Quick Reference
For
Linux Administration

By. Kr. Reddy

SUVEN IT

Chapter#1 - User and Group Administration

1. What is a user?

In Linux user is one who uses the system.

2. How many types of users available in Linux?

There are 5 types of users available in Linux.

(i) System user (Admin user who control the whole system nothing but root user).

(ii) Normal user (Created by the Super user. In RHEL - 7 the user id's from 1000 - 60000).

(iii) 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).

(iv) Network user (Nothing but remote user, ie., who are login to the system trough network created

in Windows Active Directory or in Linux LDAP or NIS).

(v) Sudo user (The normal users who are having admin or Super user privileges)

The types of users in Linux and their attributes:

Type of User	Example	User ID	Group ID	Home Directory	Default Shell
Super User	Root	0	0	/root	/bin/bash
Normal User	ram, raju, gopal, ...etc.,	500 - 60000	500 - 60000	/home/<user name>	/bin/bash
System User	ftp, ssh, apache, nobody, ...etc.,	1 - 499	1 - 499	/vat/ftp, ...etc	/sbin/nolgin
Network User	Remote user like LDAP user	Same as normal users	Same as normal users	/home/guests/ldap user	/bin/bash
Sudo User	Normal users with admin privileges	Same as normal users	Same as normal users	/home/<user name>	/bin/bash

3. What is user management?

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?

- *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?

<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?

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?

- */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?

- *(i) # 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 ofuseradd command with full options?

 # 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 "oracle user" -d /home/raju -s /bin/bash raju*

10. What is the syntax of adduser command with full options?

 # 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 "oracle user" -d /home/ram -s /bin/bash ram*

11. What is the syntax of newuser command?

 # 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?

 # 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?

We can check in different ways.

(i) # id <user name> (It shows the user id group id and user name if that is already created)

(ii) # grep <user name> /etc/passwd

14. How to verify or check the integrity of the password file?

 # 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 -----> read only*

-s -----> sort the contents by ***gid****in* ***/etc/group*** *and* ***/etc/gshadow*** *files.*

16. What is syntax of the usermod command with full options?

 # 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?

useradd -o -u 0 -g root <user name>

18. How to recover if the user deleted by mistake?

 # 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?

.bash_logout : is a user's logout ending program file. It will execute first whenever the user is logout.

.bash_profile : is user's login startup program file. It will execute first whenever the user is login. It consists the user's environmental variables.

.bashrc : This file is used to create the user's custom commands and to specify the umask values for that user's only.

20. What is a group?

The collection of users is called a group. There are two types of groups.

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

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?

groups <user name>

22. What is the syntax to create the group?

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?

groupmod <options><group name>

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 -R <group name> (to delete the group and apply changes to the root directory)

25. How to assign the password to the group?

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?

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?

grpconv (it creates the **/etc/gshadow** file from **/etc/group** file)

28. How to change the password aging policies?

we can change the password policies in 2 ways.
(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?

 # date -d "+ 45 days"

30. Explain the sudo user?

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?

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.*

%<group name> ALL=ALL
%oracle ALL=ALL or individual commands separated by commas,

* *We can also create one command alias and add some commands to that alias and mention that alias to users as follows.*

Cmnd_Alias NETWORKING=/usr/sbin/route, /usr/sbin/ifconfig
<user name> <machines>=<command alias name>
raju ALL=NETWORKING

* *We can also create one user alias and add the users to that alias and assign some commands to that alias as follows.*

User_Alias <user alias name>=<user1>, <user2>, <user3>, ...

Example : *User_Alias OURTEAM=raju, shyam, ram, gopal*
OURTEAM ALL=ALL (to give all permissions of sudo)
Defaults timestamp_timeout=0 (whenever the sudo user executes any command then it will ask password every command)

* *The above will apply to all users including root also. If we want to make it as only for normal users, then*

Defaults : <user1>, <user2>, <user3> timestamp_timeout=0 (the system will ask passwords for user1, user2, user3 to execute sudo commands)

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?

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)

34. 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/tcsh -----> c shell 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=" "%D" "%T" " (to display the date and time of each command temporarily)
 # 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=' %D %T '
*(save and exit the file and to update the effects by **#source /etc/bashrc** command)*
 # ~<user name> (to go to users home directory)
 # whatis <command> (to see the short description of that command)
 # whereis<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 -----> size 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)

35. How many types of the files are there?

There are 7 types of files.
1. *- -----> regular file*
2. *d -----> directory*
3. *c -----> character device file (Ex. console file, open and close terminals, ...etc.,)*
4. *b -----> block device file (Ex. device blocks like hard disks, CD/DVD disks)*
5. *s -----> socket file (programmers will deal this file)*
6. *p -----> pipe file (programmers will deal this file)*
7. *l -----> linked file (nothing but short cut file)*

36. What are permission types available in Linux and their numeric representations?

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

Permissions	File	Directory
r	Read a file Ex. # cat <file name>	Read a directory contents Ex. ls /dir

w	*Create, delete or modify the file contents*	*Create, delete or modify the files in a directory*
x	*Not required for file. It is required only for scripting files*	*Go to inside the directory Ex. # cd /dir*

37. What is syntax of chmod command with full options?

 # 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>

user (u) add (+) read (4) or (r) "

group(g) remove(-) write (2) or (w) "

other (o) equal (=) execute (1) or (x) "

38. What is the syntax of chown command with full options?

 # 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)

39. What is syntax of chgrp command with full options?

 # 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

40. What are the default permissions of a file and directory?

The default permissions of a file = 6 6 6

The default permissions of a directory = 7 7 7

41. What is umask in linux?

*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.*

42. How change the permissions using numeric representation?

The values for read = 4, write = 2, execute = 1 and null = 0. The total value = 4 + 2 + 1 = 7
 # 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)*
 # chmod 6 6 0 file2 (to give read and write to owner and read and write to group and null (0) permission to others)

43. Explain about set uid (suid)?

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/fdisk (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.*

44. Explain about set gid (sgid)?

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)

45. Explain about sticky bit?

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)

46. What are the uses of passwd and shadow files?

Passwd file : *(i) When we create the user one entry is updated in password and shadow files.*
(ii) It represents and tell about that user login name , uid, gid, default home directory of the use and default shell.
(iii) So, using this file we can easily get users information.

Shadow file : *(i) 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.*
(ii) If shadow file is missed or deleted we can recover those entries of shadow file using password file.
(iii) We can change the users encrypted passwords with the permissions of the higher authorities in case of emergency.

47. What is the use of group?

(i) In an organization the whole work is divided into departments for easy maintenance and easy administration.
(ii) For each department is also represented as group and that group having so many users to do different works.
(iii) 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.
(iv) 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.

48. Can we login to the user without password?

Yes, we can login.

49. How to recover the root password if missed or deleted?

RHEL - 6 :
(i) Restart the system.
(ii) Select 1st option and press 'e'.
(iii) Select 2nd option and press 'e'.
(iv) At the end give one blank space and type 1 and press Enter key.
(v) Then press 'b' to boot the system in single user mode.

(vi) Then prompt appears and type ***# passwd root*** *command.*
New password : XXXXXX
Retype password : XXXXXX
(vii) Exit
(viii) Then system starts as usual.

RHEL - 7 :
(i) Restart the system.
(ii) Using arrow keys select 1st line and press 'e' to edit.
(iii) Go to ***Linux 16*** *line press End key or* ***Ctrl + e*** *to go to the end of the line and give one space.*
(iv) Then type as ***rd.break console=tty1 selinux=0***
(v) Then press Ctrl + x to start the computer in single user mode.
(vi) After starting we get ***swith_root :/#*** *prompt appears and then type as follows.*
(vii) ***# mount -o remount, rw /sysroot*** *and press Enter and then type as follows.*
(viii) ***# chroot /sysroot*** *press Enter.*
(ix) Then ***sh - 4.2 #*** *prompt appears and type as*
(x) ***sh - 4.2 #passwd root***
New password : XXXXXX
Retype password : XXXXXX
(xi) ***sh - 4.2 # exit***
(xii) ***switch-root :/# exit***
(xiii) Then the system starts and the desktop appears.

50. How to restrict the users from login?

(i) By removing (deleting) the user we can restrict the user from login.
(ii) Put the user's hostnames as entries in ***/etc/hosts.deny*** *file (applying TCP wrappers).*
(iii) ***#passwd -l <user name>*** *(by locking his password we can restrict the users).*

51. How to put never expiry to a user?

 # passwd -x -1 <user login name>

52. Which one is the default sticky bit directory?

/tmp *is the default sticky bit directory.*

53. What is the purpose of the profiles?

(i) 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 :
(1) Only root user can set and applicable to all the users.
(2) Only global parameters can entered in this profile.
(3) The location of the global profile is ***/etc/bashrc***

Local profile **:**

(1) Every user has his/her own profile.
(2) The settings entered in this profile are only for that user.
(3) The location of the profile is ***.bash_profile*** *(hidden file) in that particular user's home directory.*

54. Can we mount/unmount the O/S file system?

No, we cannot mount or unmount the O/S file system.

55. How to find the users who are login and how to kill them?

 # fuser -cu (to see who are login)
#fuser -ck <user login name> (to kill the specified user)

56. what is Access Control List (ACL)?

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.

57. How to implement ACLs?

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>

58. How to check the ACL permissions?

 # getfacl <options><file or directory name>
The options are, -d -----> Display the default ACLs.
-R -----> Recurses into subdirectories.

59. How to assign ACL permissions?

 # 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

60. What is the syntax to assign read and write permissions to particular user, group and other?

 # 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?

 # 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?

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:
(i) # vi /etc/pam.d/system-auth
Modify as follows:
auth required pam_tally.so no_magic_root
account required pam_tally.so deny=3 no_magic_root lock_time=180 *Where,*
deny=3 *: Deny access if tally for this user exceeds 3 times.*
lock_time=180 *: Always deny for 180 seconds after failed attempt. There is also* ***unlock_time=n*** *option. It allow access after n seconds after failed attempt. If this option is used the user will be locked out for the specified amount of time after he exceeded his maximum allowed attempts. Otherwise the account is locked until the lock is removed by a manual intervention of the system administrator.*
magic_root *: If the module is invoked by a user with uid=0 the counter is not incremented. The sys-admin should use this for user launched services, like su, otherwise this argument should be omitted.*
no_magic_root *: Avoid root account locking, if the module is invoked by a user with uid=0*
Save and close the file.

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

 # 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?

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,

(i) user quotas
(ii) group quotas

Steps to enable :

First check whether the quota package is installed or not by
 # rpm -qa |grep quota *command.*
If quota ackage 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?

*(i) 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)*
*(ii) Update the quota on mount point by **# mount -o remount, usrquota <mount point>** command.*
*(iii) Create the user quota database by **# quotacheck -cu <mount point>** command (where -c means created the quota database and -u means user quota).*
*(iv) Check whether the quota is applied or not by **# mount** command.*
*(v) Enable the quota by **# quotaon <mount point>** command.*
*(vi) Apply the user quota for a user by **# edquota -u <user name><mount point>** command.*

File system	blocks	soft	hard	inodes	soft	hard
/dev/sdb1	0	0	0	0	0	0

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?

(i) 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 will be created.*
***har**d=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?

*(i) 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)

(ii) Update the quota on mount point by
***# mount -o remount, usrquota, grpquota <mount point>**command.*
(iii) 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).*
(iv) Check whether the quota is applied or not by
***# mount** command.*
(v) Enable the quota by
***# quotaon <mount point>** command.*
(vi) Apply the user quota for a user by
***# edquota -g <group name><mount point>** command.*

File system	blocks	soft	hard	inodes	soft	hard
/dev/sdb1	0	0	0	0	0	0

blocks -----> No. of blocks used (already)
soft -----> Warning limit
hard -----> Maximum limit
0 -----> Unlimited usage
inodes -----> No. of files created (already)
** Here we can specify the block level quota or file level quotas.*
** group quota can be applicable to all the users of that specified group.*
(save and exit the above quota editor)

67. How to change the password for multiple users at a time?

 # chpasswd (to change multiple user's passwords)
<user name 1> : <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.*

Chapter#2 – Managing Partitions and File Systems

1. What is partition?

A partition is a contiguous set of blocks on a drive that are treated as independent disk.

2. What is partitioning?

Partitioning means to divide a single hard drive into many logical drives.

3. Why we have multiple partitions?

- *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.*

4. What is the structure of the disk partition?

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

5. Explain the disk partition criteria?

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.

6. How to identify the disks?

- *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.*
- *FC -------→Fiber Channel*

7. What is file system?

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.

8. What are the different types of file systems supported in Linux?

- *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 RHEL7.*
- *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.*

9. How to create different types of partitions?

 # 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)

10. How to make a file system in Linux?

 # mkfs.ext2/ext3/ext4/xfs/vfat<device name> (for example/dev/sdc1)

11. How to mount the file systems temporarily or permanently?

 # 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)

12. How to delete the partition?

 # 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)

13. What is mounting and in how many types can we mount the partitions?

Attaching a parititon 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)

14. What are differences between the ext2, ext3, ext4 and xfs file systems?

S.No.	Ext2	Ext3	Ext4
1.	Stands for Second Extended file system.	Stands for Third Extended file system.	Stands for Fourth Extended file system.
2.	Does not having Journaling feature.	Supports Journaling feature.	Supports Journaling feature.
3.	Max. file size can be from 16 GB to 2 TB.	Max. file size can be from 16 GB to 2 TB.	Max. file size can be from 16 GB to 16 TB.
4.	Max. file system size can be from 2 TB to 32 TB	Max. file system size can be from 2 TB to 32 TB	Max. file system size can be from 2 TB to 1 EB *1EB = 1024 Peta bytes.

15. Which files are related to mounting in Linux?

- ***/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

16. The partitions are not mounting even though there are entries in /etc/fstab. How to solve this problem?

F*irst 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

17. When trying to unmounting it is not unmounting, how to troubleshoot this one?

Some times directory reflects error while unmounting because,
*(i) you are in the same directory and trying to unmount it, check with **# pwd**command.*
(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>

18. How to see the usage information of mounted partitions?

 # df -hT (to see device name, file system type, size, used, available size, use% and mount point)

19. How to see the size of the file or directory?

 # 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)*

20. How to assign a label to the partition?

 # 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)

21. How to mount a partition temporarily or permanently using label?

 # 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)

22. How mount the partition permanently using block id (UUID)?

 # 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)

23. What is the basic rule for swap size?

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

24. How to create a swap partition and mount it permanently?

 # 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)

25. What are the attributes of the file system?

(i) Inode number
(ii) File name
(ii) data block

26. What is inode number and what is the use of it?

Inode numbers are the objects the Linux O/S uses to record the information about the file.
Generally inode number contains two parts.
(a) Inode first part contains information about the file, owner, its size and its permissions.
(b) 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.

