaults settings information taken from this file.
   - **/etc/skell**: Stores user's all environmental variables files and these are copied from this directory to user's home directory

8. **In how many ways can we create the users?**

- Ans. **useradd** - <options><user name>
- (ii) **adduser** - <options><user name>
- (iii) **newusers** <file name> (In this file we have to enter the user details same as /etc/passwd file)

9. **What is the syntax of useradd command with full options?**
   Ans. useradd -u <uid> -g <gid> -G <secondary group> -c <comment> -d <home directory> -s <shell><user name>
   Example: useradd -u 600 -g 600 -G java -c öracle userd /home/raju -s /bin/bash raju

10. **What is the syntax of adduser command with full options?**
    Ans.adduser -u <uid> -g <gid> -G <secondary group> -c <comment> -d <home directory> -s <shell><user name>
    Example# adduser -u 700 -g 700 -G linux -c öracle userd /home/ram -s /bin/bash ram.

11. **What is the syntax of newuser command?**
    - Ans. newusers <file name> (This command will create multiple users at a time)
    - First we should a file and enter user′s data as fields same as the fields of /etc/passwd file for how many users do you want to create and mention that file as an argument for newusers command.

- When we execute this command new users will be created but their environmental files like

.bash_logout, .bash_profile, .bashrc and .bash_history files will not be copied from /etc/skell. Directory. So, we have to copied manually from /etc/skell directory.

12. **What is the syntax of userdel command with full options?**
Ans.userdel <options><user name>
The options are:

    - **-f** :forcefully delete the user even through the user is login. The user's home directory, mail and message directories are also deleted.
    - **-r** : recursively means files in the user's home directory will be deleted and his home directory also deleted but the other files belongs to that user should be deleted manually.

13. **How to check whether user is already created or not?**
Ans.We can check in different ways:

    - id <user name> (It shows the user id group id and user name if that is already created)
    - grep <user name> /etc/passwd

14. **How to verify or check the integrity of the password file?**
Ans.**pwck** <options> /etc/passwd or
pwck <options> /etc/shadow The options are,

- **-q** :quiet
- **r** : read only
- **s** : sort the contents by uidin /etc/passwd and /etc/shadow files

15. **How to verify or check the integrity of the group file?**
    - grpck <options> /etc/group or
    - grpck <options> /etc/gshadow
    - The options are, **-r**-r:read only **-s**:sort the contents by **gidin /etc/group and /etc/gshadow files.**

16. **What is syntax of the usermod command with full options?**
    Ans. usermod <options><user name> The options are,
    - -L:lock the password
    - -U : unlock the password
    - -o :creates duplicate user modify the user's id same as other user
    - -u :modify user id
    - -g : modify group id
    - -G : modify or add the secondary group
    - -c : modify comment
    - -d : modify home directory
    - -s : modify user's login shell
    - -l : modify user's login name

- -md :modify the users home directory and the old home directory

17. **How to create the duplicate root user?**
    Ans.useradd -o -u 0 -g root <user name>

18. **How to recover if the user deleted by mistake?**
    Ans.**pwunconv** (It creates the users according **/etc/passwd** file and deletes the **/etc/shadow file)**

19. **What are the uses of .bash_logout,.bash_profile and .bashrc files?**

    Ans.**.bash_logout** :is a user′s logout ending program file.
    It will execute first whenever the user is logout. **.bash**$_{profile}$:
    $isuser's loginstartupprogramfile.Itwillexecutefirstwhenevertheuserislogin.I$
    $Thisfileisusedtocreatetheuser's customcommandsandtospecifytheumaskvalu$

20) **What is a group?**
    Ans.The collection of users is called a group. There are two types of groups.

    a) **Primary group** : It will be created automatically whenever the user is created. User belongs to on group is called a primary group.

b) **Secondary group** : It will not create automatically. The admin user should be created manually and users belongs to more than one group is called secondary group. A user can be assigned to max. 16 groups. ie., 1 primary group and 15 secondary groups.

21. **What is the command to check the user belongs to how many groups?**
    Ans. groups <user name>

22. **What is the syntax to create the group?**
    Ans.**groupadd**<options><group name> The options are,
    - -f :add the group forcefully
    - -g : group id no.
    - -o :non-unique (duplicate group id)
    - -p : group password
    - -r : system group
    - -R : root group

23. **What is the syntax to modify the group?**
    Ans.The options are,
    - -g : group id
    - -n :new name for existing one, ie., rename the group
    - -o : non-unique (duplicate group id)
    - -p : group passwd

- -R :root group

24. **What is syntax to delete the group?**

    - **groupdel** <group name> (to delete the group without options)
    - **groupdel** <group name> (to delete the group without options)

25. **How to assign the password to the group?**
    Ans.**gpasswd** <group name> (to assign a password to the group without any options). **gpasswd** <options><group name> The options are,

    - -a : add users to the group
    - -d : delete the user from the group
    - -r : remove the group password
    - -R : restrict to access that group
    - -A : set the list of Administrative users
    - -M : set the list of group members

26. **How to check the integrity or consistency of the group?**
    Ans.grpck (it will check the integrity or consistency in **/etc/gpasswd** and /etc/gshadow files).

27. **How to restore /etc/gshadow file if deleted by mistake?**
Ans. grpconv (it creates the **/etc/gshadow** file from **/etc/group** file)

28. **How to change the password aging policies?**
Ans.we can change the password policies in 2 ways(I.e configuration file and Chage Command) (i) First open the /etc/login.defs file and modify the current values
Example :vim /etc/login.defs

    - min - 0:means the user can change the password to any no. of times.
    - min -2: means the user can change the password within 2 days. ie., he can change the password after 2 days.
    - max - 5: means the user should change the password before or after 5 days. Otherwise the password will be expired after 5 days.
    - inactive - 2 :means after password expiry date the grace period another 2 days will be given to change the password.
    - warning - 7 : means a warning will be given to the user about the password expiry 7 days before expiry date.

    (ii) second by executing the chage command.
    Example : chage <options><user name> The options are

    - -d : last day
    - -E : expiry date
    - -I : inactive days

- -l : list all the policies
- -m : min. days
- -M : max. days
- -w : warning days

Note :Whenever we **change** the password aging policy using chage command, the information is will be modified in /etc/shadow file.

29. **How add 45 days to the current system date?**
    Ans. date -d "+ 45 days"

30. **Explain the sudo user?**
    Ans.Sudoers (nothing but sudo users) allows particular users to run various root user commands without needing a root password. **/etc/sudoers** is the configuration file for sudoers to configure the normal user as privileged user. It is not recommended to open this file using **vim** editor because this editor cannot check the syntax by default and whatever we typed in that file that will blindly save in this file. So, one editor is specially available for opening this file, i.e.,**visudo**and all normal users cannot execute this command. Only root user can run this command. Once this file is opened nobody can open this file again on another terminal because **"The file is busy"**message is displayed on the terminal for security reasons.

31. **How to give different sudo permissions to normal users?** Ans.Open the **/etc/sudoers** file by executing visudo command and go to line no. 98 and type as **<User name> <Machine>= <Command>root**
ALL=(ALL) ALL
raju All= ALL Save and exit this file.
Note : When we trying to save this file if any syntax errors in this file, those errors are displayed with line no's and **What you do ?** (will be displayed, here press 'e' to edit this file and modify those errors or mistakes and save this file.

    - su - raju (to switch to raju user)
    - sudo useradd <useradd> (The normal user raju can also add the users to the system)
    - We can assign sudo permissions to 'n' no. of users by specifying names separated by commas (,) or line by line.
    - Instead of giving all permissions to normal user we can give only some commands.
    - **Example** student ALL=/usr/sbin/useradd, /usr/sbin/usermod
      raju ALL=NOPASSWD:/usr/sbin/useradd, /usr/sbin/usermod
    - We can also apply to one group or groups as follows.
    - First create the users, assign one group to those users and also assign the passwords for that users.
    - Open **/etc/sudoers** file by executing the command **visudo**and type as follows.
    -

    - We can also create one command alias and add some commands to that alias and mention that alias to users as follows.
    - Cmnd$_{A}liasNETWORKING = /usr/sbin/route, /usr/sbin/ifconfig$
      $username >< machines >=< commandaliasname >$
      $rajuALL =$

- We can also create one user alias and add the users to that alias and assign some commands to that alias as follows.
- User$_{A}lias < useraliasname >=< user1 >, < user2 >, < user3 >$, **Example** : $User_{A}liasOURTEAM = raju, shyam, ram, gopal$
- OURTEAM ALL=ALL (to give all permissions of sudo)
- Defaults timestamp$_{t}imeout = 0(wheneverthesudouserexecutesanycommandthenit$
  - Defaults : <user1>, <user2>, <user3> timestamp$_{t}imeout =$ $0(thesystemwillaskpasswordsforuser1, user2, user3toexecutesudocommands$

32. **In which location the sudo user commands history is logged?**

    - All the sudo users commands history is logged in **/var/log/secure**file to make a record of sudo user commands.
    - cat /var/log/secure (to see the contents of this file)
    - tailf /var/log/secure (to see the updates of this file continuously and press ctrl + c to quit the tailf)

33. **How to assign the password to normal user by him whenever first login to the system?**

Ans.Whenever the user is created and that user is trying to login to the system, it will ask the password. If the root user is not assign the password to that user, then that normal user can assign the password by his own using the following commands.

- useradd <user name> (to create the user)
- passwd -S <user name> (to see the status of the password of that user. if root user is not assigned the password then the password status is locked)
- passwd -d <user name> (then delete the password for that user)
- chage -d 0 <user name> (it will change the password age policy)
- su - <user name> (Try to switch to that user then it will display the following message)
- Newpassword : (type new password for that user)
- Retype password :(retype the password again)

The other useful commands:

- w :(this command gives the login user information like how many users currently login and full information)
- who :(to see users who are currently login and on which terminal they login)
- last :(see the list of users who are login and logout since the **/var/log/wtmp** file was created)
- lastb :(to see the list of the users who tried as bad logins)

- lastreboot:(to see all reboots since the log file was created)
- uptime:(to see the information from how long the system is running, how many users login and load average)
- The load average is from **1 sec : 5 secs : 15 secs**
- df (to see the mounted partitions, their mount points and amount of disk space)
- du (to see the disk usage of the each file in bytes)
- uname -r (gives the current kernel version)
- last -x (It shows last shutdown date and time)
- last -x grep shutdown (only shutdown time shows ie., grep will filter the 'last -x' command)
- **grep:**It is used to search a word or sentence in file (ie., inside the file)
- **find :** It is used to search a command or file inside the system)
- cat /etc/shells or chsh -l (to see how many shells that are supported by Linux)
- /bin/sh : default shell for Unix
- /bin/bash: default shell for Linux
- /sbin/nologin:users cannot login shell
- /bin/tsch:cshell to write 'C++' language programs
- /bin/csh : c shell to write 'C' language programs
- echo SHELL :(to see the current shell)
- chsh <user name> (to change the user's shell)
- Changing shell for <user name> :

- New shell : <type new shell for example /bin/sh to change the current shell>New shell changed (But it will effect by restarting the server)
- date R :(to display the time only)
- date + x :(to display the date only)
- history :(to see the history of the commands)
- history -c :(to clear the history)
- history -r :(to recover the history)
- **_.bash_history** is the hidden file to store the history of the user commands. By default history size is 1000.
- echo HISTSIZE :(to check the current history size)
- export HISTSIZE=500 (to change the current history size to 500 temporarily)
- export HISTTIMEFORMAT=
- vim /etc/bashrc (open this file go to last line and type as follows to make history i size date time formats permanently)
- HISTSIZE=1000
- HISTTIMEFORMAT='
- <user name>:(to go to users home directory)
- what is <command>:(to see the short description of that command)
- where is <command>(to see the location of that command and location of the document of that command)
- reset :(to refresh the terminal)

- whoami :(to see the current user name)
- who a mi :(to see the current user with full details like login time and others)
- passwd <user name> (to change the password of the user)
- id (to see the current user name, user id, group name and group id, ... etc.,)
- id <user name>:(to see the specified user name, user id, group name and group id)
- su :(to switch to root user without root user home directory)
- su :(to switch to root user with root user home directory)
- su <user name :(to switch to the specified user without his home directory)
- su - <user name> :(to switch to the specified user with his home directory)
- lspci :(to list all the PCI slots present in the system)
- du -sh /etc :(to see the size of the /etc on the disk in KBs or MBs)
- ls -l :(to see the long listing of the files and directories)
- d rwx rwx rwx . 2 root root 6 Dec 17 18:00 File name
- d : type of file
- rwx : owner permissions
- rwx :group permissions
- rwx :others permissions

- No ACL permissions applied
- root :owner of the file
- root :group ownership
- 6 ßize of the file
- Dec 7 18:00 : Date and Time of the created or modified
- File name :File name of that file
- ls -ld <directory name> (to see the long listing of the directories)
- stat <file name/directory name> (to see the statistics of the file or directory)

34. **How many types of the files are there?**
    Ans.There are 7 types of files.
    a) -:regular file
    b) d : directory
    c) c : character device file (Ex. console file, open and close terminals, ...etc.,)
    d) b : block device file (Ex. device blocks like hard disks, CD/DVD disks)
    e) s : socket file (programmers will deal this file)
    f) p : pipe file (programmers will deal this file)
    g) l : linked file (nothing but short cut file)

35. **What are permission types available in Linux and their numeric representations?**
Ans.There are mainly three types of permissions available in Linux and those are,

    - read —– r —– 4 null permission —— 0
    - write —– r —– 4
    - execute —– r —– 4

36. **What is syntax of chmod command with full options?**
Ans.chmod <options><file/dir name> (to change the owner or permissions of the file/dir) The options are,

    - c :changes
    - -f :silent (forcefully)
    - -v : verbose
    - -R : recursive (including sub directories and files)

    To change the permissions the syntax is, chmod <who> <what> <which> <file name or directory> To change the permissions the syntax is, chmod <who> <what> <which> <file name or directory>

37. **What is the syntax of chown command with full options?**
Ans.chown <options><file name or directory> (to change the ownership of the file or directory) The options are,

    - c :changes
    - -f :silent (forcefully)

- -v : verbose
- -h : no difference
- -R :recursive (including sub directories and files)
- -H :symbolic link to a directory (command line argument)
- -L :symbolic link to a directory (all)
- -p : do not traverse

chown <username> : <group name> <file name or directory name> (to change owner and group ownership of the file or directory)

38. **What is syntax of chgrp command with full options?**
Ans.chgrp <options><file name or directory> (to change group ownership of the file directory) The options are,
    - c: changes
    - -f : silent (forcefully)
    - -v : verbose
    - -h : no difference
    - -R : recursive (including sub directories and files)
    - -H : symbolic link to a directory
    - -L :do not traverse-p : do not traverse

39. **What are the default permissions of a file and directory?**
Ans.
    - The default permissions of a file = 6 6 6
    - The default permissions of a directory = 7 7 7

40. **What is umask in linux?**
Ans.

- The user file-creation mode mask (umask) is used to determine the file permissions for newly created files or directories. It can be used to control the default file or directory permissions for new files. It is a four-digit octal number. The umask value for normal user is **0002** and the umask value for root user is **0022.**
- So, the effected file permissions for normal users = 6 6 6 - 0 0 2 = 6 6 4.
- The effected directory permissions for normal users = 7 7 7 - 0 0 2 = 7 7 5.
- The effected file permissions for root user = 6 6 6 - 0 2 2 = 6 4 4
- The effected directory permissions for root user = 7 7 7 - 0 2 2 = 7 5 5
- umask <value> (to change the umask value temporarily)
- vim /etc/bashrc (open this file and change the umask value to effect the whole system)
- source /etc/bashrc (to updated the source file)
- vim .bashrc (open this file in user's home directory and at last type as follows)
- umask <value> (save and exit the file)
- source .bashrc or logout and login again (to the system to effect that umask value)

- If the**/etc/login.defs** file is corrupted then new users will be added and can be assigned the passwords but users cannot login.
- If the **/etc/login.defs** file is deleted then new users cannot be added

41. **How change the permissions using numeric representation?** Ans.

    a) The values for read = 4, write = 2, execute = 1 and null = 0. The total value = 4 + 2 + 1 = 7

    b) chmod <no.><no.><no.><file name or directory name> **Example :** chmod 7 7 4 file1 (to give read, write and execute to owner and read, write and execute to group and read permission to others)

    c) chmod 6 6 0 file2 (to give read and write to owner and read and write to group and null (0) permission to others)

42. **Explain about set uid (suid)?** Ans.