27. How to check the integrity of a file system or consistency of the file system?

 # 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.*

28. What is fsck check or what are the phases of the fsck?

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

29. Why the file system should be unmount before running the fsck command?

*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.*

30. Which type of file system problems you face?

(i) File system full

(ii) File system corrupted

31. How to extend the root file system which is not on LVM?

*By using **# gparted** command we can extend the root partition, otherwise we cannot extend the file systems which is not on LVM.*

32. How to unmount a file system forcefully?

 # umount -f <mount point>

 # fuser -ck <mount point>

33. How to know the file system type?

 # df -hT (command gives the file system type information)

34. How to know which file system occupy more space and top 10 file systems?

 # df -h <device or partition name> | sort -r | head -10

35. What is the command to know the mounted file systems?

 # mount or # cat /etc/mtab

36. How to know whether the file system is corrupted or not?

*First unmount the file systems and then run **fsck** command on that file system.*

37. How to recover if a file system is corrupted or crashed?

*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.

38. How to create a file with particular size?

 # dd if=/dev/zero of=/orafile bs=1MB count=500 (to create 500MB size /orafile with 4KB blocksize)

39. How to find how many disk are attached to the system?

 # fdisk -l (to see how many disk are attached to the system)

40. What is journaling?

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.

41. How to repair the Superblock of the file system?

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)

42. How to create the file systems with the user specified superblock reserve space?

 # mkfs.ext4 -m <no.><partition name> (to format the partition with <no.>% of reserve space to superblock)
Whenever we format the file system, by default it reserve the 5% partition space for Superblock.

43. How to modify the superblock reserve space?

 # tune2fs -m <no.><partition name> (to modify the superblock reserve space to <no.>%)

44. 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 -a (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 -AR -t no ext3 -y (to run fsck on all file systems except 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 ^has_journal /dev/sdb1 (to convert ext3 file system to ext2 file system)
 # tune2fs -O dir_index, has_journal, unit_bg /dev/sdb1 (to convert ext2 file system to ext4 file system)
 # tune2fs -O extents, dir_index, unit_bg /dev/sdb1 (to convert ext3 file system to ext4 file system)
 # mount -o remount, rw /dev/sdb1 (to mount the partition with read and write permissions)
 # 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 the location of the /run/log to another like /var/log/journal by*
 # 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).

Chapter#3 – Logical Volume Management and RAID Levels

1. What is LVM and why we go for LVM?

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.*

2. What are the components of the LVM?

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

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****.*

Physical Extent (PE) :

It is chunk of disk space. Every physical volume is divided into a number of equal sized PEs.

Volume Group (VG) :

It is composed of a group of physical volumes and logical volumes. It is the organizational group of LVM.

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.

Logical Extent (LE) :

It is also a chunk of disk space. Every logical extent is mapped to a specific physical extent.

3. How to create the LVM, make a file system and mount that permanently?

(i) 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.

(ii) Convert the Physical disk into physical volumes by,

```
# pvcreate   /dev/sdb   /dev/sdc
```

(iii) 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>
```

(iv) 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>
```

(v) Make a file system on the above created logical volume by,

 # mkfs.ext2/ext3/ext4/xfs /dev/<volume group name>/<logical volume name>

(vi) Create a mount point to mount the above created LVM file system by,

 # mkdir /mnt/<directory name>

(vii) 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)

4. How to see the details of the Physical Volumes?

 # 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)

5. How to see the details of the Volume Groups?

 # 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)

6. How to see the details of the Logical Volumes?

 # 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)

7. How to extend the Volume Group?

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)

8. How to extend the logical volume and update it's file system?

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 # xfs_growfs** commands.*

Example : # df -hT
 # lvextend -L +<size in MB></dev/vgname/lvname> or
 # lvresize -L +<size in MB></dev/vgname/lvname>
 # resize2fs </dev/vgname/lvname>
 # lvdisplay </dev/vgname/lvname> (to check the size of the logical volume)
 # df -hT (to check the size of the file system)

9. How to reduce the logical volume and update the file system?

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)

10. How to move or migrate the logical volume data from one physical volume to another physical volume?

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
```

11. How to delete or remove the logical volume?

*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)
```

12. How to delete or remove the volume group?

*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)
```

13. How to delete or remove the physical volume?

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)

14. How to restore the volume group which is removed mistakenly?

*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 **#vgscan**and the logical volume state by **# lvscan** commands.*
*Then activate that volume group by **# 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.

 # mount -a

15. How to change the volume group name and other parameters?

 # 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)
Ex: # 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)

16. How to change the logical volume name and other parameters?

 # 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)

17. How to disable the volume group and logical volume?

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

18. How to take a backup of the volume group?

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

19. What is the configuration file of the logical volume?

 # cat /etc/lvm/lvm.conf (to see the contents of the LVM configuration file)

20. What are the locations of the logical volume and volume groups?

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

21. How to know the current version of the LVM package?

 # rpm -qa lvm (to know the current version of the LVM package)*

22. What are the attributes of the volume group?

 # 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)

23. How to extend the logical volume to max. disk space and half of the disk space?

 # lvextend -l +100% FREE <logical volume>
(to extend the logical volume by adding the volume group's total available space)
 # lvextend -l 50% <vgname><lvname>
(to extend the logical volume by adding the 50% free space of the volume group)

24. How to check on which physical volume the data is writing in the logical volume?

 # 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)

25. How many types of file systems available?

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

26. How to scan and detect the luns over the network?

 # ls /sys/class/fc_host (to check the available fibre channels)
 # echo "---" > /sys/class/scsi_host/<lun no.>/scan (to scan and detect the luns over the network)

27. How to mount a pen drive in Linux?

 # 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)

28. How to mount a CD/DVD ROM drives in Linux?

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)

29. How to mount the " .iso " image files in Linux?

 # 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)

30. What is RAID? What is the use of the RAID and how many types of RAIDs available?

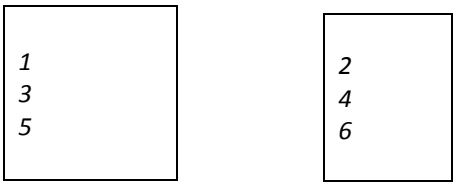
RAID stands for Redundant Array of Independent Disks.
It provides fault tolerance, load balancing using stripping, mirroring and parity concepts.
There are mainly two types of RAIDs available.
(i) Hardware RAID (Depends on vendors and also more expensive)
(ii) Software RAID (Does not depends on vendors and less expensive when compared to Hardware RAID and also it is maintained by system administrator only.

31. How many types of software RAIDs available and their requirements?

(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

32. How to configure RAID - 0 in Linux?

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 ....

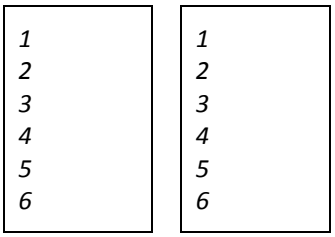


If the Disk - 1 is /dev/sdb and the Disk - 2 is /dev/sdc then,

```
# 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_device=3  (to grow the RAID - 0 file system)
```

33. How to configure RAID - 1 in Linux?

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 ....



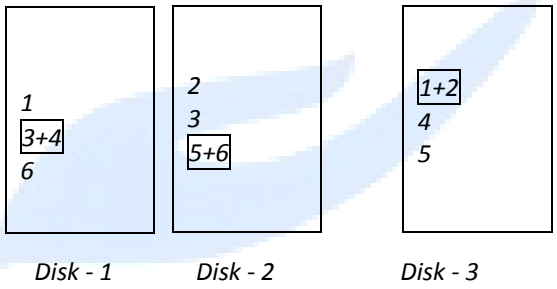
If the Disk - 1 is /dev/sdb and the Disk - 2 is /dev/sdc then,

```
# 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_device=3  (to grow the RAID - 1 file system)
```

34. How to configure RAID - 5 in Linux?

To configure RAID - 5, minimum 3 disks are required and the partition id is "fd".
In every disk approximately 25 - 30% of space is reserved for parity.
Reading 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 ....



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_device=4  (to grow the RAID - 5 file system)
```

35. What are the main advantages of RAID - 5

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.*

36. How will you troubleshoot if one of the eight disks failed in LVM?

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.

37. What is pvmove and when it is used in LVM?

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.

38. How to inform the client and then troubleshoot if the disk is full?

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.

39. Did you work on storage?

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.

40. I have four disks each 1TB in RAID - (1+0). So, total how much disk space can I utilize in that *RAID (1+0)?* *RAID - (1+0) means Mirroring + Stripping. It requires 4 disks, ie., 2 disks for mirroring and remaining 2 disks for stripping. And 5 - 10% disk space is used for superblock information. So, finally we can utilize 2TB - 2TB X 10% disk space in that RAID - (1+0).*

41. If two disks failed in RAID - (1+0), can we recover the data?

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.

42. How many types of disk space issues can we normally get?

(i) Disk is full.
(ii) Disk is failing or failed.
(iii) File system corrupted or crashed.
(iv) O/S is not recognizing the remote luns when scanning, ...etc.,

43. What is a link file and how many types?

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.
(i) Soft link (ii) Hard link

44. What is soft link and how to create it?

Soft link is nothing but a short cut file. If original file is deleted, no use of short cut file. ie., we cannot access the original data by selecting the link file. Soft link can be applied on both directories and files. These files can be stored in any of the file system. ie., the original file may be in one file system and the link file may be on another file system. If we edit any file, the link files are also updated automatically. When we create a soft link file, the permissions are full permissions. The soft link file and the original file inode no's are different. The size of the soft link file is same as the length of the original file name. The soft link can be created by

 # ln -s <original file or directory><link file or directorywith path> (to create a soft link)

 # ln -s /root/script /root/Desktop/script (to create a link file for the script and stored on root Desktop)

45. What is hard link and how to create it?

Hard link in nothing but a backup file. If the original file is deleted, there is no effect on hard link file. i.e., we can access the original file data even though the link file is deleted. Hard links can be applied on files only not on directories. Hard link files can be stored in the same file system. ie., original and hard link files both should be in the same file system not on different file systems. The inode no's are same for original and hard link files. If the original is edited, the updations are applied on both original and hard link files. The size of the hard link file is same as the size of the original file.

46. What are the commands to search files and directories?

To search files and directories there are two commands.

(i) # locate

(ii) # find

47. Explain the locate command and how to use it?

locate always looks the locate database and not in a specific location. The data of the locate is stored in /var/lib/mlocate/mlocate.db file. If the data is not updated in locate database or the locate database is available or locate database is deleted, we cannot locate the files and directories. # updatedb is the command to update the locate database. locate database cannot be find the newly created files and directories. It is not recommended to use on production servers because it impacts on performance of the servers. So, to overcome this problem we normally use # find command on production servers.

 # updatedb (to update the locate database)

 # locate <file name/directory name> (to search the specified file or directory)

48. Explain the find command and how to use it?

find command required the specific location. Without specific location we cannot find the files or directories.

 # find <location><options><file or directory> (to find the specific file or directory)

The options are,

-name -----> search files and directories

-prem -----> search for permissions

-size -----> search for sizes

-user -----> search for the owner

-uid -----> search for files/directories of uid)

-gid -----> search for files/directories of gid)

-group -----> search for group owner

-empty -----> search for empty files
-amin -----> search for access time
-mmin -----> " "
-cmin -----> " "
-atime -----> search for access day (access day, minutes, hrs, ...etc)
-mtime -----> search for modify day (change the content)
-ctime -----> search for change day (permissions, ...etc)

Examples :

find / -name <file name> (to search for file names in / directory)
find / -name <file name> -type f (to find file names only)
find / -name <directory name> -type d (to find directories with small letters only)
find / -iname <file/directory name> -t d (to search for small or capital letter files/directories)
#find / -empty (to search empty files or directories)
find / -empty -type f (to search for empty files only)
find / -empty -type d (to search for empty directories only)
find / -name " *.mp3" (to search for .mp3 files only)
find / -size 10M (to search for exact 10M size file/directories)
find / -size -10M (to search for less than 10M size files/directories)
find / -size +10M (to search for greater than 10M size files/directories)
find / -user student (to search for student user files/directories)
find / -group student (to search for student group files/directories)
find / -user student -not -group student
(to search for student user files and not student group files)
find / -user student -o -group student
(to search for student user and student group files/directories)
find / -uid <uid no.>
(to search for files/directories which belongs to the user having the specified user id)
find / -gid <gid no.>
(to search for files/directories which belongs to the group having the specified group id)
find / -prem 755 (to search file/directories which are having the permissions 755)
find / -prem -755 (to search file/directories which are having the permissions below 755 and also at least one match also)
find / -mmin 20 (to search for files/directories which are modified within 20 minutes,
+20 ----> above 20 minutes and -20 -----> below 20 minutes)
find / -mtime 2 (to search files/directories which are modified within 2 days)
find / -name "*.mp3" -exec rm -rf { } \; (to search all .mp3 files and delete them)
find / -name "*.mp3" -exec cp -a { } /ram \ ;
(to search all mp3 files and copy them into /ram directory)
find / -user student -exec cp -a { } /ram \;
(to search student user's files and directories and copy them into /ram directory)
find / -nouser -exec mv -a { } /home/ram \;
(to search files/directories which are not belongs to any user and move them into /home/ram directory)
du -h / |sort -r |head -n 10 (to search 10 big size files in reverse order)

Chapter#4 – Networking Configuration and Troubleshooting

1. What is Network?

Combination of two more computers connected together to share their resources each other by means of communication like cable is called Network.

2. What is Networking?

It is a connection between two or more computers to communicate with each other.

3. what are the basic requirements for networking?

(a) NIC (Network Interface Card or controller)
(b) Media (nothing but cables)
(c) Topology
(d) Protocol
(e) IP Addresses

4. Explain about NIC card?

A Network Interface Card or controller is hardware component that connects a computer to a computernetwork. Each NIC card will be having MAC (Media Access Controller) address to avoid conflicts between same NIC adapters. In Linux these NIC adapter is represented by the word "eth" . For example if two NIC cards are there in a system then it will be denoted as "eho","eth1", ...etc.,

5. What is media?

Media is nothing but cable to connect two or systems. Example : RJ 45, CAT 5 and CAT 6, ...etc.,

6. What is topology?

Topology is a design in which the computers in network will be connected to each other. Example for topologies are Bus, Ring, Star, Mesh, Tree topologies.