    - If we plan to allow all the users to execute the root users command then we go for set uid (suid).
    - It can be applied for user level and is applicable for files only.
    - chmod u+s <file name> (to set the suid on that file)
    - chmod u-s <file name> (to remove the suid from that file)

- ls -l (if 'x' is replaced with 's' in owner's level permissions that means suid is applied on that file)
- - r w s r w x r w x <file name> (here 's' is called set uid or suid)
- **Example :** chmod u+s /usr/sbin/init 6 (then any user can restart the system using this command init 6)
- chmod u+s /sbin/fdis (then any user can run the fdisk command)
- strings <command name> (to read the binary language of the command ie., the string command converts the binary language into human readable language)
- strings mkfs (to read the mkfs command's binary language into human readable language)
- Normally set uid (suid) permission will be given on scripting files only

43. **Explain about set gid (sgid)?**
Ans.If we plan to allow all the users of one group to get the group ownership permissions then we go for set gid (sgid). It can be applied for group level and is applicable on directories only. **Example:** chmod g+s <directory name> (to set the sgid on that directory)
chmod g-s <directory name> (to remove the sgid from that directory)

44. **Explain about sticky bit?**
Ans.It protects the data from other users when all the users having full permissions on one directory.
It can be applied on others level and applicable for directories only. Example : chmod o+t <directory name> (to set the sticky bit permission on that directory)
ls -ld <directory name> r w x r w x r w t <directory name> (where 't' is called the sticky bit)

45. **What are the uses of passwd and shadow files?**
Ans. **Passwd file**:

a) When we create the user one entry is updated in password and shadow files.

b) It represents and tell about that user login name , uid, gid, default home directory of the use and default shell.

c) So, using this file we can easily get users information.

Shadow file ;

a) This file tells about the login id, user's encrypted password, password when last changed, min. days the password valid, max. days valid, warning days, inactive days and expiry days.

b) If shadow file is missed or deleted we can recover those entries of shadow file using password file.

c) We can change the users encrypted passwords with the permissions of the higher authorities in case of emergency.

46. **What is the use of group?**
Ans.

a) In an organization the whole work is divided into departments for easy maintenance and easy

b) For each department is also represented as group and that group having so many users to do different works.

c) So, if we create one group and assign that group to all the users in that department, then we can easily identify which user belongs to which group.

d) We can share files, directories and execute some programs to that group and also give permissions to that group. So, each user of that group can easily share those directories and also can easily access, execute or even write in those shared files and directories.

47. **Can we login to the user without password?**
Ans.Yes, we can login.

48. **How to recover the root password if missed or deleted?**
Ans:**RHEL - 6 :**

a) Restart the system.

b) Select 1st option and press 'e'.

c) Select 2nd option and press 'e'.

d) At the end give one blank space and type 1 and press Enter key.

e) Then press 'b' to boot the system in single user mode.

f) Then prompt appears and type passwd root command.
New password : XXXXXX Retype password : XXXXXX

g) Exit

h) Then system starts as usual

RHEL - 7 :

a) Restart the system.

b) Using arrow keys select 1st line and press 'e' to edit.

c) Go to **Linux 16** line press End key or **Ctrl + e** to go to the end of the line and give one space.

d) Then type as **rd.break console=tty1 selinux=0**

e) Then press Ctrl + x to start the computer in single user mode.

f) After starting we get **swith**$_{r}oot : /promptappearsandthentypeasfollo$

g) chroot /sysroot press Enter

h) Then **sh - 4.2** prompt appears and type as

i) **sh - 4.2 passwd root** New password : XXXXXX Retype password : XXXXXX

j) **sh - 4.2 exit**

k) **switch-root :/exit**

l) Then the system starts and the desktop appears.

49. **How to restrict the users from login?**
Ans.

a) By removing (deleting) the user we can restrict the user from login.

b) Put the user′s hostnames as entries in **/etc/hosts.deny** file (applying TCP wrappers).

c) **passwd -l <user name>** (by locking his password we can restrict the users).

50. **How to put never expiry to a user?**
Ans.passwd -x -1 <user login name>

51. **Which one is the default sticky bit directory?**
Ans. /tmp is the default sticky bit directory.

52. **What is the purpose of the profiles?**
Ans.Profile is a file to enter some settings about users working environment. ie., we can set user home directory, login shell, path, ...etc., Profiles are two types. (a) Global profile (b) Local profile **Global profile**

a) Only root user can set and applicable to all the users.

b) Only global parameters can entered in this profile.

c) The location of the global profile is **/etc/bashrc**

Local profile

a) Every user has his/her own profile.

b) The settings entered in this profile are only for that user.

c) The location of the profile is**bashprofile**(hidden file) in that particular user′s home directory.

53. **Can we mount/unmount the O/S file system?**
Ans. No, we cannot mount or unmount the O/S file system.

54. **How to find the users who are login and how to kill them?**
Ans. fuser -cu :(to see who are login) fuser -ck <user login name> :(to kill the specified user)

55. **what is Access Control List (ACL)?**
Ans.Define more access rights nothing but permissions to files and directories. Using Access Control list we assign the permissions to some particular users to access the files and directories. ACL can cab be applied on ACL enabled partition that means you need to enable ACL while mounting the partition.

56. **How to implement ACLs?**
Ans.
    - Create a partition and format it with ext4 file system.
    - Mount the file system with ACL.
    - Apply ACL on it.

- Create a partition using **fdisk** command.
- Format the above partition with ext4 file system using **mkfs.ext4 <partition name>** command.
- Create the mount point using **mkdir /<mount point>** command.
- Mount that file system on the mount point using **mount -o acl <partition name><mount point>** command.
- Mount the partition permanently using **vim /etc/fstab** (open this file and make an entry as below
- **<partition name><mount point><file system type> defaults, acl 0 0**
- Save and exit this file.
- If the partition is already mounted then just add **acl** after defaults in **/etc/fstab** file and execute
- the below command **mount -o remount <partition name>**

57. **How to check the ACL permissions?**
    Ans.getfacl <options><file or directory name> The options are,
    - -d:Display the default ACLs.
    - -R :Recurses into subdirectories

58. **How to assign ACL permissions?**
    Ans.setfacl <options><argument> : <username>: <permissions><file or directory name> The options are,

- -m : Modifies an ACL.
- -x : Removes an ACL.
- -b : Remove all the ACL permissions on that directory.
- -R : Recurses into subdirectories The arguments are,
- u : user
- g : group
- o : other

59. **What is the syntax to assign read and write permissions to particular user, group and other?**
    Ans.
    - setfacl -m u : <user name> : <permissions><file or directory>
    - setfacl -m g : <user name> : <permissions><file or directory>
    - setfacl -m o : <user name> : <permissions><file or directory>

60. **What is the syntax to assign read and write permissions to particular user, group and other at a time?**
    Ans.setfacl -m u : <user name> : <permissions>, g : <user name> : <permissions>, o : <user name> : <permissions><file or directory>
    Useful commands :
    - setfacl -x u : <user name><file or directory name> (to remove the ACL permissions from the user)

- setfacl -x g : <user name><file or directory name>(to remove the ACL permissions from group)
- setfacl -x o : <user name><file or directory name> (to remove the ACL permissions from other)
- setfacl -b <file or directory> (to remove all the ACL permissions on that file directory)

61. **How will you lock a user, if he enters wrong password 3 times?**
    Ans.pam_tally.so module maintains a count of attempted accesses, can reset count on success, can deny access if too many attempts fail. Edit /etc/pam.d/system-auth file, enter:

    - vi /etc/pam.d/system-auth Modify as follows: auth required pam$_{t}ally.sono_{m}agic_{r}ootaccountrequiredpam_{t}ally.sodeny =$ $3no_{m}agic_{r}ootlock_{t}ime = 180$**deny=3** : $Denyaccessiftallyforthisuserex$

- **lock_time=180** : Always deny for 180 seconds after failed attempt. There is
- alsounlock$_{t}ime = n\ option.Itallowaccessafternsecondsafterfailedattempt.Ifthiso$ $Ifthemoduleisinvokedbyauserwithuid = 0thecounterisnotincremented.Thesys -$ $adminshouldusethisforuserlaunchedservices, likesu, otherwisethisargumentshould$
  - no$_{m}agic\_root$: $Avoidrootaccountlocking, ifthemoduleisinvokedbyauserwith$ $0.Saveandclosethefile.$

62. **How to see the no. of failed logins of the users?**
    Ans.

    - faillog -u <user name> :(to see the specified users failed login attempts)

- faillog -a : (to see failed login attempts of all users)
- faillog -M <Max. no> -u <user name> :(to set Max. login failed attempts to that user)
- faillog -M 5 -u raju :(to set Max. login failed attempts to 5 for user raju)

63. **What is disk quotas and how to enable them?**
    Ans.By configuring the disk quotas we can restrict the user to use unlimited space on the file system and also to restrict the unlimited files in the file system. We can configure the disk quotas in ways. They are,

    - user quotas
    - group quotas

    Steps to enable : First check whether the quota package is installed or not by **rpm -qa |grep quota command. If quota** package is not Installed then install the quota package by **yum install quota* -y** command.