7. What is protocol?

A Network Protocol defines rules and conventions for communication between the network devices. Protocols are generally use packet switching techniques to send and receive messages in the form of packets. Example for protocols are TCP/IP (Transmission Control Protocol and Internet Protocol), UPD (User Datagram Protocol) and HTTP (Hyper Text Transfer Protocol), ...etc.,

8. What are the differences between TCP/IP and UDP protocols?

TCP/IP	UDP
Transmission Control Protocol	User Datagram Protocol
It is connection oriented	It is connection less
Reliable	Non-Reliable
TCP Acknowledgement will be sent / received	No Acknowledgement
Slow communication	Fast communication
Protocol No. for TCP is 6	Protocol No. for UDP is 17
HTTP, FTP, SMTP, ...etc., uses TCP	DNS, DHCP, ...etc., uses UDP

9. What is an IP address?

Every Computer will be assigned an IP address to identify each one to communicate in the network. The IP address sub components are Classes of an IP address, Subnet masks and Gateway.

***Classes of IP address** :*

The IP addresses are further divided into classes. The classes are A, B, C, D, E and the ranges are given below.

Class	Start	End	Default Subnet mask	Classless Inter Domain Routing
Class A	0.0.0.0	127.255.255.255	255.0.0.0	/8
Class B	128.0.0.0	191.255.255.255	255.255.0.0	/16
Class C	192.0.0.0	223.255.255.255	255.255.255.0	/24
Class D	224.0.0.0	239.255.255.255		
Class E	240.0.0.0	255.255.255.255		

10. What is loopback address?

A special IP number (127.0.0.1) is designated for the software loopback interface of a machine. 127.0.0.0 and 127.255.255.255 is also reserved for loopback and is used for internal testing on local machines.

11. What is multicasting?

Multicasting allows a single message to be sent to a group of recipients. Emailing and Teleconferencing are examples of multicasting. It uses the network infrastructure and standards to send messages.

12. What is subnet mask?

A subnet mask allows the users to identify which part of an IP address is reserved for the network and which part is available for host use.

13. What is Gateway?

A Gateway is the network point that provides entrance into another network. On the internet a node or stopping point can be either gateway node or a host (end point) node. Both the computers of internet users and the computer that serve the pages to users are host nodes. The computer that control traffic within your company's network or at our local internet service provider (ISP) are the gateway nodes.

14. What are important configuration files in network configuration?

 # cat /etc/sysconfig/network

(This file keeps the information about the hostname assigned to the system and if we want to change the hostname permanently, we need to change the hostname in this file)

 # cat /etc/sysconfig/network-scripts/

*(This directory keeps the configuration of network devices connected to the system. Examples are **ifcfg- eht0, ifcfg-eth1, ifcfg-eth2,** .....etc.,)*

 # cat /etc/hosts

(This file is responsible for resolving hostname into IP address locally. ie., local DNS if DNS server is not available)

 # cat /etc/resolve.conf

(This file keeps the address of the DNS server to which the clients will be accessing to resolve IP address to hostname and hostname to IP address)

15. What are the differences between MAC and IP addresses?

MAC Address	***IP Address***
It is a permanent address. So we cannot change this address.	*It is a temporary address. So, we can change this address any no. of times.*
It stands for Media Access Control Address.	*Internet Protocol address.*
It is a physical address.	*It is a logical address.*
It is divided into 6 parts. *--- : --- : --- : --- : --- : --- (each 8 bits. So, 8 X 6 = 48 bits*	*It is two types.* ***IPV4 :****(It is divided into 4 parts)* *--- . --- . --- . --- (each 8 bits. So, 8 X 4 = 32 bits* ***IPV6 :*** *(It is divided into 16 parts)* *--- . --- . --- . --- . --- . --- . --- . --- . --- . --- . --- . --- . --- . --- . --- . --- (each 8 bits. So, 8 X 16 = 128 bits.*
ifconfig *(to see the MAC address)*	***# ifconfig*** *(to see the IP address)*

16. How many types of NIC cards available?

(a) eth0 (1st NIC card)
(b) eth1 (2nd NIC card)
(c) br0 (Bridge -----> used for communication from physical to virtual)
(d) lo (loopback device name and IP address is 127.0.0.1)
 # ifconfig (to see all the NIC devices connected to the system)

17. How many types of cable connections available?

(i) Cross cable (to connect two systems directly)
(ii) Straight cable (to connect more systems with the help of switch)
 # ethtool <device name> (to check the network cable is connected or not)
 # miitool <device name> (It is also used to check the network cable but it will not supports RHEL - 7 and only supports RHEL - 6 and it also works on physical system only not on virtual system)

18. In how many ways we can configure the network?

There are two ways to configure the network.
(a) Static Network.
(b) Dynamic Network.

Static Network :

In this way we assign the IP address and hostname manually. Once we configure the IP address, it will not change.

Dynamic Network :

In this way we assign the IP address and hostname dynamically. This means the IP address will change at every boot.

19. How to assign the static IP address to the NIC card?

In RHEL - 6 :

 # setup
(Move the cursor to Network configuration and press Enter key)
(Move the cursor to Device configuration and press Enter key)
(Select the NIC adapter ie., eth0 and press Enter key)
(Assign the above IP address and other details as per our requirements and move the cursor to "OK" and press enter key)
(Move the cursor to "Save" to save the changes in device configuration and press Enter key)
(Once again move the cursor to "Save & Quit" button and press Enter key)
(Finally move the cursor to "Quit" button and press Enter key to quit the utility)
(Then restart the network service and check for the IP address by # service network restart command)
(If the change is not reflected with the above service, then restart the network manager by ***# service NetworkManager restart*** *command)*
 # ifconfig (to see the IP address of the NIC card)
 # ping < IP address > (to check whether the IP is pinging or not)

In RHEL - 7 :

 # nmcli connection show (to see all the network connections)
 # nmcli device show
(to see the network details if already configured manually or dynamically)
 # nmcli connection add con-name "System eth0" ifname eth0 type ethernet
(to add the network connection)
 # nmcli connection modify "System eth0" ipv4.addresses ' < IP address >/< netmask >< gateway > ' ipv4.dns < dns server IP address > ipv4.dns-search < domain name> ipv4.method <static or manually>
(to assign IP address, gateway, dns, domain name and configure the network as static or manually)
 # nmcli connection up "System eth0" (to up the connection)
 # systemctl restart network (to restart the network service)
 # systemctl enable network (to enable the network service)
 # ifconfig (to see the IP address of the NIC card)
 # ping < IP address > (to check whether the IP is pinging or not)

20. What are the differences between RHEL - 6 and RHEL - 7 network configuration files?

RHEL – 6	RHEL - 7
/etc/sysconfig/network-scripts is the directory which contains the NIC configuration information.	/etc/sysconfig/network-scripts is the directory which contains the NIC configuration information.
/etc/sysconfig/network-scripts/ifcfg-<device name> is the file which contains the NIC configuration details.	/etc/sysconfig/network-scripts/ifcfg-<device name> is the file which contains the NIC configuration details.
/etc/resolve.conf is the file which contains DNS server IP and domain name location.	/etc/resolve.conf is the file which contains DNS server IP and domain name location.
/etc/sysconfig/network is the hostname configuration file.	/etc/hostname is the hostname configuration file.
/etc/hosts is the file which contains the local DNS server IP address.	/etc/hosts is the file which contains the local DNS server IP address.

21. What are the differences between Dynamic and Static configuration information?

Dynamic configuration information	*Static configuration information*
Device =<NIC device name>	*Device =<NIC device name>*
HWADDR=02:8a:a6:30:45	*HWADDR=02:8a:a6:30:45*
Bootproto=DHCP	*Bootproto=none (means static network)*
Onboot=yes (yes means whenever we restart the system this connection will be activated and no means whenever we restart the system the connection will be deactivated)	*Onboot=yes*
Type=Ethernet	*Type=Ethernet*
Userctl=yes/no ----> If it is yes all normal users can disable the NIC card and If it is no except root user nobody can disable the NIC card.	*Userctl=yes/no ----> If it is yes all normal users can disable the NIC card and If it is no except root user nobody can disable the NIC card.*

22. How to set the hostname temporarily and permanently?

RHEL - 6 :

 # hostname <fully qualified domain name> *(to set the hostname temporarily)*
 # vim /etc/sysconfig/network *(to set the hostname permanently)*
HOSTNAME=<fully qualified domain name>
(save and exit this file)
 # service network restart *(to update the hostname in the network)*
 # chkconfig network on *(to enable the connection at next reboot)*

RHEL - 7 :

 # hostname <fully qualified domain name> *(to set the hostname temporarily)*
 # hostnamectl set-hostname <fully qualified domain name> *(to set the hostname permanently)*
 # systemctl restart network *(to update the hostname in the network)*
 # systemctl enable network *(to enable the connection at next reboot)*

23. How to troubleshoot if the NIC is notworking?

*(a) First check the NIC card is present or not by **# ifconfig** command.*
(b) If present thencheck the status of the NIC card is enabled or disabledby click on System menu on the status bar, then select Network Connections menu.
(c) Click on IPV4 settings tab, select the device eth0 or any other and select Enable button, then Apply, then OK.
*(d) Open **/etc/sysconfig/network-scripts/ifcfg-eth0** file check Userctl=yes or no. If it is yes make it as no, then check Onboot= yes or no. If it is no make it as yes and save that file.*
(e) If not present thencheck the status of the NIC card is enabled or disabled by click on System menu on the status bar, then select Network Connections menu.
(f) Click on IPV4 settings tab, select the device eth0 or any other and select Enable button, then Apply, then OK.
*(g) Using **# setup** (in RHEL - 6) or **# nmcli** (in RHEL - 7) commands assign the IP address to the system and restart the network service by **# service network restart** (in RHEL - 6) or **# systemctl restart network** (in RHEL - 7) commands and enable the service at next reboot by **# chkconfig network on** (in RHEL - 6) or **# systemctl enable network** (in RHEL - 7) commands.*
*(h) Then up the connection by **# ifconfig eth0 up** (in RHEL - 6) or*

 # nmcli connection up <connection name> *commands.*

(i) Even though it is not working may be the fault in NIC card. If so, contact the hardware vendor by taking the permissions from higher authorities.

24. What is bonding and how to configure bonding? (from RHEL - 6)

What is link aggregation or bridging or teaming and how to configure teaming? (from RHEL - 7)

Bonding or Teaming or Bridging:

Collection of multiple NIC cards and make them as single connection (virtual) NIC card is called bonding.
It is nothing but backup of NIC cards.
In RHEL - 6 it is called as Bonding or Bridging.
In RHEL - 7 it is called as Teaming or Link aggregation.
There are 3 types of backup in Bonding or Teaming.
(a) Mode 0 -----> Round Robbin
(b) Mode 1 -----> Activebackup
(c) Mode 3 -----> Broadcasting

Mode 0 :

It provides load balancing and fault tolerance.
Data will be shared by both NIC cards in round robbin.
If one NIC card failed then another NIC card will be activated to communicate with the server
So, there is a load balancing and fault tolerance features.

Mode 1 :

Activebackup means only one NIC card is activated at a time and another one is in down state.
So, there is no load balancing.
But if one NIC card is failed then another NIC card will be activated automatically.

Mode 3 :

In this mode broadcasting is done.
In this the same data will be transferred through two NIC cards.
So there is no load balancing.
But if one NIC card is failed then second NIC card will be activated automatically.
So, all the 3 modes are supports only fault tolerance, but round robbin is the only one mode that provides load balancing.

Requirements to configure :

(i) Minimum two NIC cards.
(ii) One IP address.
(iii) Connection type is bond (in RHEL - 6) and team (in RHEL - 7) not the ethernet type.
Here no need to assign the IP addresses for two NIC cards and we are giving only one IP address to bond or team.

Bonding configuration : (in RHEL - 6)

(i) # vim /etc/sysconfig/network-scripts/ifcfg-bond0
DEVICE=bond0
IP ADDR=<IP address>
TYPE=ethernet
NETMASK=255.225.225.0 or <IP address class netmask>

ONBOOT=yes
BOOTPROTO=none
USERCTL=no
MASTER=yes
BONDING_OPTS="mode0 or mode1 or mode3 miimon=50" *(Save and exit this file)*

(ii) vim /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
MASTER=bond0
SLAVE=yes *(Save and exit this file)*

(ii) vim /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
MASTER=bond0
SLAVE=yes *(Save and exit this file)*

(iv) ***To add virtual NIC cards eth1 and eth2 :***
 # setup -----> Networking -----> Device configuration -----> New Device -----> eth1
Name : eth1
Device : eth1 *(save and exit this setup)*
 # setup -----> Networking -----> Device configuration -----> New Device -----> eth2
Name : eth2
Device : eth2 *(save and exit this setup)*

(v) Adding bond0 connection :
 # setup -----> Networking -----> Device configuration -----> New Device -----> bond0
Name : bond0
Device : bond0
IP address : <IP address>
Netmask : 255.255.255.0
Default gateway : <gateway IP address> *(save and exit this setup)*
 # ifdown bond0
 # ifdown eth1
 # ifdown eth2
 # ifup bond0
 # service NetworkManager stop
 # service network restart
 # chkconfig network on
 # service NetworkManager restart
 # cat /proc/net/bonding/bond0 *(to check the bonding information)*
 # watch -n 1 cat /proc/net/bonding/bond0 (to check the bonding information for every 1 minute)
 # echo "eth1" > /sys/devices/virtual/net/bond0/bonding/active_slave

(to put the eth1 NIC in active state)

Teaming configuration :

(i) Add the team0 connection by

 # nmcli connection add con-name team0 ifname team0 type team config ' { "runner" : { "name" : "roundrobbin" or "activebackup" or "broadcasting" }} '

(iii) Add the two NIC cards one by one to the above created connection by

 # nmcli connection add con-name port1 ifname eth1 type team-slave master team0

 # nmcli connection add con-name port2 ifname eth2 type team-slave master team0

(iii) Assign the static IP address to the team0 connection by

#nmcli connection modify team0 ipv4.addresses <IP address>/<netmask> ipv4.method static

(iv) Up the connection by

 # nmcli connection up team0

(v) To see the team0 connection up details by

 # teamdctl team0 state

(vi) To check the connection communication by

 # ping -I team0 <IP address>

(vii) To down the one NIC card in team0 by

 # nmcli connection down port1

(viii) teamdctl team0 state (to check the team0 NIC card up or down details)

25. What is the difference between TCP and UDP protocol?

TCP is a connection oriented protocol and contain the information of sender as well as receiver.
Example : HTTP, FTP, Telnet
TCP is slower than UDP due to its error checking mechanism
UDP protocols are connection less packets have no information to where they are going. These type of ports are generally used for broadcasting.
For example : DNS, DHCP
UDP are faster

26. What are the benefits of NIC Teaming?

(i) Load balancing
(ii) Fault Tolerance
(iii) Failover

27. Mention all the network configuration files you would check to configure your ethernet card?

*(i) /etc/sysconfig/network-scripts/ifcfg-eth**
(ii) /etc/sysconfig/network
(iii) /etc/resolve.conf
(iv) /etc/nsswitch.conf

28. What is the use of /etc/resolve.conf?

It contains the details of nameserver, i.e., details of your DNS server which helps us connect to Internet.

29. What is the use of /etc/hosts file?

To map any hostname to its relevant IP address.

30. What is the command to check all the open ports of your machine?

#nmap localhost

31. What is the command to check all the open ports of remote machine?

 # nmap <IP address or hostname of the remote system>

32. What is the command to check all the listening ports and services of your machine?

 # netstat -ntulp

33. How can you make a service run automatically after boot?

 # chkconfig <service name> on

34. What are the 6 run levels of linux? And how can you configure your script to run only when the system boots into GUI and not to any other runlevel?

0 Power off
1 Single user
2 Multi user without network
3 Multiuser with network
4 Development purpose
5 GUI
6 Restart

```
# chkconfig --level 5 service_name on
# chkconfig --level 1234 service_name off
```

35. What is a 3 way handshake protocol? Give an example of it.

SYN - system 1 sends SYN signal to remote system.
SYN-ACK - remote system receives the syn signal and sends ack signal.
ACK - system again receives ack signal from remote system and connection is established.
For Example: When you ping to a machine you are sending a SYN signal which is ACK by the remote machine then it sends a SYN ACK signal back to the host machine. Then the host machine receives SYN ACK and sends the ACK signal back to confirm the same.

36. What are the possible ways to check if your system is listening to port 67?

```
# nmap localhost | grep 67
# netstat -ntulp | grep 67
```

37. Explain about IPV6?

It's length is 128 bits. It's netmask is 64
 # nmcli connection modify "System eth0" ipv6.addresses 2005:db8:0:1::a00:1/64 ipv6.method static (to add the IPV6 version of IP address to the connection "System eth0")
 # nmcli connection modify "System eth0" ipv4.addresses '172.25.5.11/24 172.25.5.254' ipv4.dns 172.25.254.254 ipv4.dns-search example.com ipv4.method static ipv6. addresses 2005:ac18::45/64 ipv6.method static (to assign ipv4 and ipv6 IP addresses to "System eth0 connection)
 # nmcli connection down "System eth0" (to down the "System eth0" connection)
 # nmcli connection up "System eth0" (to up the "System eth0" connection)

38. How to troubleshoot if the network is not reaching?

(i) First check the network cable is connected or not by # ethtool <NIC device name> command. if connected then check the IP address is assigned or not by # ifconfig <NIC device name> command.
(ii Then check the system uptime by # uptime command.
(iii) Then check the network services status by # service network status and
 # service NetworkManager status commands.
(iv) Then check the network service at Run Level by # Chkconfig --list network command.
(v) Then check whether the source network and destination network are in the same domain or not.
(v) Then finally check the routing table by # route -n command.

Other useful commands :

 # ping <IP address or hostname> (to check the pinging)
Normally the ping command pings continuously until a stop signal reaches by Ctrl + c, so to avoid continuous pinging by
 # ping -c <number><IP address> (to ping upto the specified no of times)
 # ipcalc -m <IP address) (to find the subnet mask for that specified IP address)
Normally IP addresses are assigned by ISP (Internet Service Provider) and managed by IANA (Internet Assign Number Authority)
 # ifconfig (to see or check all the NIC device names and IP addresses)
 # ethtool <NIC device name> (to check the network cable is connected or not)
 # miitool <NIC device name> (It is also used to check the network cable but it works on physical system not on virtual system and supports in RHEL - 6 only)
 # ip addr show (to show all NIC devices present on the system)
 # hostname (to see the hostname with fully qualified domain name)
 # hostname -i (to see the IP address of the system)
 # hostname -d (to check the domain name of the system)
 # hostname -s (to check the hostname without domain name)
 # netstat -r (to check the default gateway and routing table)
 # route (to check the default gateway with routing table)
 # ip route (to display the NIC device with default gateway)
 # dig or # host or #nslookup (all are used to resolve the name to IP and IP to name)
 # nslookup <IP address> (to resolve IP to name)
 # nslookup <hostname> (to resolve name to IP)
 # host <IP address> (to resolve IP to name)
 # host <fully qualified domain name> (to resolve name to IP address)
 # dig -x <IP address> (to resolve IP address to name)
 # dig <fully qualified domain name> (to resolve name to IP address)
 # nmcli (Network Manager Command Line Interface used to configure the network setup in RHEL - 7)
 # setup (to setup the static network in RHEL - 2, 3, 4, 5 and 6)
 # nmtui (to setup the static network in GUI mode for RHEL - 7)
 # nmcli device show (It displays all the NIC devices network information of the system)
 # nmcli device show eth0 (to see all the network devices information of the eth0)
 # nmcli connection or nmcli connection show (to see all the network connection names)
 # nmcli connection add con-name <connection name> ifname <NIC device name> type ethernet

(to create a new connection name for eth0)
 # nmcli connection show --activate (it shows which connection is active currently)
 # nmcli connection add con-name <connection name> ifname <NIC device name> type ethernet
(to add a connection name to NIC device)
 # nmcli connection modify <connection name> ipv4.addresses ' <IP address>/<netmask> <defaultgateway> ' ipv4.dns <dns server IP address> ipv4.dsn-search <domain name> ipv4.method <static/manual>
(to modify the connection as static and assign the IP, gateway, dns IP, domain name)
 # nmcli connection delete <connection name> (to delete the specified connection)
 # nmcli connection modify <connection name> ipv4.method <static/manual>
(to modify dynamic connection to static connection)
 # nmcli connection up <connection name> (to activate or up the specified connection)
 # nmcli connection down <connection name> (to disable or down the specified connection)
 # nmcli connection show <connection name> (to see the information about the specified NIC device)
 # ping -I <NIC device name><IP address> (to check the connection from NIC device to IP address)
 # hostname <fully qualified domain name> (to set the hostname temporarily)
 # hostnamectl set-hostname<fully qualified domain name> (to set the hostname permanently in RHEL- 7)

NOTE: *Whenever we change any parameters in /etc/sysconfig/network-scripts/ifcfg-<NIC device name> file, then we have to reload that file and again we have to up the connection (nothing but activate the connection by # nmcli connection reload command.*
 # nmcli connection reload (to reload the configuration of the connection if any changes on it and it reloads all configuration files)
 # nmcli connection reload /etc/sysconfig/network-scripts/ifcfg-<NIC device name>
(to reload a single file)
 # hostnamectl status (it displays full details of the hostname and works in RHEL - 7 only)
 # nmcli networking off (to disable all the connections at a time)
 # nmcli device status (to display all NIC device connections statuses)
 # nmcli connection modify <connection name> + ipv4.dns <secondary dns server IP>
(to add a secondary dns server IP to the existing connection)
 # netstat -ntulp (to check how many open ports are there in local system)
 # ss -ntulp (" ")
 # nmap (to check how many open ports are there in remote system)
 # tracepath (it displays the routing information)
 # miitool <NIC device name> (to check the network cable is connected or not)
 # ethtool <NIC device name> (" ")
 # ifconfig (to check the NIC card is enable or not)
 # ifup <NIC device name> (to enable or up the NIC card)
#ifdown <NIC device name> (to disable or down the NIC card)
 # route -n (to check the gateway)
 # cat /etc/resolve.conf (to check the dns server information)
 # cat /etc/sysconfig/network-scripts/ifcfg-<NIC device name> (to see the NIC device information)
 # hostname or cat /etc/sysconfig/network (to check the hostname in RHEL - 6)
 # hostnamectl status or cat /etc/hostname (to check the hostname in RHEL - 7)
 # ping <IP address> (to check the connection communication)

 # chkconfig --list (to list all the services which are running at boo time in RHEL - 6 & 7)
 # systemctl list-unit-files (to list all the processes which are running at boot time in RHEL - 7)
 # chkconfig --level <service name> (it will set the service at run level 3 when the system is booting)
 # service --status-all (to see the list of all the processes which are currently running)
 # ls /etc/init.d (is the location of all the services and deamons in RHEL - 6)
 # ls /usr/lib/systemd/system (is the location of all the services and deamons in RHEL - 7)
 # /etc/rc.local (is the last script to be run when the system is booting)
*(If we enter as **sshd** **stop** at the last line of the script file then **sshd** will be stopped even though that **sshd** is enabled)*
 # service sshd status (to check the sshd status)
 # service --service -all (to see the process ID of all the services)
 # netstat -ntulp (to see all the services with port no., status, process ID and all open ports in local system, routing table and NIC device information)
-n -----> port no. (numeric no) -t ----->tcp protocol
-u -----> upd protocol -l -----> port is listening or not
-p -----> display the process ID
 # netstat -r (to see all routing table information)
 # netstat -i (to see all the NIC cards information)
 # nmap (to see the network mapping ie., open ports list on remote system)
***Note** : By default this command will not available. So, first install the **nmap** package by*

 # you install nmap -y
 # nmap <remote system IP address>
(to see all the services which are running in the specified remote system)
 # nmap <remote IP 1><remote IP 2><remote IP 3>
(to see the running services on specified remote systems)
 # nmap 172.25.0.11 - 50 (to see the running service on 172.25.0.11 to 172.25.0.50 systems)
 # nmap -p 80 <remote IP> (to see the http port is running or not on specified remote system)
 # nmap -p 80 - 90 <remote IP>
(to see port no's 80 to 90 are running or not on remote systems)
 # nmap -sp 172.25.0.0/24 (to see all the systems which are in upstate ie., 172.25.0.1, 172.25.0.2, 172.25.0.3, ...upto 172.25.0.254 systems)
(where s -- scan & p -- ping)
Open a file, write all the systems IP addresses, save & exit the file. Example has given below,
 # vim coss
172.25.2.50
172.25.3.50
172.25.4.50 ....etc., (save and exit this file)
 # nmap -iL coss
(to scan all the IP addresses by reading the coss file)(where -i ----> input, -L ----> list)
 # nmap --iflist (to see all the routing table information in the network)
 # nmap 172.25.0.10 - 20 --exclude 172.25.0.15
(to scan all the systems from 172.25.0.10 to 172.25.0.20 systems and excluding 172.25.0.15 system)
 # nmcli connection show --active (to control the network connections)
 # ip link (to check the network connection)
 # ping -I eth1 <IP address> (to check the 2nd NIC card connection)

Chapter#5 –Managing SELinux

1. What is SELinux?

It is a one type of security that enhances the security that allows users and administrators more control over which users and applications can access which resources, such as files, Standard Linux access controls etc.,
It is mainly used to protect internal data (not from external data) from system services. In real time SELinux is disabled and instead of this IP tables are used. It protects all the services, files and directories by default if SELinux is enabled.

2. In how many ways we can implement the SELinux? Explain them.

We can implement the SELinux mainly in 2 modes.
(i) Enabled
(ii) Disabled (default mode)
***Enabled** :*
Enabled means enabling the SELinux policy and this mode of SELinux is divided into two parts.
(a) Enforcing
(b) Permissive
***Disabled** :*
Disabled means disabling the SELinux policy.

3. What is Enforcing mode in SELinux?

Enforcing means SELinux is on. It checks SELinux policy and stored a log. No can access the services by default but we can change the policy whenever we needed.

4. What is Permissive mode in SELinux?

SELinux is on and it don't check SELinux policy and stored the log. Everybody can access the services by default and we can also change the SELinux policy. It is also called as debugging mode or troubleshooting mode. In this mode SELinux policies and rules are applied to subjects and objects but actions are not affected.

5. What is Disabled mode in SELinux?

SELinux is turned off and no warning and log messages will be generated and stored.

6. What are Booleans?

Booleans are variables that can either be set as true or false. Booleans enhance the effect of SELinux policies implemented by the System Administrators. A policy may protects certain deamons or services by applying various access control rules.

7. What is SELinux policy?

The SELinux policy is the set of rules that guide the SELinux security engine. It defines types for file objects and domains for process. It uses roles to limit the domains that can be entered and the user identities to specify the role that can be attained.

8. What are the required files for SELinux?

 # vim /etc/selinux/config -----> It is main file for SELinux.
 # vim /etc/sysconfig/selinux -----> It is a link file to the above file.
 # vim /var/log/audit/audit.log -----> SELinux log messages will be stored in this file.

9. what is the command to see the SELinux mode?

 # getenforce (to check the SELinux mode)

10. What is command to set the SELinux mode temporarily?

 # setenforce 0 or 1 (to set the SELinux mode. Where ' 0 ' -----> permissive and ' 1 ' -----> Enforcing)

***Note** : (i) To change the SELinux mode from Permissive to Enforcing or Enforcing to Permissive modes the system restart is not required.*

(ii) To change Enforcing mode to Disabled mode or Disabled mode to Enforcing mode the system restart is required.

*(iii) The above commands are changed the SELinux mode temporarily only. To make the selinux changes permanently then open **/etc/selinux/config** and go to ,*

***SELINUX=Enforcing or Permissive or Disabled** (save and exit this file)*

11. What is command to see the SELinux policy details?

 # sestatus (to see the SELinux policy details)

***Other useful commands** :*

 # ls -Z <file name> (to see the SELinux context of the file)
 # ls -ldZ<directory name> (to see the SELinux context of the directory)
 # ps -efZ | grep <process name>(to see the SELinux context of the process running on the system)
 # ps -efZ | grep http (to see the SELinux context of the http process running on the system)
 # chcon -t <argument><file/directory name> (to change SELinux context of the file or directory)
*# chcon -t public_content_t /public (to change the SELinux context of the **/public** directory)*
*# chcon -R public_content_t /public (to change the SELinux context of the **/public** directory and its contents)*
 # restorecon -v <file/directory name> (to restore the previous SELinux context of the file/directory)
 # restorecon -v /public (to restore the previous SELinux context of that directory)
 # restorecon -Rv <directory> (to restore the previous SELinux context of the directory and its contents)
 # restorecon -Rv /public (to restore the previous SELinux context of the /public directory and its contents)
 # getsebool -a | grep <service name> (to see the booleans of the specified service)
 # getsebool -a | grep ftp (to see the booleans of the ftp service)
 # setsebool <boolean><option on/off> (to change the boolean of a specified service)
 # setsebool allow_ftpd_anon_write on (to change the boolean of the ftpd service temporarily)
 # setsebool -P <service name> = <0/1> (to change the boolean for the service on or off permanently)
 # setsebool -P samba_export_all_rw = 1 (to change the boolean for samba service permanently on)

Chapter#6 – Booting Procedure and Kernel Parameters

1. Explain the booting procedure?

In Linux systems the booting is done in 6 stages.