    - quotaon :(to enable the quota)
    - quotaoff :(to disable the quota)
    - edquota :(to edit or modify the quota)
    - repquota :(to display or report the present quota)
    - quotacheck :(to create a quota database)

    quotas cab be applied on file systems only.

64. **How to enable the user quota on a file system?**
    Ans.

- Open the /etc/fstab file by **vim /etc/fstab** command and goto the mount point entry line and type as, /dev/sdb1 /mnt/prod ext4 defaults, usrquota 0 0 (save and exit this file)
- Update the quota on mount point by **mount -o remount, usrquota <mount point>** ii command.
- Create the user quota database by quotacheck -cu <mount point> command (where -c means created the quota database and -u means user quota).
- Check whether the quota is applied or not by mount command.
- Enable the quota by quotaon <mount point> command.
- Apply the user quota for a user by **edquota -u <user name><mount point>**
- blocks: No. of blocks used (already)
- soft : Warning limit
- hard : Maximum limit
- 0 : Unlimited usage
- inodes : No. of files created (already)

If soft=10 and hard=15 means after crossing the soft limit a warning message will be displayed and if hard limit is also crosses then it won't allow to create the files for that user. (save and exit the above quota editor)

65. **How to enable the quota on block level?**
Ans.Apply the user quota for a user by edquota -eu <user name><mount point> command. File system blocks soft hard inodes soft

hard /dev/sdb1 0 5000 10000 0 0 0 (save and exit the quota editor)

- soft=5000 : means if it reaches upto 5MB, there is no warnings. If it exceeds ie., from 5MB - 10MB there will be warnings messages displayed, but the files
- hard=10000 : If it reached to 10MB, then it will not allow to create the files. The grace period by default is 7 days. So, we can change the grace period by edquota -t command, here we can change the default 7 days grace period to our required days of grace period.grace period means, if the user not created any files within the grace period days the soft limit becomes as hard limit. ie., soft and hard limits are equal.

edquota -p <user name 1><user name 2>:to apply user name 1 quotas to user name 2, ie., no need to edit the quota editor for user name 2)

66. **How to enable the group quota?**
Ans.

a) Open the **/etc/fstab file by vim /etc/fstab** command and goto the mount point entry line and type as,/dev/sdb1 /mnt/prod ext4 defaults, grpquota 0 0 save and exit this file

b) Update the quota on mount point by **mount -o remount, usrquota, grpquota <mount point>**command

c) Create the user quota database by **quotacheck -cug <mount point> command** where -c means created the quota database, -u means user quota and -g means group quota).

d) Check whether the quota is applied or not by **mount** command.

e) Enable the quota by quotaon **<mount point>** command.

f) Apply the user quota for a user by **edquota -g <group name><mount point> command.**

g) File system blocks soft hard inodes

h) /dev/sdb1 0 0 0 0 0 0

i) **How to change the password for multiple users at a time**
Ans.chpasswd :(to change multiple user′s passwords)

- <user name 1> : <password>
- <user name 2> : <password>
- <user name 3> : <password>
- <user name 4> : <password>
- <user name 5> : <password>
- (Ctrl + d —–> to save and exit)

Then the above 5 user′s passwords will be changed at a time. But here the passwords will not be encrypted while typing passwords. So, anybody can see the passwords. ie., there is no security.

Managing Partitions and File Systems

a) **What is partition?**
Ans.A partition is a contiguous set of blocks on a drive that are treated as independent disk.

b) **What is partitioning?**
Ans.Partitioning means to divide a single hard drive into many logical drives.

c) **Why we have multiple partitions?**
Ans.

- Encapsulate our data.
- Since file system corruption is limited to that partition only.
- So we can save our data from accidents.
- We can increase the disk space efficiency
- Depending on our usage we can format the partition with different block sizes.
- So we can reduce the wastage of the disk.
- We can limit the data growth by assigning the disk quotas

d) **What is the structure of the disk partition?**
Ans.The first sector of the O/S disk contains the MBR (Master Boot Record). The MBR is divided into 3 parts and it's size is 512 bytes. The first part is IPL (Initial Program Loader) and it contains the Secondary Boot Loader. So, IPL is responsible for booting the

O/S and it’s size is 446 bytes The second part is PTI (Partition Table Information). It contains the number of partitions on the disk, sizes of the partitions and type of the partitions

e) **Explain the disk partition criteria?**
Ans.Every disk can have max. 4 partitions. The 4 partitions are 3 Primary partitions and 1 Extended partition. The MBR and O/S will install in Primary partition only. The Extended partition is a special partition and can be further divided into multiple logical partitions.

f) **How to identify the disks?**
Ans.

- In Linux different types of disks will be identified by different naming conventions.
- IDE) drives will be shown as /dev/hda, /dev/hdb, /dev/hdc, ...etc., and the partitions are /dev/hda1, /dev/hda2, /dev/hda3, ...etc.
- iSCSI/SCSI and SATA drives will be shown as /dev/sda, /dev/sdb, /dev/sdc, ...etc., and the partitions are /dev/sda1, /dev/sda2, /dev/sda3, ...etc.,
- Virtual drives will be shown as /dev/vda, /dev/vdb, /dev/vdc, ...etc., and the partitions are /dev/vda1, /dev/vda2, /dev/vda3, ...etc.,
- IDE :Integrated Drive Electronics.

- iSCSI:Internet Small Scale System Interface.
- SCSI : Small Scale System Interface.

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

h) **What are the different types of file systems supported in Linux?**
Ans.

- The Linux supported file systems are ext2, ext3, ext4, xfs, vfat, cdfs, hdfs, iso9660 ...etc.,
- The ext2, ext3, ext4 file systems are widely used in RHEL-6 and xfs file system is introduced on RHEL-7.
- The vfat file system is used to maintain a common storage between Linux and Windows O/S.
- The cdfs file system is used to mount the CD-ROMs and the hdfs file system is used to mount DVDs.
- The iso9660 file system is used to read CD/DVD.iso image format files in Linux O/S.

i) **How to create different types of partitions?**
Ans. fdisk -l fdisk /dev/sdc Command (m for help) : n (type n for new partition) (p - primary) or e - extended) : p (type p for primary partition or type e for extended partition)

- First cylinder : (press Enter for default first cylinder)
- Last cylinder : + <size in KB/MB/GB/TB>

Command (m for help) : t (type t to change the partition id) for example: 8e for Linux LVM, 82 for Linux Swap and 83 for Linux normal partition) Command (m for help) : w (type w tosave the changes into the disk) partprobe /partx -a/kpartx /dev/sdc1 (to update the partitioning information in partition table)

j) **How to make a file system in Linux?**
Ans. mkfs.ext2/ext3/ext4/xfs/vfat <device name> (for example/dev/sdc1)

k) **How to mount the file systems temporarily or permanently?**
Ans.mkdir /mnt/oracle mount /dev/sdc1 /mnt/oracle (temporary mount) vim /etc/fstab /dev/sdc1 /mnt/oracle xfs defaults 0 0 Esc+:+wq! mount -a (permanent mount)

l) **How to delete the partition?**
Ans. fdisk /dev/sdc Command (m for help) :d (type d for delete the partition) Partition number : (specify the partition number) Command (m for help) : w (type w to write the changes into disk) partprobe/partx -a/kpartx /dev/sdc1(to update the partition table without restarting the system)

m) **What is mounting and in how many types can we mount the partitions?**
Ans. Attaching a paritiiton to a directory under root is known as mounting.There two types of mountings in Linux/Unix.

- Temporary Mounting:In a temporary mounting first we create a directory and mount the partition on that directory. But this type mounting will last only till the system is up and once it is rebooted the mounting will be lost. Example: mount <options><device name><directory name (mount point)>
- Permanent Mounting :In this also first we create the directory and open the /etc/fstab file and make an entry as below, <device name><mount point><file system type><mount options><take a backup or not><fsck value>

Whenever the system reboots mount the partitions according to entries in /etc/fstab file. So, these type of mountings are permanently even after the system is rebooted. mount -a to mount the partitions without reboot)

n) **Which files are related to mounting in Linux?**
Ans.

- **/etc/mtab:** is a file which stores the information of all the currently mounted file systems and this file is dynamic and keep on changing.
- **/etc/fstab** is keeping information about the permanent mount points. If we want to make our mount point permanent then make an entry about the mount point in this file.