BIOS
MBR
GRUB
Kernel
Init
Runlevel

BIOS :

BIOS stands for Basic Input and Output System. Whenever we power on the system , the system runs self diagnostic checks and detects all the connected input and out peripherals. This process is called POST (Power On Self Test). If any errors found it displays on the screen. Then BIOS locates the booting disk in the system and locates and loads the Primary boot loader nothing but MBR (Master Boot Record) into the memory. So, in simple terms the BIOS loads the MBR into memory and executes the MBR.

MBR :

MBR stands for Master Boot Record. It is located in the 1st sector of the bootable disk (it may be /dev/hda or /dev/sda). The size of the MBR is 512 bytes and it contains three components.
(i) Primary boot loader information and its size is 446 bytes.
(ii) Partition table information and its size is 64 bytes.
(iii) MBR validation check and its size is 2 bytes. Its main purpose is whether the MBR is valid or not.
The primary boot loader contains the secondary boot loader nothing but GRUB or LILO (in old systems). Then primary boot loader locates and loads the secondary boot loader into memory.
So, in simple terms the MBR loads and executes the GRUB boot loader.

GRUB or LILO :

GRUB stands for Grand Unified Boot loader. LILO stands for Linux Loader and is used in old Linux systems. If we have multiple kernel images installed in our system, we can choose which one to be executed. GRUB displays a splash screen, waits for few seconds. If we do not enter anything, it loads the default kernel image as specified in the grub configuration file. GRUB has the knowledge of the file system (the old LILO didn't understand the system). GRUB configuration file is ***/boot/grub/grub.conf*** *(****/etc/grub.conf*** *is a link to this). This file contains kernel and initrd images. So, in simple terms GRUB just loads and executes kernel and initrd images.*

Kernel :

Kernel initialises itself and loads the kernel modules and mounts the root file system as specified in the "root=" in grub.conf and then kernel executes the ***/sbin/init*** *program. Since init was the 1st program to be executed by Linux kernel, it has the process ID (PID) of 1. We can see this id by* ***# ps -ef | grep init*** *command. initrd stands for initial RAM Disk. initrd is used by kernel as temporary file system until kernel is booted and the real root the file system is mounted. It also contains necessary drivers compiled inside which helps it to access the hard drive partitions and other hardware.*

init level :

*In this init program reads the **/etc/inittab** file and put the system into specified run level. init identifies the default run level from **/etc/inittab** file and we can change the this default run level whenever we needed. We can find the default run level by **# grep "initdefault" /etc/inittab** command on our system. Normally the default run level in Linux is 3 in CLI (Command Line Interface) mode and 5 in GUI (Graphical User Interface)mode.*

Run Level Programs :

The following run levels are available in Linux systems.

0 -----> halt or shutdown the system
1 -----> Single user mode
2 -----> Multi user without NFS
3 -----> Full multi user mode but no GUI and only CLI mode
4 -----> Unused
5 -----> Full multi user mode with GUI (X11 system)
6 -----> reboot the system

Whenever we start the Linux system is booting we can see various services getting started. Those services are located in different run levels programs executed from the run level directory as defined by our default run level. Depending on our default init level setting, the system will execute the programs from one of the following directories.

Run level 0 -----> /etc/rc.d/rc0.d
Run level 1 -----> /etc/rc.d/rc1.d
Run level 2 -----> /etc/rc.d/rc2.d
Run level 3 -----> /etc/rc.d/rc3.d
Run level 4 -----> /etc/rc.d/rc4.d
Run level 5 -----> /etc/rc.d/rc5.d
Run level 6 -----> /etc/rc.d/rc6.d

*The above directories are also having symbolic links available for those directories under **/etc/rc0.d, /etc/rc1.d,** ....etc., So, the /etc/rc0.d is linked to /etc/rc.d/rc0.d*

Booting procedure in RHEL - 7:

*Upto kernel the booting process is same as the above. **/boot/grub2/grub.conf** is the GRUB configuration file in RHEL - 7. **systemd** is the initial process in RHEL - 7 and its process ID is **1**. **linux16** read the root (/) file system and then **initrd16**process will mount the root (/) file system in read & write mode and starts the **systemd**process. And the **systemd** process will read the **/etc/fstab** file and mount all the file systems. Then it reads the file **/etc/systemd/system/default.target** file and brings the system into the default run level according to the scripts the processes will start or stop.*

2. How to check the current run level of the system?

 # who -r (to see the present run level of the system)

3. How to change the default run level?

First open the /etc/inittab file by # vim /etc/inittab command and go to last line change the run level number as we required and then reboot the system by # init 6 command. After rebooting the system check the current run level by # who -r command.

4. How to start the graphical interface if the system is in run level 3 now?

 # startx (it changes the run level 3 to 5 and reboots the system)

5. How to troubleshoot if the boot disk is not available?

(i) First check the hard disk is present in the system or not. If not present connect the hard disk and restart the system.

(iv) If the hard disk is present, then go to BIOS and find the location of the hard disk.

(v) Check the boot priority in the BIOS. If boot priority is not the hard disk then change it to hard disk and restart the system.

(iv) Even though the system is not started then boot the system with CDROM in single user mode and open the /boot/grub/grub.conf file and see the hard disk name and partition number. Normally it should be /dev/hda1 (if the hard disk is IDE hard disk) or /dev/sda1 (if the hard disk is SATA or SCSI). If the hard disk name and partition number is different instead of the original then change them and reboot the system with hard disk.

(v)If the GRUB is corrupted then reboot the system with CDROM in single user mode and restore the grub information from the recent backup and then restart the system with hard disk.

6. How to reboot the production server?

(i) In general the production servers will not be rebooted frequently because the end users will suffer if the productions server are in down state. If any changes made to the system like grub, selinux policy, default run level is changed and if kernel patches are applied the system reboot is required.

(ii) If any inconsistency is root (/) file system, then take the business approval from higher authorities,make a plan for proper scheduleand also inform to the different teams like application team to stop the application, databaseteam to stop the databases, QC team to stop the testing, monitoring people to ignore the alerts from thisserver and other teams if any and then reboot the system withCDROM in single user mode and then run #fsck command on that file system.

(iii) If O/S disk is corrupted or damaged then, reboot the system temporarily with the mirror disk then fix that problem and again boot the system with original disk.

7. What is the difference between # reboot and # init 6 commands?

Both commands are used to restart or reboot the system.
 # reboot command will not send the kill signals to the system and it will kill all the running processes and services forcefully and then restart the system.
 # init 6 command will send the kill signals to the system and it will stop all the processes and services one by one and then restart the system.

8. What is console port and how to connect to the console port?

Console port is used to connect the system even though the system is not booted with the main O/S. This port is used to connect the system for troubleshooting purpose only. We can connect the console port as same as connect to systems LAN port and it is also having IP address, user name and password to connect to the console.

There are different types of console ports for different types of servers. They are given below.

Server Name	Name of the Console port	Expansion name
DELL	DRAC or i-DRAC	DRAC ---> DELL Remote Access Controllers i-DRAC ---> Integrated DELL Remote Access Controllers
IBM Power series	HMC	Hardware Management Console
HP	ILO	Integrated Light Out

9. System is continuously rebooting. How to troubleshoot it?

(i) Connect the system through console port through putty by providing IP address, user name and password.

(vi) At console prompt and boot with CDROM in single user mode and mount the root (/ ---> O/S) file system on temporary mount point.

(vii) Check any wrong entries in the cron jobs ie., crontab editor see any reboot scripts are there or not. If found remove those entries and reboot the system.

(iv) If the above is not resolved, then check the memory (RAM).

(viii) If RAM module is not working the system get panic and it may continuously reboots.

(ix) If the RAM module is working then check the RAM size whether the sufficient RAM that requires to run the application is available or not. If not there then increasing the RAM size may be resolve this issue.

(vii) Check "/var/log/messages" file for any messages regarding continuous rebooting.

(x) Even though there is a sufficient RAM may be swap space is not sufficient to run all the services and applications then system get panic and may continuously reboots. If so, then increasing the swap size may resolve this issue.

10. What is TCP handshaking?

The procedure that takes place between two TCP/IP nodes to establish a connection. Known as the Synchronization, Synchronize-Acknowledgement and Acknowledgement handshake.

For example if computer A transmits a Synchronize packet to computer B, which sends back a Synchronize- Acknowledge packet to compute A. Computer A then transmits an Acknowledge packet to computer B and the connection is established. This whole above said process is called the TCP handshaking.

11. How many links will be created when we create the directory?

Whenever we create any directory there are two links will be created.

12. What are the differences between run level 2 and run level 3?

Run Level 2 :

(i) It supports multiuser operations.

(ii) Multiple users can access the system.
(iii) All the system deamons will run except NFS and some other network service related deamons.
(iv) So, without NFS we can use all other services.

Run Level 3 :
(i) It is also supports Multi user operations.
(ii) Multiple users can access the system.
(iii) All the system deamons including NFS and other network related service deamons will run.
(iv) So, we can avail all the services including NFS also.

13. Server running in single user mode, can you login remotely and how?

We can login to the system remotely in single user mode also but it is possible to connect to console instead of LAN port through putty tool by giving IP address, user name and password. Then console port appears and boot the system with CDROM in single user mode.

14. How to check the present kernel version?

 # uname -r (it displays the present kernel version)
 # uname -a (it displays the present kernel version with other details)
 # cat /boot/grub/grub.conf (in this file also we can find the kernel version)

15. What is the command to see the system architecture?

 # arch or
 # uname -m (both commands gives the architecture of the system)

16. How to check the version of the O/S ?

 # cat /etc/redhat-release (gives the version of the O/S)

17. How to repair the corrupted boot loader and recover it?

This problems may be occur if the GRUB is corrupted. So, we have to recover the GRUB. Basically the repairing of GRUB means installing the new grub on the existing one from RHEL - 6 DVD. The steps are given below.
(i) Insert the RHEL - 6 DVD and make sure that system should boot from CD/DVD.
(ii) Boot the system in Rescue Installed System mode.
(iii) Select the language with which we want to continue and click on OK.
(iv) Select the Keyboard type as US and click OK.
(v) Select Local CD/DVD and click OK.
(vi) Move the cursor to NO to ignore the Networking.
(vii) Move the cursor to Continue tab to mount the root (/) from CD/DVD and press Enter key.
(viii) Now the root (/) file system is mounted on /mnt/sysimage, here click on OK and Press Enter to continue.
(ix) Select the "shell Start shell" option and click on OK, then shell will be displayed on screen.
(xi) At shell prompt type as # chroot /mnt/sysimage command, press Enter.
(xii) Check the /boot partition by
 # fdisk -l command.

(xiii) Install the new grub on the boot device ie., may be /dev/sda2 by
 # grub-install <device name>
command (For example
 # grub-install /dev/sda2).
(xiv) If it show no error reported that means we have successfully recovered the grub.
(xv) Then type # exit command and again type
 # exit or
 # reboot command to reboot the system.

18. What are Modules or Kernel Modules? How to find the Kernel Modules?

The drivers is Linux system are known as Modules or Kernel Modules. These modules are assigned by kernel depending on the hardware. Hardware can only be communicated and can work efficiently when the proper module is loaded in the kernel. we can find the kernel modules by # ls /etc/lib/modules command.
*All the kernel modules in the system will be ended with " .ko " extension. So, we can see all the modules in the system by # find / -name *.ko command.*

19. What other commands related to kernel modules?

 # lsmod (to list all the currently loaded modules)
 # lsmod |grep -i <module name> (to check whether the particular module is loaded or not)
 # lsmod |grep -i fat (to check the fat module is loaded or not)
There might be a situation where our module is not working properly, in that case we have to remove that module and re-install it again by,
 # modprobe -r <module name> (to remove the specified module)
 # modprobe -r fat (to remove the fat module)
 # modprobe <module name> (to install or re-install the module)
 # modprobe fat (to install or re-install the module)
 # modinfo <module name> (to see the specified module information)
 # uname (to see the which O/S is present in the system)
 # uname -s (to see which O/S kernel is this either Linux or Unix)
 # rpm -qa kernel --last (to see the kernel installation date and time)
 # rpm -qa kernel (to see how many kernels are there in the system)*
 # ls /proc (to see the kernel processes information)
 # ls /boot (to see the present kernel version created time)
 # ls /etc/lib/modules (installed kernel module drivers)
 # ls /usr/src (kernel source code location)
 # kudzu (to scan the new hardware in RHEL - 4)
 # depmod (to scan the new hardware from RHEL - 5, 6 and 7)
 # rmmod <module name> (to remove the specified module)
 # insmod <module name> (to install the kernel module without dependency modules)

20. How to see the run level?

 # who -r (to see the current run level)

21. How to block the USB / CDROM driver?

 # lsmod |grep -i usb (to see the USB module is loaded or not)
 # mount (to check the USB is mounted or not)
 # modprobe -r usb_storage (remove the USB module, if it is mounted it will not remove)
 # umount /<mount point> (to unmount the USB if it is mounted)
 # vim /etc/modprobe.d/blocklist.conf (it will open the blocklist.conf file, then put an entry of USB)
blocklist usb_storage (after type this save and exit this file)

22. What is " wait " and where it is stored?

(i) If there is not enough memory to run the process, then it will wait for free space in memory. That process is called wait.
(xi) wait is stored in buffer like cache memory.

23. What is run level?

(i) Run level is nothing but to put the system in different levels to perform different maintenance modes.
(ii) There are 7 run levels. Those are 0, 1, 2, 3, 4, 5 and 6.
(iii) The above levels are used to put the system in different stages to avail different services.

24. What is the default run level?

(i) When we boot the server the system automatically go to one particular run level. That run level is called the default run level.
(xii) In Linux the default run level is 5 in GUI and 3 in CLI.
(iii) We can modify the default run level by put an entry in /etc/inittab file.

25. Which run level are you using?

Run level 3.

26. How to change the run level temporarily?

 # init <run level no.> (to change the run level temporarily)
Example : # init 0 or
#init 1 or
 # init 2 or
 # init 3 or
#init 4 or
#init 5 or
#init 6

27. Can I mount on two disks alternatively when booting?

No it is not possible to mount on two disks alternatively when booting because we can specify only one disk as boot disk but not two disks as booting disks in BIOS settings.So, it is not possible to mount on two disks alternatively when booting.

Chapter#7 – Job Automation

1. What is Job scheduling?

*The process of creating the jobs and make them occur on the system repeatedly hourly, daily, weekly, monthly and yearly is called Job scheduling. In Linux and other Unix systems this process is handled by the **cron** service or deamon called **crond**and **atd** is the at jobs deamon which can be used to schedule the tasks (also called as jobs).*

2. What is the importance of the job scheduling?

The importance of the job scheduling is that the critical tasks like backups, which the client usually wants to be taken in nights, can easily performed without the intervention of the administrator by scheduling a cron job. If the cron job is scheduled carefully then the backup will be taken at any given time of the client and there will be no need for the administrator to remain back at nights to take the backup.

3. What are the differences between cron and at jobs?

***cron job** :*

(i) cron jobs are scheduling jobs automatically at a particular time, day of the week, week of the month and month of the year.

(ii) The job may be a file or file system.

(iii) We cannot get the information as a log file if the job was failed to execute ie., when it was failed and where is was failed and also cannot execute automatically the failed jobs.

***at job** :*

(iv) at jobs are executes only once.

(v) Here also we cannot get the information if the job is failed and it is also do not execute the failed jobs automatically.

4. What are the important files related to cron and at jobs?

/etc/crontab *-----> is the file which stores all the scheduled jobs.*

/etc/cron.deny *-----> is the file used to restrict the users from using cron jobs.*

/etc/cron.allow ***----->*** *is used to allow only users whose names are mentioned in this file to use cron jobs and this file does not exist by default.*

/etc/at.deny *----->same as cron.deny for restricting the users to use at jobs.*

/etc/at.allow *-----> same as cron.allow for allowing users to use at jobs.*

5. What is the format of the cron job?

 # crontab -e (to edit the cron job editor to create or remove the cron jobs)

<minutes><hours><day of the month><month of the year><day of the week><job or script>

(0 - 59) (0 - 23) (1 - 31) (1 - 12 or jan, feb, ...) (0 - 6 or sun, mon, ...)

Options	Explanation
*	Is treated as a wild card. Meaning any possible value.

*/5	Is treated as ever 5 minutes, hours, days or months. Replacing he 5 with any numerical value will change this option.
2, 4, 6	Treated as an OR, so if placed in the hours, this could mean at 2, 4 or 6 o-clock
9-17	Treats for any value between 9 and 17. So if placed in day of the month this would be days 9 through 17 or if put in hours, it would be between 9 AM and 5 PM.

6. How to check the assigned cron jobs of currently login user?

```
# crontab -l -u <user name>     (to check the specified user's assigned cron jobs)
# crontab -l -u raju            (to check the raju user's assigned cron jobs)
# crontab -l                    (to check the root user's assigned cron jobs)
```

7. How to allow or deny cron jobs for a user?

For allow	For deny
(i) Open **/etc/cron.allow** file.	(i) Open **/etc/cron.deny** file.
(ii) Put the entries of the user names whom do we want to allow the cron jobs.	(ii) Put the entries of the user names whom do we want to deny the cron jobs.

8. What is at job and atq source?

(i) at jobs are executes only once.
(ii) atq means how many at jobs are in queue by **# atq** command.

9. How to check the jobs?

```
# at -l                         (to check the at jobs)
```

10. How to add crontab entry in command mode?

```
(i)  # define editor=vim        (to define the editor as vim)
(ii) # export $editor           (export the defined editor)
(iv) # crontab -e               (to edit the crontab)
```

11. How to troubleshoot if the cron job failed?

(i) See the crontab entries for syntactical errors. If there are any errors then correct them, otherwise it will not execute.

(ii) Check whether the **crond** deamon is working or not. If it is running, then stop the deamon and again start the deamon. Even though the problem occurs, then the crontab entries may be wrong.

(v) If all the above are ok, then see whether the user who executing cron job has permissions to execute the cron jobs or not ie., check the user entries in **/etc/cron.allow** and **/etc/cron.deny** files.

(vi) If all are ok, again put the job entry in crontab and execute it.

12. How to schedule the cron task or job?

(i) Open one shell script file..

(ii) Enter all the commands which are required to complete the task or job.
(iii) If the job requires more CPU and more memory, then schedule those jobs at night time or non-peak hours (generally night time is the non-peak time).
(iv) Then open crontab editor by
 # crontab -e <user name> *command and then put the entries as below,*
<minutes><hours><day of the month><month of the year><day of the week><script name with path>
(v) Save and exit from the crontab editor.

13. How to add at job and delete the at job?

Adding :

(i) # at <time> (to enter the at job)
(ii) Before that open a file vim and enter the job commands in that file and save as xxxx.sh (some name with extension must be as .sh)
(iii) Enter the above saved file name within the at job editor.
(iv) Press Ctrl + d to exit from the editor.
(v) Then system will assign a job id to that job. We can see the list of at jobs by # atq command.

Delete :

(vi) See the job id which job we want to delete by ***# atq*** *command and note that job id.*
(vii) Then delete that job by ***# at -r <job id>*** *command.*

14. How to know currently scheduled at jobs?

 # atq (to see the currently scheduled at jobs)

15. How to allow or deny at jobs for a user?

For allow	For deny
(i) Open ***/etc/at.allow*** *file.*	*(i) Open* ***/etc/at.deny*** *file.*
(ii) Put the entries of the user names whom do we want to allow the at jobs.	*(ii) Put the entries of the user names whom do we want to deny the at jobs.*

16. Where is the location of the crontab and at jobs?

/var/spool/cron -----> is the crontab file location.
/var/spool/at -----> is the at jobs file location.

17. Where is the location of the crontab and at jobs log files?

/var/log/cron -----> is the log file location for both cron and at jobs.

Other useful commands :

 # service atd restart (to restart the atd deamon in RHEL - 6)
 # chkconfig atd on (to enable the atd deamon at next boot in RHEL - 6)
 # service atd status (to see the status of the atd deamon in RHEL - 6)
 # service atd stop (to stop the atd deamon in RHEL - 6)
 # service atd start (to start the atd deamon in RHEL - 6)

 # service crond restart *(to restart the crond deamon in RHEL - 6)*
 # chkconfig crond on *(to enable the crond deamon at next boot in RHEL - 6)*
 # service crond status *(to see the status of the crond deamon in RHEL - 6)*
 # service crond stop *(to stop the crond deamon in RHEL - 6)*
 # service crond start *(to start the crond deamon in RHEL - 6)*
 # systemctl restart atd *(to restart the atd deamon in RHEL - 7)*
 # systemctl enable atd *(to enable the atd deamon at next boot in RHEL - 7)*
 # systemctl status atd *(to see the status of the atd deamon in RHEL - 7)*
 # systemctl stop atd *(to stop the atd deamon in RHEL - 7)*
 # systemctl start atd *(to start the atd deamon in RHEL - 7)*
 # systemctl restart crond *(to restart the crond deamon in RHEL - 7)*
 # systemctl enable crond *(to enable the crond deamon at next boot in RHEL - 7)*
 # systemctl status crond *(to see the status of the crond deamon in RHEL - 7)*
 # systemctl stop crond *(to stop the crond deamon in RHEL - 7)*
 # systemctl start crond *(to start the cron deamon in RHEL - 7)*
 # at -l *(to see the list of at jobs)*
 # atq *(to see the jobs in the queue)*
 # atrm <job id> *(to remove the specified at job)*
 # at <time> *(to set the at job to be executed at the specified time)*
 # at 9:30 *(to set the at job to be executed at 9:30 AM)*

Example : *# at 9:30*
at> useradd gopal
at> groupadd manager
at> rm -rf /opt
*at> tar -cvf /root/etc.tar /etc/**
press Ctrl + d to save and exit from at job

 # at -r <job id> *(to remove the specified job)*
** at jobs can be performed only one time. It cannot repeat daily.*
** at jobs once scheduled, we cannot edit the jobs or modify the time of the job.*
 # at now +5min *(to execute the at job now after 5 minutes)*
at> touch f1 f2 f3
at> mkdir /ram
at><EOT> or Ctrl + d *(to save and exit from at job editor)*
 # tailf /var/log/cron *(to see the last 10 lines of at or cron log file contents)*
 # at Jan 20 2015 *(to schedule the at job on 20th Jan 2015)*
 # at 5PM Jan 13 2015 *(to schedule the at job on 13th Jan 2015 at 5PM)*
 # at noon + 4days *(to schedule the at job today and after 4 days)*
 # at midnight *(to schedule the at job today midnight)*
 # at midnight + 4days *(to schedule the at job today midnight and after 4 days)*
 # vim /etc/at.deny *(to deny the at jobs for specified users)*
 # vim /etc/at.allow *(to allow the at jobs for specified users)*
** If both /etc/at.deny and /etc/at.allow files are deleted, except root user every user will be deny to execute at jobs.*
** Once scheduled the cron jobs, we can modify, edit that job any no. of times.*
 # cat /etc/crontab *(to see the cron jobs list)*

 # crontab -lu <user name> (to list all the cron jobs of the specified user)
 # crontab -eu <user name> (to create or edit the cron jobs)
 # crontab -ru <user name> (to erase or remove the specified user's cron jobs)
 # crontab -r <job id> (to remove the specified cron jobs)
 # vim /etc/cron.deny (to deny the cron jobs for specified users)
 # vim /etc/cron.allow (to allow the cron jobs for specified users)
** If both files are remove or deleted, except root user all the users are deny to execute the cronjobs.*
 # crontab -eu raju
55 14 20 1 2 /usr/sbin/useradd gopal; usr/sbin/groupadd team
(save & exit this crontab)
** This job executes the useradd and groupadd commands on Tuesday 20th Jan every year*

Examples for crontab :

(i)58 14,15 20-25 1 2,3,6 /usr/sbin/passwd
where 58 -----> 58 minutes
14,15 -----> 14 hours and 15 hours (14:58 and 15:58)
20-25 -----> dates 20, 21, 22. 23, 24 and 25
1 -----> January
2, 3, 6 -----> 2nd day, 3rd day and 6th day

*(ii) 58 15 * * * <command>*
where 58 -----> 58 minutes
15 -----> 15 hours (at 15:58)
** * * -----> every day*

*(iii) 58 */2 * * * <commands>*
where 58 -----> 58 minutes
**/2 -----> Every 2 hours*
** * * -----> every day*
*(iv) 00 */2 * * * sync ; echo "---" > /sys/class/scsi_hosts/host2/scan*
(vii) @reboot <mail command> (every reboot, one mail will be send to the root)
(viii) @monthly <command> (every month the command will be executed)
(ix) @yearly <command> (every year the specified command will be executed)

(viii) @reboot /usr/sbin/ or /bin/sh /root/coss.sh
(every reboot the specified script file will be executed)
** If the system is scheduled for a job, but at that time the system is under down then anacron command is responsible for those pending jobs to be executed.*

 # cat /etc/anacron is the configuration file for anacron jobs.
 # anacron (anacron is used to execute the pending cron jobs)
 # vim /etc/rc.local (to execute the cron pending jobs automatically whenever the system is rebooted)
** Open the above file and go to last line and type as, anacron then save and exit this file to execute the pending jobs automatically whenever the system is rebooted.*

Chapter#8 – Administrating Remote Systems

1. What is remote administration and explain it?

(i) Remote administration means administration of servers which are located in remotely.
(ii) Normally servers are placed in datacenters like books arranged in a rack.
(iii) These datacenters are normally located in US, UK and Australia ... etc.,
(iv) Generally we login as normal user in local systems and get the remote desktop or console using remote desktop tools like putty, VNC server, ... etc.,
(vi) If it is through remote desktop, we can manage the servers using the GUI tools.
(vii) If it is through putty, we can manage the serves using command line interface only. In both ways we should give server name or IP address, port no., user name and password.

2. What is SSH and explain it?

SSH is stands for Secure Shell. It was designed and created to provide the best security when accessing another computer remotely. Not only does it encrypt the session, it also provides better authentication facilities. On windows systems install the putty software and through putty we can access the remote system by configuring ssh. SSh is protocol which facilitates secured communication between two systems using Client-Server architecture and allows users to login to the server host systems remotely. It is used to connect to remote system and perform administrative task or jobs. By default ssh takes password authentication mechanism and its port no. is 22. Through ssh the data will be transferred in encrypted format.

3. What is telnet?

Telnet is a mechanism to connect and to administrate the remote system from local system. This is the oldest program which is available on most network capable operating systems. Accessing a remote shell account through the telnet method is danger because in that everything that you send or receive over that telnet session is visible in plain text on your local network and the local network of the machine you are connecting to. So, anyone can sniff the connection in-between can see our user name, password, email and other messages that we read and command that we run. For these reasons we need a more sophisticated program than telnet to connect to a remote host.

4. What are the differences between Telnet and SSH?

Telnet	***SSH***
(a) Through telnet we can connect the remote system, but any network hacker may see the transferred data. And the telnet port no. is ***23.***	*(a) Through ssh also we can connect the remote system, but nobody can see the transferred data. And the ssh port no. is* ***22.***
(b) Data will be transferred in non-encrypted format.	*(b) Data will be transferred in encrypted format.*
(c) We cannot trust this telnet connection.	*(c) We can trust this ssh connection.*
(d) We cannot give the trusting in telnet.	*(d) We can give the trusting in ssh.*

(e) By snooping or sniffing technologies we can see the data like system or hostname, login name, password and other data. So, there is no security.	*(e) By snooping or sniffing technologies we cannot see the data like system name or hostname, login name, password and other data. So, there is a security*
(f) # telnet<IP address of the remote system> (provide login name and password)	*(f) # ssh<IP address of the remote system> (provide login name and password)*

5. In how many ways we can connect the remote host through ssh?

Through ssh we can connect the remote host by two methods.

(i) Command Line Interface (CLI).
Example : # ssh <IP address of the remote system> (provide login name and password)

(ii) Graphical User Interface (GUI).
Example : open VNS server window and provide remote hostname, login name and password.

6. What are the requirements for ssh?

(i) Remote systems IP address.
(ii) Remote systems user name and password
(iii) A proper network ie., our local and remote systems should be in the same network.
(iv) Open ssh package to configure the ssh.

7. In how many ways we can connect the remote system?

(i) telnet *(ii) ssh*
(iii) rlogin *(iv) rcp*
(v) ftp *(vi) scp*
(vii) sftp *(viii) tftp*

8. What is the syntax for ssh?

 # ssh <IP address of the remote system> -l <user name>
 # ssh <user name>@<IP address of the remote system>
 # ssh <user name>@<remote hostname with fully qualified domain name>
** After executing any of the above commands, it may asks user name and password.*
Then type user name and
passwords to connect the remote systems.