/etc/fstab entries are: 1 2 3 4 5 6 device name mount point F/S type mount options Dump FSCK

o) **The partitions are not mounting even though there are entries in /etc/fstab. How to solve this problem?**
Ans. First check any wrong entries are there in /etc/fstab file. If all are ok then unmount all the partitions by executing the below command, _umount -a Then mount again mount all the partitions by executing the below command, _mount -a

p) **When trying to unmounting it is not unmounting, how to troubleshoot this one?**
Ans.Some times directory reflects error while unmounting because,(i) you are in the same directory and trying to unmount it, check with pwdcommand. (ii) some users are present or accessing the same directory and using the contents in it, check this with

- fuser -cu <device name> (to check the users who are accessing that partition)

- lsof <device name> (to check the files which are open in that mount point)
- fuser -ck <opened file name with path> (to kill that opened files)

Now we can unmount that partition using umount <mount point>

q) **How to see the usage information of mounted partitions?**
Ans.df -hT (to see device name, file system type, size, used, available size, use

r) **How to see the size of the file or directory?**
Ans.

- du -h <filename or directory name> :(to see the size of the in that directory)
- du -h :(to see all the file sizes which are located in the present working directory)
- du .| sort -nr | head -n10 :(to see the biggest files from current location)
- du -s * | sort -nr | head -n10 : (to see the biggest directories from that partition)
- ncdu :(to list biggest files and directories, we have to install the ncdu package before executing this)

s) **How to assign a label to the partition?**
Ans.e2label <device name or partition name><label name> (to assign the label to that partition) Example : e2label /dev/sdb1 oradisk (to assign oradisk label to /dev/sdb1 partition) mount -l (to list all the mounted partitions along with their labels)

t) **How to mount a partition temporarily or permanently using label?**
Ans.mount LABEL=<label name><mount point> ex : mount LABEL=oradisk /mnt/oracle (to mount the oradisk label on /mnt/oracle directory) vim /etc/fstab LABEL=oradisk /mnt/oracle ext4 defaults 0 0 Esc+:+wq! (to save and exit the file) mount -a (to mount the partitions) mount (to verify whether it is mounted or not)

u) **How mount the partition permanently using block id (UUID)?**
Ans. blkid <partition name or disk name> (to see the UUID or block id of that partition) Example : blkid /dev/sdb2 (to see the UUID or block id of the /dev/sdb2 partition) Copy that UUID with mouse and paste it in /etc/fstab file and make an entry about that. Example: vim /etc/fstab UUID="....................../ mnt/oracle ext4 defaults 0 0 Esc+:+wq! (to save and exit)

v) **What is the basic rule for swap size?**
Ans.

- If the size of the RAM is less than or equal to 2GB, then the size of the swap = 2 X RAM size.
- If the size of the RAM is more than 2GB, then the size of the swap = 2GB + RAM size

w) **How to create a swap partition and mount it permanently?**
Ans.

- free -m :(to see the present swap size)
- swapon -s :(to see the swap usage)
- fdisk <disk name> (to make a partition)
- Example: fdisk /dev/sdb
- Command (m for help) : n (to create a new partition)
- First cylinder : (press Enter to take as default value)
- Last cylinder : +2048M (to create 2GB partition)
- Command (m for help) : t (to change the partition id)
- Enter the partition No.: 2 (to change the /dev/sdb2 partition id)
- Enter the id : 82 (to change the partition id Linux to Linux Swap)
- Command (m for help) : w (to save the changes into the disk)

- partprobe /dev/sdb (to update the partition table information)
- mkswap <device or partition name> (to format the partition with swap file system)
- Example : mkswap /dev/sdb2 (to format the /dev/sdb2 partition with swap file system)
- swapon <device or partition name> (to activate the swap space)
- Example : swapon /dev/sdb2 (to activate /dev/sdb2 swap space)
- free -m (to see the swap size)
- vim /etc/fstab (to make an entry to permanent mount the swap partition)
- /dev/sdb2 swap swap defaults 0 0
- Esc+:+wq! (to save and exit)

x) **What are the attributes of the file system?**
Ans.

- Inode number
- File name
- data block

y) **What is inode number and what is the use of it?**
Ans.Inode numbers are the objects the Linux O/S uses to record the information about the file.Generally inode number contains two parts.

- Inode first part contains information about the file, owner, its size and its permissions.
- Inode second part contains pointer to data blocks associated with the file content.

That's why using the inode number we can get the file information quickly.

z) **How to check the integrity of a file system or consistency of the file system?**
Ans. **fsck <device or partition name>** command we can check the integrity of the file system. But before running the fsck command first unmount that partition and then run fsck command.

) **What is fsck check or what are the phases of the fsck?**
Ans.

- First it checks blocks and sizes of the file system
- Second it checks file system path names
- Third it checks file system connectivity
- Fourth it checks file system reference counts (nothing but inode numbers)
- Finally it checks file system occupied cylindrical groups

) **Why the file system should be unmount before running the fsck command?**
Ans.If we run **fsck** on mounted file systems, it leaves the file systems in unusable state and also deletes the data. So, before running the fsck command the file system should be unmounted.

) **Which type of file system problems you face?**
Ans.

- File system full
- File system corrupted

) **How to extend the root file system which is not on LVM?**
Ans.By using **gparted** command we can extend the root partition, otherwise we cannot extend the file systems which is not on LVM.

) **How to unmount a file system forcefully?**
Ans.umount -f <mount point>
fuser -ck <mount point>

) **How to know the file system type?**
Ans.df -hT (command gives the file system type information)

) **How to know which file system occupy more space and top 10 file systems?**
Ans. df -h <device or partition name> | sort -r | head -10

) **What is the command to know the mounted file systems?**
Ans. mount or cat /etc/mtab

) **How to know whether the file system is corrupted or not?**
Ans. First unmount the file systems and then run **fsck** command on that file system.

) **How to recover if a file system is corrupted or crashed?**
Ans. If the normal or not related to O/S file system is corrupted first unmount that file system and run fsck command on that file system and if the O/S related file system is corrupted then boot the system with CDROM in single user mode and run the fsck command. If the normal or not related to O/S file system is crashed then restore it from the recent backup and if the O/S related file system is crashed then boot the system with CDROM in single user mode and restore it from the recent backup

) **How to create a file with particular size?**
Ans.dd if=/dev/zero of=/orafile bs=1MB count=500 (to create 500MB size /orafile with 4KB blocksize)

) **How to find how many disk are attached to the system?**
Ans. fdisk -l (to see how many disk are attached to the system)

) **What is journaling?**
Ans. It is a dedicated area in the file system where all the changes are tracked when the system crashed. So the possibility of the file system corruption or crashes is less because of this journaling feature.

) **How to repair the Superblock of the file system?**
Ans.Whenever we want to store the data into the hard disk, if the input/output error occurs then the Superblock of the file system may be erased or corrupted. So, we have to restore or repair that Superblock. umount <file system mount point> (to unmount the file system) dumpe2fs </dev/vgname/lvname> | grep superblock (to list the superblocks first primary superblock and then secondary superblock and so on) e2fsck -b <copy and paste the secondary super block from the above list></dev/vgname/lvname> (to restore the damaged superblock) mount -a (to mount the file system)

) **How to create the file systems with the user specified superblock reserve space?**
Ans. mkfs.ext4 -m <no.><partition name> (to format the partition with <no.>

) **How to modify the superblock reserve space?**
Ans. tune2fs -m <no.><partition name> (to modify the superblock reserve space to <no.>

) **How to modify the superblock reserve space?**
Ans. tune2fs -m <no.><partition name> (to modify the superblock reserve space to <no.>
Important Commands :

- fsck <partition name> :(to check the consistency of the file system)
- e2fsck <partition name> :(to check the consistency of the file system in interactive mode)
- e2fsck -p <partition name>:(to check the consistency of the file system without interact mode)
- mke2fs -n <partition name> :(to see the superblock information)
- mke2fs -t <file system type><partition name> :(to format the partition in the specified filesys type)
- mke2fs <partition name>:(to format the partition in default ext2 file system type)
- blockdev –getbs /dev/sdb1 (to check the block size of the /dev/sdb1 file system)fsck <device

    or partition name> (to check and repair the file system)

  Note: Before running this command first unmount that partition then run fsck command.