9. How to configure the ssh with keybased authentication or explain the ssh trusting?

(i) SSH keybased authentication is used to access the remote system without asking any passwords.
(ii) For that, first we have to generate the public and private keys by executing # ssh-keygen command on our system. Then the public and private keys are generated in /home/<user name>/.ssh location. ie., .ssh directory in users home directory. And the keys are id_rsa (private key) and id_rsa.pub (public key).
(iii) Then copy the public key id_rsa.pub on the remote system by executing the below command. # ssh-copy-id -i <user name>@<IP address of the remote system>
(iv) Go to remote system and check whether the above key is copied or not by # cat /home/<user name>/.ssh/authorized_keys file. And the private key should be in our system.
(vi) Whenever we are trying to establish a connection the public key on remote system should

be matched with the private key on our system. otherwise there is no connection is established.

(vii) If both public and private keys are matched then connection will be established and first time it will ask the password. Once the connection is established, next time onwards it won't ask any passwords.

 # ssh <user name>@<remote hostname or IP address> (first time it will asks the password)

(viii) The authentication is done through the public and private keys, so this type of authentication is called keybased authentication.

10. How to prevent the remote login root user or how to configure the ssh to prevent the remote *login for root?*

(i) The location of the ssh configuration file is /etc/ssh/sshd_config

(ii) Open the configuration file by # vim /etc/ssh/sshd_config

-----> go to line no. 42 (in RHEL - 6) or

-----> go to line no. 48 (in RHEL - 7) PermitRootLogin yes and uncomment that line and type as " no " in place of " yes " andsave and exit this file.

(iii) Then restart the or reload the sshd deamon by

 # service sshd restart (to restart the sshd deamon or service in RHEL - 6)
 # systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
 # chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
 # systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
 # service sshd reload (to reload the sshd deamon in RHEL - 6)
 # systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

(iv) Then no root user cannot access our system remotely through ssh service.

11. How to allow the remote users to run GUI commands through ssh?

(i) Open ssh configuration file by # vim /etc/ssh/sshd_config

-----> go to line no. 109 in RHEL - 6 or

-----> go to line no. 117 in RHEL - 7 X11 Forwarding no

type as " yes " in place of " no " then save and exit this file.

** If it is yes, then GUI commands can be executed on the remote system.*

** If it is no, then GUI commands cannot be executed on the remote system.*

(ii) Then restart the sshd service or deamon to effect the above modification by

 # service sshd restart (to restart the sshd deamon or service in RHEL - 6)
 # systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
 # chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
 # systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
 # service sshd reload (to reload the sshd deamon in RHEL - 6)
 # systemctl reload sshd (to reload the sshd deamon in RHEL - 7)
(iii) # gedit (to open the gedit editor on remotely)

12. How to allow empty password through ssh?

(i) Open the ssh configuration file by # vim /etc/ssh/sshd_config

-----> go to line no. 65 in RHEL - 6 or

-----> go to line no. 77 in RHEL - 7 PermitEmptyPassword no

type as " yes " in place of " no " then save and exit this file.

* If it is yes, then the remote system will be allow the users with empty password ie., without password.
* If it is no, then the remote system will not be allow the users with empty passwords.

(ii) Then restart the sshd service or deamon to effect the above modifications by

service sshd restart (to restart the sshd deamon or service in RHEL - 6)
systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
service sshd reload (to reload the sshd deamon in RHEL - 6)
systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

(iii) Now, the users who are having empty passwords are also access the remote systems through ssh.

13. How to prevent the password authentication mechanism in ssh?

(i) Open the ssh configuration file by # vim /etc/ssh/sshd_config
-----> go to line no. 66 in RHEL - 6 or
-----> go to line no. 78 in RHEL - 7 PasswordAuthentication no
type as " no " in place of " yes " then save and exit this file.
* If it is yes, then the remote system will ask the password.
* If it is no, then the remote system will not ask any type of passwords.

(ii) Then restart the sshd service or deamon to effect the above modifications by

service sshd restart (to restart the sshd deamon or service in RHEL - 6)
systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
service sshd reload (to reload the sshd deamon in RHEL - 6)
systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

(iii) Now, we can access the remote systems through ssh without Password Authentication mechanism.

14. How to allow or deny the uses or group to access the remote systems through ssh?

(i) If we want to allow or deny the particular users then go to last line of the ssh configuration file and type as

DenyUsers <user 1><user 2><user3> ...etc., (these users will be denied the ssh service)
AllowUsers <student><user 4><user 5> ...etc., (these users will be allowed the ssh service)
DenyGroup <group 1><group 2><group 3> ...etc., (these group users will be denied the ssh service)
AllowGroup <group 1><group 2><group 3> ..etc., (these group users will be allowed the ssh service)

(ii) Then restart the sshd service or deamon to effect the above modifications by

service sshd restart (to restart the sshd deamon or service in RHEL - 6)
systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
service sshd reload (to reload the sshd deamon in RHEL - 6)
systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

15. How allow the specified no. of users to access remote system at a time?

(i) Open the ssh configuration file by
vim /etc/ssh/sshd_config then go to MaxAuthTries line and type as,

MaxAuthTries <no.> (type any numeric value equal to Max. users to allowat a time in place of <no.>, then save and exit this file)

(ii) Then restart the sshd service or deamon to effect the above modifications by

 # service sshd restart (to restart the sshd deamon or service in RHEL - 6)
 # systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
 # chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
 # systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
 # service sshd reload (to reload the sshd deamon in RHEL - 6)
 # systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

16. How to allow or deny the hosts or networks to use the ssh?

To deny IP addresses or hostnames :

(i) Open /etc/hosts.denyfile by # vim /etc/hosts.deny and go to last line and type as,

sshd: <IP address 1><IP address 2><IP address 3> ...etc., (to deny IP 1, IP 2, IP 3, ...etc.,)
sshd: <hostname 1><hostname 2><hostname 3> ...etc.,
*sshd: *.example.com *.my133t.org ...etc., (to deny all the hosts from these domains)*
sshd: 192.168.0. 172.25.0. ...etc., (to deny 192.168.0 and 172.25.0 networks)
sshd: ALL Except <hostname or IP address>
(to deny all the hosts or IP addresses except the specified one in that network)
and save & exit the file.

(ii) Then restart the sshd service or deamon to effect the above modifications by

 # service sshd restart (to restart the sshd deamon or service in RHEL - 6)
 # systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
 # chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
 # systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
 # service sshd reload (to reload the sshd deamon in RHEL - 6)
 # systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

To allow IP addresses or hostnames :

(i) Open /etc/hosts.allow file by # vim /etc/hosts.allow and go to last line and type as,

sshd: <IP address 1><IP address 2><IP address 3> ...etc., (to allow IP 1, IP 2, IP 3, ...etc.,)
sshd: <hostname 1><hostname 2><hostname 3> ...etc.,
*sshd: *.example.com *.my133t.org ...etc., (to allow all the hosts from these domains)*
sshd: 192.168.0. 172.25.0. ...etc., (to allow 192.168.0 and 172.25.0 networks)
sshd: ALL Except <hostname or IP address> (to allow all the hosts or IP addresses except the specified one in that network) and save & exit the file.

(ii) Then restart the sshd service or deamon to effect the above modifications by

 # service sshd restart (to restart the sshd deamon or service in RHEL - 6)
 # systemctl restart sshd (to restart the sshd deamon or service in RHEL - 7)
 # chkconfig sshd on (to enable the sshd deamon at next reboot in RHEL - 6)
 # systemctl enable sshd (to enable the sshd deamon at next reboot in RHEL - 7)
 # service sshd reload (to reload the sshd deamon in RHEL - 6)
 # systemctl reload sshd (to reload the sshd deamon in RHEL - 7)

17. How to check whether the ssh is running or not on remote host?

 # nmap -p 22 <IP address of the remote host>(to see the ssh is running or not on remote system)

18. How to troubleshoot if the client has complain that I am not accessing the server using ssh?

(i) First check the pinging of the client system. If it is not pinging then check the IP address of the client system. If client system and sever system are in different domains or networks it will not ping. So, bring the client system into the network of the server system. Check the network is working or not and also check whether the network cable is connected or not.

(ii) If both systems are pinging then check whether the openssh package is installed or not. If not installed then install that package and configure ssh on the client system and restart the sshd deamon.

(iii) Check the client <IP address or hostname> in /etc/hosts.deny files. If there is an entry of the client system in this file, then remove that entry and restart the sshd deamon.

(iv) Finally open the ssh configuration file by # vim /etc/ssh/sshd_config and see any client user name is present or not and check other lines for client entries in this file, if present remove those entries, save that file and restart the sshd service.

(v) Finally check whether the client user is there in the server or not, if not create the client user, assign the password share those details to client. If user is there then check whether the client user's password is locked, account expired and any other or not, if locked then remove the lock, if client account is expired then activate that account, assign the password and make the ssh trusting between client and server systems.

19. How to copy the file from our system to remote system?

 # scp <source file name with full path><IP address of the remote system>:<destination location>
Example: ssh /root/script1 192.168.1.1:/root/script1 (to copy /root/script1 file into 192.168.1.1 system)
ssh -r /root/raju/ 192.168.1.1:/root/raju/ (to copy /root/raju directory to remote system)
** scp means secured copy to copy the files or directories from local system to remote system.*

20. What is rsync and explain it?

rsync is a very good program for backing up or mirroring a directory tree of files from one machine to another machine and for keeping the two machines " in sync ". It is designed to speedup file transfer by coping the differences between two files rather than coping an entire file every time.
If rsync is combined with ssh, it makes a great utility to sync the data securely otherwise by sniffing any one can see our data ie., no security for our data.

21. A system is able to ping locally but not out site. Why?

(i) May be there is no access to outside.
(ii) May be outside is in different network from the local.
(iii) May be permission is denied for that system to access outside.
(iv) If there is access, but router or modem or network switch or NIC may not be working to access the outside.
(v) May be outside is not available temporarily.

22. A system is echoing the ping, but not able to login via telnet. Why?

(i) Check telnet service is started or not. If not started, start the telnet service.

(ii) May be telnet service is disabled, if so, enable the telnet service.
(iii) May be telnet port is blocked, if so, release that port no.
(iv) May be telnet permission is denied, if so, change the permissions to allow the telnet service.
(v) Check all the files whether the telnet service is blocked or not, if blocked remove those entries.

23. How will you login or start the system in what mode if you don't know the root password?

(i) If the user having sudo permissions, then login as sudo user.
(ii) If no sudo permissions then boot with CDROM in single user mode and start the system.
Then provide the root password to root user if there is no root password.
(iii) Even though if it is not possible then finally break the root password.

Other useful commands :

 # telnet <IP address or hostname> (to connect the specified remote system through telnet)
 # ssh <IP address or hostname> (to connect the specified remote system through ssh)
Username : xxxxxx
Password : xxxxxxx
 # ssh <IP address> -l <user name> (to connect the remote system using user name)
Password : xxxxxxx
 # ssh 192.168.1.1 -l root (to connect this remote system as root user)
 # ssh root@192.168.1.1 (to connect this remote system as root user)
 # ssh root@server1.example.com (to connect the server1 system in example.com domain)
 # w (to see all the users who are login to our system)
 # w -f (to see all the users who are login to our system with other details)
 # ssh <IP address> (if we not specified the user name, then it will ask the current users password and search the current account in remote system)
 # cat /root/.ssh/known_hosts (to see the ssh trusting remote hosts finger print information)
 # ssh root@192.168.1.1 <command>
(to run a command on remote host without login to that system)
 # ssh root@192.168.1.1 -X (to run GUI commands on the remote system because by default the ssh is configured as command line interface, X is capital)
 # lastb (to see the login failed tries)
 # last -x |grep shutdown (to see the date & time of the system's last shutdown)

Chapter#9 – Memory and Swap Management

1. What is swap?

Swap space in Linux is used when the amount of the Physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in the memory are moved from RAM to swap space. It helps the machines which are having small amount RAM and it should not be considered a replacement for more RAM. Swap is located on the hard disks which have slower access time than Physical memory.

2. What is the recommended swap space?

Generally the recommended swap space is double the RAM size, but the following table shows actual amount.

Apart from the below recommendation a basic rule is applied to create the swap partition.

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

** If the RAM size is more than 2 GB, then the size of the swap = 2 GB + RAM size.*

Amount of RAM in the System	Recommended Amount of Swap Space
4 GB or less	Min. 2 GB
4 GB - 16 GB	Min. 4 GB
16 GB - 64 GB	Min. 8 GB
64 GB - 256 GB	Min. 16 GB
256 GB - 512 GB	Min. 32 GB

3. Is it necessary to create the swap at the time of installation?

Yes, swap space is compulsory to be created at the time of installation. But additional swap space can be created and deleted at any point of time, when it is required. Sometimes we need to increase the swap space, so we create additional swap space which will be added to the existing swap space to increase the size.

4. What is swap-in and swap-out or page-in and page-out?

swap-in *or* ***page-out*** ***:***

If we run or open any application, it requires some amount of memory to load its features. So, first it looks or occupy physical memory (RAM). If there is not enough space in RAM, the application's data is transferred from RAM to swap space. If the pages are moving from RAM to swap space, that is called swap-in or page-out.

swap-out *or* ***page-in*** ***:***

If older or previous application is closed, then the space occupied by those applications also cleared. ie., some of the space is available in RAM. So, automatically some data which is already occupied in swap space is also moved from swap to RAM. If the pages are moving from swap space to RAM, that is called swap-out or page-in.

5. How paging space is allocated?

(i) Paging means data transferred from RAM to swap space.

ii) If we open or run any application, first it will occupy the required space in RAM. If there is not

enough space in RAM, then some amount of application's data will be transferred from RAM to swap space. ie., swap space is allocated to that application. This allocation is called paging space or page-out allocation.
(iii) paging will takes place in swap by blocks. First it will create the required no. of blocks in swap space.
(iv) If RAM space cleared by older or other applications, then swap occupied data is transferred from swap to RAM. This is called page-in. So, that much amount of space is unallocated in swap ie., removed the created blocks in swap.