  - umount -a :(to unmount all the file systems except (/) root file system)
  - mount:to mount all the file systems which are having entries in /etc/fstab file)
  - fsck -A : (to run fsck on all file systems)
  - fsck -AR -y : (to run fsck without asking any questions)
  - fsck -AR -t ext3 -y : (to run fsck on all ext3 file systems)
  - fsck -n /dev/sdb1 :(to see the /dev/sdb1 file system report without running fsck)
  - tune2fs -l /dev/sdb1 : (to check whether the journaling is there or not)
  - tune2fs -j /dev/sdb1 : (to convert ext2 file system to ext3 file system)
  - tune2fs -l /dev/sdb1 : (to check whether the journaling is added or not)
  - tune2fs -O $^{h}as_{j}ournal/dev/sdb1 : (toconvertext3filesystemtoext2$ $Odir_{i}ndex, has_{j}ournal, unit_{b}g/dev/sdb1 : (toconvertext2filesystem$

- tune2fs -O extents, dir$_{i}ndex, unit_{b}g/dev/sdb1 : (toconvertext3filesystemtoext4fi$ $oremount, rw/dev/sdb1 : (tomountthepartitionwithreadandwritepermissions)$
- mount -o remount, ro /dev/sdb1: (to mount the partition with read only permissions)

- mount < directory name> : (to check whether this directory is mount/ normal directory)
- dump2fs <device or partition name> :(to check the metadata of the partition and repair the metadata)
- fdisk -l :(to list total hard disks attached to system and their partitions)
- fuser -cu <device or partition name> :(to see the users who are accessing that file system)
- fuser -cK <device or partition name> :(to kill the users processes who accessing the file systems)

  Note: Even though we kill those users processes sometimes we cannot unmount those partitions, so if this situation arises then first see the process id's of the user opened files by **lsof <mount point> kill -9 <process id>** killthose processesforcefully journalctl (It tracks all the log files between two different timings and by default saved in **/run/log) /run/log** is mounted on **tmpfs** file system. ie., if system is rebooted, the whole information in that location will be deleted or erased. We can change /run/log is mounted on tmpfs file system. ie., if system is rebooted, the whole information in that location will be deleted or erased.

  - mkdir -p /var/log/journal :(to make a directory in /var/log location
  - chown root : systemd-journal /var/log/journal (to change the group ownership of /var/log/-journal
  - chmod g+s /var/log/journal:(to set the sgid on /var/log/journal)

- killall -URS1 systemd-journald:(It is necessary to kill old /run/log process and the location of journal messages is changed to /var/log/journal)
- journalctl -n 5 : (to display last five lines of all the log files)
- journalctl -p err : (to display all the error messages)
- journalctl -f :(to watch journalctl messages continuously)
- journalctl –since<today> or <yesterday> : (to see all the journalctl messages since today or yesterday)
- journalctl –since "date-until "date": (to see the journal messages between the specified two dates)
- journalctl -pid=1 :(to see the pid=1 process name)
- auditctl :(to see the audit report).

Logical Volume Management and RAID Levels

a) **What is LVM and why we go for LVM?**
Ans. **Lvm**means Logical Volume Management. The combination of 2 or more physical disk in order to make a big logical disk is called Logical Volume.
If normal Linux partition is full and an application

requires some more disk space, then normal partition cannot be extended for that application requirement. For this first we have to take a backup of that normal partition, delete that partition and again create that partition with more disk space, format and mount that partition and finally restore the application from the backup. This process requires down time So, to overcome this problem LVM concept is coming into the picture. Using this LVM we can extend or reduce the file systems as per requirement without loss of any data.

b) **What are the components of the LVM?**
Ans.

- Physical Volume (PV)
- Physical Extent (PE)
- Volume Group (VG)
- Logical Volume (LV)
- Logical Extent (LE)

i. **Physical Volume (PV)** :It is the standard partition that we add to the LVM. Normally a physical volume is a standard primary or logical partition with the partition code as **8e.**

ii. **Physical Extent (PE)** :It is chunk of disk space. Every physical volume is divided into a number of equal sized PEs.

iii. **Volume Group (VG)** :It is composed of a group of physical volumes and logical volumes. It is the organizational group of LVM.

iv. **Logical Volume (LV)**: It is composed of a group of LEs. We can format (make a file system) and mount any file system on the logical volume. The size of these logical volumes can easily be increased or decreased as per the requirement.

v. **Logical Extent (LE)**:It is also a chunk of disk space. Every logical extent is mapped to a specific physical extent.

c) **How to create the LVM, make a file system and mount that permanently?**
Ans.

- Take two physical disks for example **/dev/sdb** and /dev/sdc. if there is no second disk then make the required partitions using fdisk command and change the partition code as 8e.
- Convert the Physical disk into physical volumes by,**pvcreate /dev/sdb /dev/sdc**
- Then create the volume group by combining physical volumes by, **vgcreate <volume group name><physical volume names> or vgcreate -s <PE size in MBs><volume group name><physical volume names>**
- Then create the logical volume on the above created volume group by, **lvcreate -L +<size in MBs> -n <logical volume name><Volume group name> or lvcreate -l <no. of PEs> -n <logical volume name><volume group name>**
- Make a file system on the above created logical volume by, **mkfs.ext2/ext3/ext4/xfs /dev/<volume**

group name>/<logical volume name> Create a mount point to mount the above created LVM file system by, **mkdir /mnt/<directory name>**

- Mount the LVM on the above created mount point temporarily by, **mount /dev/<volume group name>/<logical volume name><mount point>or** Mount the LVM on mount point permanently by, **vim /etc/fstab /dev/<VG name>/<LV name> /mnt/<directory> <file system type> defaults 0 0** Esc+:+wq!
- **mount -a**
- **df -hT** : (to see the mounted partitions with file system types)

d) **How to see the details of the Physical Volumes?**
Ans.

- pvs :(displays all physical volumes with less details)
- pvdisplay : (displays all physical volumes with more details)
- pvdisplay <physical volume name> : (displays the details of the specified physical volume)
- pvscan :(to scan all the physical volumes)
- pvscan <PV name> :(to scan the specified physical volume)

e) **How to see the details of the Volume Groups?**
Ans.

- vgs :(displays all volume groups with less details)
- vgdisplay :(displays all volume groups with more details)
- vgdisplay <VG name> :(displays the specified volume group with more details)
- vgscan :(to scan all the volume groups)
- vgscan <VG name>:(to scan the specified volume group)

f) **How to see the details of the Logical Volumes?**
Ans.

- lvs :(displays all logical volumes with less details)
- lvdisplay :(displays all logical volumes with more details)
- lvdisplay <LV name>:(displays the specified logical volume details)
- lvscan :(to scan all the logical volumes)
- lvscan <LV name> : (to scan the specified logical volume)

g) **How to extend the Volume Group?**
Ans. Extending the volume group is actually adding a new physical volume to the volume group. To extend the volume group we need to create a new partition using **fdisk** command and make sure that it's

partition id should be **8e,** save the changes and update the partition table by **partprobe**
Create a physical volume on the newly created partition using **pvcreate** command. Add the partition to the volume group using **vgextend** command Example : fdisk /dev/sdb

- Command (m for help) : n
- First cylinder : press Enter for default one
- Last cylinder : +500M :(create 500MB partition)
- Command (m for help) : t (to change the partition id)
- Select the partition : type the partition number
- Specify the Hexa code : 8e
- Command (m for help) : w (to save the changes)

partprobe /dev/sdb1 pvcreate /dev/sdb1 vgextend <VG name> /dev/sdb1 vgdisplay <VG name> :(to check the size of the volume group)

h) **How to extend the logical volume and update it's file system?**
Ans. Sometimes the file system size may be full, so we need to increase the size of the logical volume to continue adding the data in it. The size of the logical volume can be increased online, no downtime required. Check current size of the logical volume by **lvdisplay <LV name>**and the size of the file system by df -hT command. Increase the size of the logical volume by **lvextend or lvresize**commands. Then finally update the file system by **resize2fs or**

$\mathbf{xfs}_{g}rowfscommands.Example : df - hTlvextend - L+ < sizeinMB >< /dev/vgname/lvname > orlvresize - L+ < sizeinMB >< /dev/vgname/lvname > resize2fs < /dev/vgname/lvname > lvdisplay < /dev/vgname/lvname >: (tocheckthesizeofthelogicalvolume)df - hT : (tocheckthesizeofthefiles$

i) **How to reduce the logical volume and update the file system?**
Ans.Reducing the size of the logical volume is a complicated task and we have remember some points before reducing the logical volume, otherwise the file system may be damaged . Logical volume size cannot be reduced online and it requires downtime because we have to unmount the file system by **umount <file system mount point>command.** Check the consistency of the file system by **e2fsck <device or partition name> command.** Reduce the logical volume by lvreduce **-L - <Size of in MB></dev/vgname/lvname> command.** Then update the file system by resize2fs </dev/vgname/lvname> Finally mount the file system by mount -a Example: umount <file system mount point> e2fsck <device or partition name> lvreduce -L -<size in MB></dev/vgname/lvname> resize2fs </dev/vgname/lvname> lvdisplay </dev/vgname/lvname> :(to check the size of the logical volume> mount -a :(to mount the file system) df -hT :(to check the size of the file system)

j) **How to move or migrate the logical volume data from one physical volume to another physical volume?**

Ans.There might be a situation where the physical volume might be failing and it is required to replaced. In such case, we need to migrate or move the logical volume data from the failed physical volume new physical volume and isolate (remove) the failed physical volume. First access the mount point of the failing physical volume and check the data in it. Verify the size of the physical volume by pvs or **pvdisplay </dev/vgname**/lvname>command. Unmount the file system of that physical volume by **umount <file system mount point>** Add a new physical volume and the size should be same size or higher than that failing physical volume. Migrate the physical volume contents to the new physical volume using **pvmove <old PV>**<new PV> Mount back the logical volume, access the mount point and verify the data in it. Remove the failed the physical volume by vgreduce **<vgname><pvname> command.** Example :

- cd <file system mount point>
- ls
- pvs <pvname> or pvdisplay <pvname>
- umount <file system mount point>
- pvcreate <device or partition name>
- vgextend <vgname><pvname>
- pvmove <old pvname><new pvname>
- mount -a
- vgreduce <vgname><failed pvname>
- cd <file system mount point>
- ls

k) **How to delete or remove the logical volume?**
Ans.To delete or remove the logical volume, first unmount the file system by **umount <mount point>**Remove the entry in /etc/fstab file. Remove the logical volume by **lvremove </dev/vgname/lvname>command.** Verify whether the logical volume is removed or not by **lvs or lvdisplay command.** Example : umount <file system mount point> vim /etc/fstab :(delete the entry of the logical volume) Esc+:+wq! :(save and exit the file) lvremove </dev/vgname/lvname> lvs or lvdisplay :(to verify whether logical volume is removed or not)

l) **How to delete or remove the volume group?**
Ans.To delete or remove the volume group, first make sure that any logical volume should not be mounted because while removing a volume group it will delete or remove the logical volumes in that volume group. Then delete or remove the volume group by vgremove <vgname>command. Verify whether the volume group is remove or not by vgs or vgdisplay command. Example : umount <file system mount point> : (to unmount the file system if there is any LV) vim /etc/fstab :(delete the entry of the logical volume) Esc+:+wq! :(save and exit the file) vgremove <vgname> vgs or vgdisplay :(to verify whether volume group is removed or not)

m) **How to delete or remove the physical volume?**
Ans. Deleting or removing a physical volume is very

simple and the only thing we should check that the physical volume we are going to delete should not belong to any volume group ie., we can only delete or remove the physical volume which is free. Then delete or remove the physical volume by **pvremove <pvname>**command Verify whether the physical volume is removed or not by pvs or pvdisplay command. Example : pvremove <pvname> pvs or pvdisplay :(to verify whether the physical volume is removed or not)

n) **How to restore the volume group which is removed mistakenly?**
Ans. First unmount file system by **umount <file system mount point>** command.Check the volume group backup list by vgcfgrestore –list <volume group name>command. Then remove the logical volume by **lvremove </dev/vgname/lvname>** command. Copy the backup file which is taken backup before removed the volume group from the above backup list and paste it in this command vgcfgrestore -f <paste the above copied file name><vgname> The logical volume is created automatically after restoring the volume group but the volume group and logical volumes both will be in inactive state. So, check the state of the volume group by vgscanand the logical volume state by lvscan commands. Then activate that volume group by textbf vgchange -ay <volume group name>commandand activate the logical volume by lvchange -ay <logical volume name>command. Mount the logical volume file system

by **mount -a** command **Example :**

- umount <file system mount point>
- vgcfgrestore –list <volume group name> (copy the backup file from the list)
- lvremove </dev/vgname/lvname>
- vgcfgrestore -f <paste the above copied file><volume group name>
- vgscan (to check the status of the volume group)
- lvscan (to check the status of the logical volume)
- vgchange -ay <volume group name> :(activate the volume group if it is in inactive state)
- lvchange -ay <logical volume name> :(activate the logical volume if it is in inactive state)

Note: The option a means active VG or LV and option y means yes.

o) **How to change the volume group name and other parameters?**
Ans.

- vgrename <existing volume group name><new volume group name> (to rename the volume group)
- By default, unlimited logical volumes can be created per volume group. But we can control this limit by
- vgchange -l <no.><volume group> (to limit max. no. of logical volumes to the specified number)

- Example : vgchange -l 2 <vgname> (to limit max. 2 logical volumes cab be created in this volume group)
- vgchange -p <no.><volume group> (to limit max. no. of physical volumes to the specified number)
- Example : vgchange -p 2 <vgname> (to limit max. 2 physical volumes can be added to this volume group)
- vgchange -s <block size in no.><volume group> (to change the block size of the volume group)
- Example : vgchange -s 4 <vgname> (to change the volume group block size to 4MB)

p) **How to change the logical volume name and other parameters?**
Ans.

- lvrename <existing lvname><new lvname> (to rename the logical volume)
- lvchange -pr <logical volume> (to put the logical volume into read only mode)
- lvs (to see the logical volume permissions)
- lvchange -prw <logical volume> (to put the logical volume into read and write mode)

q) **How to disable the volume group and logical volume?**
Ans.

- vgchange -an <volume group> :(to disable the volume group) lvchange -an <logical volume> :(to disable the logical volume)

r) **How to take a backup of the volume group?**
   Ans.

   - vgcfgbackup :(to take a backup of all volume groups)
   - vgcfgbackup <volume group> :(to take a backup of the specified volume group)

- **What is the configuration file of the logical volume?**
  Ans. cat /etc/lvm/lvm.conf (to see the contents of the LVM configuration file)

- **What are the locations of the logical volume and volume groups?**
  Ans.

  - cd /etc/lvm/backup :(the logical volumes backup location)
  - cd /etc/lvm/archive (:the volume groups backup location)

- **How to know the current version of the LVM package?**
  Ans. rpm -qa lvm* :(to know the current version of the LVM package)

- **What are the attributes of the volume group?**
  Ans. vgs (to see the attributes of the volume group) [The attributes are w —-> writable z —-> extendable n —-> normal] vgs -v (to check the UUID of the volume group)

- **How to extend the logical volume to max. disk space and half of the disk space?**
  Ans. lvextend -l +100
  lvextend -l 50

- **How to check on which physical volume the data is writing in the logical volume?**
  Ans. lvdisplay -m :(to check on which physical volume the data is currently writing from all logical volumes) lvdisplay -m <lvname> :(to check on which physical volume the data is writing from the Specified logical volume)

- **How many types of file systems available?**
  Ans.
  - ext2 :Second extended file system (default in RHEL - 3 4)

        - ext3 :Third extended file system (default in RHEL - 5)
        - ext4 :Fourth extended file system (default in RHEL - 6)
        - xfs :Extended file system (default in RHEL - 7)
        - ufs :Unix file system (default in Solaris)
        - jfs : Journal file system (default in IBM-AIX)
        - hfs : High performance file system (default in HP-UX)
        - vxfs : Veritas file system
        - procfs : Process file system (temporary)
        - tempfs :Temporary file system (temporary)
        - cdfs : Compact disk file system
        - hdfs : DVD file system
        - iso9660 : To read the CD/DVD.iso image format files in Linux

    - **How to scan and detect the luns over the network?**
      Ans. ls /sys/class/fc$_{h}ost : (tochecktheavailablefibrechannels)echo$
      $- -»/sys/class/scsi_{h}ost/ < lunno. > /scan : (toscananddetectthelunsoverthenetwork)$

- **How to mount a pen drive in Linux?**
  Ans.

  - lsusb or fdisk -l :(to know the pen drive name)
  - mkdir /mnt/pendrive :(to create a mount point for pen drive)
  - mount <pen drive name><mount point> :(to mount the pen drive on the above created mount point)
  - cd /mnt/pendrive :(to access the pen drive)

- **How to mount a CD/DVD ROM drives in Linux?**
  Ans.The CD/DVD ROM device name in Linux is /dev/cdrom
  - mkdir /mnt/mycdrom :(to create the mount point for CD/DVD)
  - mount /dev/cdrom /mnt/mycdrom :(to mount the CD/DVD on the above created mount point)
  - cd /mnt/mycdrom :(to access the CD/DVD ROM drives)

  - **How to mount the ".iso ïmage files in Linux?**
    Ans.
    - mount -t iso9660 /root/rhel6.iso /iso -o ro, loop :(to mount the .iso image files)
    - cdrecord /root/Desktop/rhel6.iso : (to write the CD/DVD ROM. Before executing this

- * command put the empty CD/DVD into CD/DVD drive)
  * eject : (to eject the CD/DVD drive tray)
  * eject -t : (to insert and close the CD/DVD drive tray)

– **What is RAID? What is the use of the RAID and how many types of RAIDs available?**
  Ans.RAID stands for Redundant Array of Independent Disks.It provides fault tolerance, load balancing using stripping, mirroring and parity concepts. There are mainly two types of RAIDs available.

  * Hardware RAID :(Depends on vendors and also more expensive)
  * Software RAID :(Does not depends on vendors and less expensive when compared to Hardware

– **How many types of software RAIDs available and their requirements?**
  Ans.

  i. RAID - 0 —- Stripping —- Minimum 2 disks required
  ii. RAID - 1 —- Mirroring —- Minimum 2 disks required
  iii. RAID - (1+0) — Mirroring + Stripping —- Minimum 4 disks required

iv. RAID - (0+1) — Stripping + Mirroring —- Minimum 4 disks required

v. RAID - 5 —- Stripping with parity —- Minimum 3 disks required

- **How to configure RAID - 0 in Linux?**
  Ans.To configure RAID - 0, minimum 2 disks are required and the partition id is "fd".Reading and writing is very fast. So, it produces high performance. if one disk is failed we cannot recover the data. So, there is no redundancy and fault tolerance in RAID - 0. Example : For example if the data is 1, 2, 3, 4, 5 and 6 then ....
  Disk - 1 Disk - 2 If the Disk - 1 is /dev/sdb and the Disk - 2 is /dev/sdc then,

  * mdadm -Cv /dev/md0 -n 2 /dev/sdb /dev/sdc -l 0 (to create the RAID - 0 using disk - 1 and disk - 2)
  * cat /proc/mdstat (to check the RAID - 0 is created or not)
  * mkfs.ext4 /dev/md0 (to create the ext4 file system on the RAID - 0)
  * mkdir /mnt/raid0 (to create the RAID - 0 mount point)
  * mount /dev/md0 /mnt/raid0 (to mount RAID - 0 on the mount point)
  * mdadm -D /dev/md0 (to see the details of the RAID - 0 partition)

    - mdadm /dev/md0 -f /dev/sdb (to failed the disk manually)
    - mdadm /dev/md0 -r /dev/sdb (to remove the above failed disk)
    - mdadm /dev/md0 -a /dev/sdd (to add the new disk in place of failed disk)
    - umount /mnt/raid0 (to unmount the raid file system)
    - mdadm –stop /dev/md0 (to stop the RAID - 0 volume)
    - mdadm /dev/md0 –add /dev/sde (to add third disk to the RAID - 0 volume)
  - mdadm –grow /dev/md0 –raid$_{d}evice = 3(togrowtheRAID - 0filesystem)$

- **How to configure RAID - 1 in Linux?**
  Ans. To configure RAID - 1, minimum 2 disks are required and the partition id is "fd". In this the same data will be written on 2 disks ie., exact copy on both the disks. if one disk is failed we can recover the data from another disk. So, there is a high availability, redundancy and fault tolerance in RAID - 1. In this writing speed is slow compared to RAID - 0. Example : For example if the data is 1, 2, 3, 4, 5 and 6 then ....
  If the Disk - 1 is /dev/sdb and the Disk - 2 is /dev/sdc then,

    - mdadm -Cv /dev/md0 -n 2 /dev/sdb /dev/sdc -l 1 (to create the RAID - 1 using disk - 1 and disk - 2)
    - cat /proc/mdstat (to check the RAID - 1 is created or not)
    - mkfs.ext4 /dev/md0 (to create the ext4 file system on the RAID - 1)
    - mkdir /mnt/raid1 (to create the RAID - 1 mount point)
    - mount /dev/md0 /mnt/raid1 (to mount RAID - 1 on the mount point)
    - mdadm -D /dev/md0 (to see the details of the RAID - 1 partition)
    - mdadm /dev/md0 -f /dev/sdb (to failed the disk manually)
    - mdadm /dev/md0 -r /dev/sdb (to remove the above failed disk)
    - mdadm /dev/md0 -a /dev/sdd (to add the new disk in place of failed disk)
    - umount /mnt/raid1 (to unmount the raid file system)
    - mdadm –stop /dev/md0 (to stop the RAID - 1 volume)
    - mdadm /dev/md0 –add /dev/sde (to add third disk to the RAID - 1 volume)
- mdadm –grow /dev/md0 –raid$_{d}evice = 3(togrowtheRAID - 1filesystem)$

- **How to configure RAID - 5 in Linux?**
  Ans.To configure RAID - 5, minimum 3 disks are required and the partition id is "fd". In every disk approximately 25 - 30Reading and writing is very fast. So, it produces high performance. This is used Stripping with parity concept. if one disk is failed we can recover the data using remaining two disks and parity. If two disks are failed, then we cannot recover the data. So, there is no redundancy and fault tolerance in RAID - 5. Example : For example if the data is 1, 2, 3, 4, 5 and 6 then ....
  Disk - 1 Disk - 2 Disk - 3 If the Disk - 1 is /dev/sdb, the Disk - 2 is /dev/sdc and Disk - 3 is /dev/sddthen,
  * mdadm -Cv /dev/md0 -n 2 /dev/sdb /dev/sdc -l 5 (to create the RAID - 5 using disks - 1, 2 and 3)
  * cat /proc/mdstat (to check the RAID - 5 is created or not)
  * mkfs.ext4 /dev/md0 (to create the ext4 file system on the RAID - 5)
  * mkdir /mnt/raid5 (to create the RAID - 5 mount point)
  * mount /dev/md0 /mnt/raid5 (to mount RAID - 5 on the mount point)
  * mdadm -D /dev/md0 (to see the details of the RAID - 5 partition)
  * mdadm /dev/md0 -f /dev/sdb (to failed

    the disk manually)

    * mdadm /dev/md0 -r /dev/sdb (to remove the above failed disk)
    * mdadm /dev/md0 -a /dev/sde (to add the new disk in place of failed disk)
    * umount /mnt/raid5 (to unmount the raid file system)
    * mdadm –stop /dev/md0 (to stop the RAID - 5 volume)
    * mdadm /dev/md0 –add /dev/sdf (to add fourth disk to the RAID - 5 volume)

  * mdadm –grow /dev/md0 –raid$_{d}evice = 4(togrowtheRAID - 5filesystem)$

- **What are the main advantages of RAID - 5**
  Ans.RAID - 5 uses Stripping with parity and requires only three disks. Because of Stripping the data reading and writing will be fast.And by usingparity we can recover the data if one of the three disks failed. So, the main advantage of RAID - 5 we can get fast writing, reading and also redundancy fault tolerance with less expensive.

- **How will you troubleshoot if one of the eight disks failed in LVM?**
  Ans. First umount the file system and add the new disk with same size of the failed

disk to the volume group. Then move the data from failed physical volume to newly added physical volume and then remove the failed physical volume from the volume group. And finally mount the file system.

- **What is pvmove and when it is used in LVM?**
  Ans.The pvmove command is used to move the data from failed physical volume to newly added physical volume. This command is used when one of the physical volume is failed in the LVM.

- **How to inform the client and then troubleshoot if the disk is full?**
  Ans.First check which files are accessing more disk space by **du -h** |sort - r command. if any temporary and junk files are present remove them from the disk to make a room for new or updated data. Then inform the actual situation to the client, take the permission from the client to get the lun from storage and extend the file system by adding that lun to the LVM.

- **Did you work on storage?**
  Ans.Actually I did not work on storage but I know the procedure how to export the lun from storage to client using iSCSI target. Then

scan that lun at cleint side and add the lun to the LVM. I also know the storage hardware from Emc square, Netapp and others. And I am dreaming to work on storage, cloud and virtualization.

– **I have four disks each 1TB in RAID - (1+0). So, total how much disk space can I utilize in that RAID – (1+0)?**
  Ans.RAID - (1+0) means Mirroring + Stripping. It requires 4 disks, ie., 2 disks for mirroring and remaining 2 disks for stripping. And 5 - 10

– **If two disks failed in RAID - (1+0), can we recover the data?**
  Ans.The RAID - (1+0) requires minimum 4 disks and it uses Mirroring + Stripping. If one disk is failed we can recover the data, but if two disks are failed we cannot recover the data.

– **How many types of disk space issues can we normally get?**
  Ans .

  * Disk is full.
  * Disk is failing or failed.
  * File system corrupted or crashed.

  - O/S is not recognizing the remote luns when scanning, ...etc.,

- **What is a link file and how many types?**
  Ans. Link file is a short cut file to the original file. Creating and removing (deleting) inks between two files is known as managing links. There are two types of links files available in Linux.
  - Soft link
  - Hard link