6. How to create the swap partition?

 # fdisk -l (to see the available disks in the system)
 # fdisk /dev/sdb
Command (m for help) : n (to create a new partition)
First cylinder : (press Enter key)
Last cylinder : +2048M
Command (m or help) : t (to change the hex code)
Partition no. (1-2) : 2 (to change the partition number hex code)
Hex code : 82 (82 is the hex code for Linux swap)
Command (m for help) : w (write the changes to the disk)
 # partprobe or # partprobe /dev/sdb (to update the partition table information)
 # mkswap /dev/sdb2 (to convert the raw disk to swap file system)
 # swapon /dev/sdb2 (to turn on the swap partition)
 # vim /etc/fstab (to make the permanent mount of swap partition)
/dev/sdb2 swap swap defaults 0 0 (save and exit this file)
 # mount -a (to mount all the partitions which are having entries in /etc/fstab file)
 # df -hT (will not show the swap size)
 # free -m (to see the total RAM and swap size)

7. How to remove the swap partition?

 # swapon -s (to see the swap partition names or disks)
 # swapoff /dev/sdb2 (to turn off the swap space)
 # vim /etc/fstab (open this file and remove the swap partition entry)
(after removing the swap partition save and exit this file)
 # fdisk /dev/sdb (to delete the swap partition)
Command (m for help) : d (d for to delete the partition)
Partition no. (1-2) : 2
Command (m for help) : w (to write the changes into the disk)
 # partprobe or # partprobe /dev/sdb
 # free -m (to see the RAM as well as swap sizes)

8. In how many ways can we create the swap spaces?

(i) By creating a new swap partition on the disk. (separate swap partition)
(ii) By creating swap file.

9. How to create the swap space using the swap file?

Sometimes it is unable to create a swap partition because may be there is no disk space or may be the partition limit is already exceeded. So, in these scenarios we have to create only the space file.

 # dd if = /dev/zero of = /root/linuxswap bs = 1M count = 2048 (to create 2048MB empty file)
 # du - /root/linuxswap (to see the linuxswap size)
 # mkswap /root/linuxswap (to convert the existing file system to swap file system)
 # swapon /root/linuxswap (to turn on the swap file)
 # vim /etc/fstab (to make a permanent mount of swap space)
/root/linuxswap swap swap defaults 0 0
(save and exit this file)
 # mount -a (to mount all the partitions which are having entries in /etc/fstab file)
 # df -hT (will not show the swap size)
 # free -m (to see the total RAM and swap size)

10. What is virtual memory?

The combination of Physical memory (RAM) and swap space is called the virtual memory.
So, Virtual memory = Physical memory (RAM) + swap space.

Other useful commands :

 # swap -s (to see how many swap partitions are there and with their names)
 # swapon -a (to turn on all the swap partitions)
 # swapoff -a (to turn off all the swap partitions)
 # cat /etc/mtab (to see the current and temporary mount points)
 # mountpoint <directory or mount point> (to check the specified directory is a normal directory or a mount point)
 # df -ih (to check how many inode numbers are available in the mounted partitions)

11. What happens when the /usr is full?

(i) Users cannot login to the system.
(ii) If already login users not able to execute any command.

12. What happens when memory ie., pagein space is full?

(i) The new applications cannot load due to lack of memory.
(ii) So, users cannot login to the application and cannot access the applications features.
(iii) So, if we increase the swap memory to the required size then the problem will be solved.

13. How to restore the data and upgrade your O/S ?

(i) We can restore the data from backup by, tar, cpio, dd, net backup or other tools.
(ii) If it is in mirror, we can sync the data from mirrored disk.
(iii) We can upgrade the O/S in two ways.

a) Online :

The O/S is upgraded from previous to present while the system is running.It is risky and takes long time.

(b) Offline :

First take backup of all the system and then remove previous O/S and install the present O/S and restore the backup from backup disks or tapes. So, it is very easy and non-risky job.

Chapter#10 – Software Management

1. What is software?

Software is a collection of programs to perform some tasks or manage systems, applications, databases

2. What is package and package management?

Package is nothing but a software to perform some tasks. Software is the basic of any O/S allowing to install and use different utilities.

Package management means installing, updating, querying, repairing and removing packages. In Linux there are two tools to perform package management.

rpm -----> redhat package manager and yum -----> yellowdog updater modifier.

3. What is rpm?

rpm is a package managing system (collection of tools to manage software packages). rpm is a powerful and most popular open source tool used for software management for installing, uninstalling (removing), verifying, querying and updating software packages. It is installed under /var/lib/rpm database directory. It deals with .rpm files, which contains the actual information about the packages. The rpm log messages will be stored in /var/log/yum.log file.

4. What are the draw backs of rpm?

(i) rpm cannot resolve the dependency. It means, if we want to install any software, first the dependency packages should be installed.

(ii) There is no configuration file for rpm.

5. What are the basic modes of rpm commands?

(i) Install -----> used to install rpm packages.

(ii) Update -----> used to updated the packages.

(iii) Troubleshooting -----> used to repair the packages.

(iv) Remove -----> used to remove or uninstall the packages.

(v) Querying -----> used to query (gather information) on packages.

6. How many types of packages are available in Linux?

(i) x86_64.rpm -----> 64 bit package and can be install on 64 bit O/S only.

(ii) x86.rpm -----> 32 bit package and can be install on 32 bit or 64 bit O/S only.

(iii) i 386.rpm -----> 32 bit package and can be install on 32 bit or 64 bit O/S only.

(iv) i 486.rpm -----> " "

(v) i 586.rpm -----> " "

(vi) i 686.rpm -----> 64 bit package and can be install on 64 bit O/S only.

(vii) noarch.rpm -----> no-architecture and can be install on either 32 bit or 64 bit O/S.

7. What is the syntax of rpm command with full options?

 # rpm <options><package name>

The options are, -i -----> install

-v -----> verbose
-h -----> progress in hash codes (in %)
-qi -----> query information about the package
-ql -----> list all package related files.
-qd ----> query about the document of the package
-qc -----> displays the configuration files for that package
-qa -----> query on all installed packages
-V -----> (capital V) to verify the package for repair that package
-R -----> list all dependent packages
--force -----> install the package forcefully
--nodeps -----> install the package without dependency (do not check the dependencies)
--last -----> all installed packages with date and time

Other useful rpm commands :

 # rpm -ivh <package name> (to install the package)
 # rpm -qa (to list all installed packages)
 # rpm -qa <package name> (to check whether the package is installed or not)
 # rpm -qa |wc -l (to count how many packages already installed)
 # rpm -qa --last | less (to check last installed packages)
 # rpmquery -qa (to list all the installed packages)
 # rpm -qa |grep -i <package name> (to check the specified package is installed or not)
 # rpm -ivh --test <package name> (to check the package consistency)
** If the installation status shows 100%, then the package is in good condition or consistent. But while showing the hash progress if it shows any error, then the package is in inconsistent state.*
 # rpm -ivh finger (to install the finger package)*
 # rpm -qa finger (to check whether the package is installed or not)
 # finger <user name> (to check whether the installed package is working or not)
 # rpm -e <package name> (to erase or remove or uninstall the package)
 # rpm -evv <package name> (to remove the package in verbose mode)
 # rpm --test -ivh (to test the package before installing ie., whether the package is suitable or not)
 # rpm -qi <package name> (to see the details or information on the installed package)
 # rpm -ql <package name> (to list all package related files)
 # rpm -qlc <package name> (to list all the configuration files of that package)
 # rpm -qd <package name> (to list all the document files of that package)
 # rpm -ivh <package name> --force (to install the package forcefully)
 # rpm -qR <package name> (to list the dependencies of that package)
 # rpm -qip <package full name> (to display the package information before installation)
 # which <command name> (to display the location of that command)
 # rpm -qf <location of the command> (to check the package name for that command)
 # rpm -V <package name> (to verify that package, ie., 100% package is there or not, if any files missed in that package, those are displayed as a list)
 # rpm -ivh <package name> --replacepkgs (to replace the missed files in that package)
 # rpm -qp --changelog <package name> (displays all the changed logs like lat time,

when the package is installed, ...etc.,)

 # rpm -qp --scripts <package name> (to see the package installation scripts)

 # rpm -K <package full name> (to see the package key)

 # rpm -Uvh <package name> (to update the package)

** Update is over write the old version of the package. If any problems in new package, we cannot solve those issues. So, the better one is install that package as a fresh one (not update option).*

** Update will look first the package is available in that system or not. If it is available, it will update that package otherwise it will install as fresh package.*

 # rpm -qRp <package name> (to check the dependency packages of that package before install)

 # rpm -ivh <package name> --nodeps (to install the package without dependent packages)

8. What is yum and explain the yum?

yum stands for yellow dog updater modified. yum is a package management application for computers running on Linux O/S.yum is a standard method of managing the installation and removal of software. It is from RHEL - 5 onwards. Packages are downloaded from collections called repositories, which may be online, on a network and or on installation media. yum is a front end tool for rpm. It is used to resolve the dependency which cannot be done by rpm. The yum command has access the repository where the packages are available and can install, update/upgrade, remove and query the packages automatically.

9. What are the important files that are related to yum?

/etc/yum.conf -----> is the yum configuration file.

/etc/yum.repos.d -----> is the directory which contains the yum repository configuration file.

/etc/yum.repos.d/xxxxx.repo ------> is the yum repository configuration file.

/var/lib/yum -----> is the directory which contains the yum databases.

/var/log/yum.log -----> is the file which stores the yum log messages.

10. How setup the yum server?

*(i) Insert the RHEL DVD, goto that directory and install the vsftpd package by # rpm -ivh vsftpd**

(ii) Goto /var/ftp/pub directory and create rhel6 directory by # mkdir rhel6

(iii) Goto DVD mounted directory and copy all the DVD content into /var/ftp/pub/rhel directory by # cp -rvpf /media/DVD/ /var/ftp/pub/rhel6

(iv) Restart the vsftpd service by # service vsftpd restart command.

(v) Then enable the vsftpd service by # chkconfig vsftpd on command.

(vi) Goto /etc/yum.repos.d directory and create one yum repository file by # vim linux.repo command.

(vii) In the above file the contents are as below,

[linux] (Linux repo id)

name=yum repo server (yum server name)

baseurl=file:///var/ftp/pub/rhel6 or baseurl=ftp://<IP address of the system>/pub/rhel6

gpgcheck=0 (0 means while installing it will not ask any signature keys of yum packages, If it is 1, then it will ask the signature keys while installing the packages)

enabled=1 (if multiple repositories are there, then enable this only)

(save and exit this file)

(viii) # yum clean all (to clean the old one update the new repository)

(ix) # yum repolist (it displays no. of packages in that repository)

11. How to setup the yum client?

(i) Goto /etc/yum.repos.d directory and create the repository file by # vim linux.repo
(ii) Type the entries as below,
[linux] (Linux repo id)
name=yum repo client (yum repo client)
baseurl=ftp or http://<IP address of the server>/pub/rhel6
gpgcheck=0 (0 means while installing it will not ask any signature keys of yum packages, If it is 1, then it will ask the signature keys while installing the packages)
enabled=1 (if multiple repositories are there, then enable this only) (save and exit)
(iii) # yum clean all (to clean the old one update the new repository)
(iv) # yum repolist (it displays no. of packages in that repository)

12. How to configure the yum repository to deny some packages to be installed?

(i) To configure the yum tool the yum configuration file is /etc/yum.conf
(ii) To deny some packages, open the yum configuration file by # vim /etc/yum.conf command.
(iii) Gotolast line and type as, exclude=(all) kernel* ftp* then save and exit this file.*
(iv) Then kernel and ftp* packages will be denied when we trying to install those packages.*

13. How to change the yum repository default location?

(i) Open yum configuration file by # vim /etc/yum.conf command.
(ii) Goto last line and type as, repository=<yum repository new location with full path> then save and exit this file.
(iii) Then the yum repository new location will be changed from old one new one.

14. How to change the yum log file default location?

(i) Open the yum configuration file by # vim /etc/yum.conf command.
(ii) Goto last line and type as, log=<yum log file new location with full path> then save and exit this file.
(iii) Then the default log location is changed from /var/log/yum.log file to new location.

15. How to configure the yum to restrict the architecture (64 bit or 32 bit) etc.,?

(i) Open the yum configuration file by # vim /etc/yum.conf command.
(ii) Goto last line and type as, exactarch=1 then save and exit this file.
(iii) 1 means first it installs 64 bit packages and if it is 0 then 32 bit packages will be installed.
(iv) Open the yum configuration file by # vim /etc/yum.conf command.
(v) Goto last line and type as, cachedir=<download new location> then save and exit this file.
(vi) Then whenever we install the packages the downloaded location will be the new location.
(vii) Open the yum configuration file by # vim /etc/yum.conf command.
(viii) Goto last line and type as, assumeyes=1 then save and exit this file.
(ix) Whenever we install any package using yum then no need to mention -y option if assumeyes=1 and if assumeyes=0 then we have to mention -y option when we install the package.

16. What is O/S patch and how to add those patches on production servers or how to upgrade the *kernel*?

(i) O/S patch is nothing but update the new kernel. Normally O/S patch is software that contains some programs to fix the bugs in O/S ie., in kernel.

(ii) If our server is registered and configured in RedHat network, then we will get the information about that updated kernel s information and then download that kernel updations.
(iii) Every O/S patch is supplied with a document about pre-requisites to apply that patch.
(iv) Check the pre-requisites, space requirements and others. if all are ok,
(v) Then we take the business approval and make CRQ's (Change requests).
(vi) Then the project manager will initiate the mail thread ie., sending the mail or messages to various teams who are dealing with that server.
(vii) We get the response from different teams which are involving in this process.
(a) For example Monitoring team to ignore alerts from that server if the system hangs or rebooted.
(b) DBA team if database stopped or crashed or system failed.
(c) Application team if the application effects while patching.
(viii) If the server is in cluster, then move the service group and resources to another systems manually called switch over.
(ix) Inform the Application team to stop the application and database team to stop the database.
(x) If the server is in cluster there is no need of reboot (no down time) else down time needed to reboot.
(xii) If mirror disk is there, split the mirror disk from original disk and boot in single user mode and add the patch by # rpm -ivh <patch name> command.
(xiii) Then reboot the system and won't attach the mirror disk to avoid any unexpected situations or problems and put that server under test upto 1week or 10 days depending on the company's policy.
(xiv) After the test period, if there is no problems raised then attach the system in live mode and also with mirror disk to sync the data to update the system.
(xv) Then we inform the Application, Database, Monitoring and other teams who are dealing with that server to test application, database, monitoring and others see the status.
(xvi) Then finally close the issue or CRQ.

17. After installation of package or patch if the package or patch is removed then what will happened?

(i) If kernel patch is removed, then the system will hang and for others there is no effect.
(ii) If package is removed then the application that belongs to that removed package will effect.

18. After applying the patch need to reboot the system or not?

(i) If the patch is kernel patch or clustered patch then only the system reboot is required.
(ii) If the patch is normal patch then there is no need of the reboot required.

19. If the package is not installing. How to troubleshoot?

(i) Check the package pre-requisites to install the package.
(ii) If pre-requisites are not matched with our system, then the package will not be installed i.e., O/S compatibility to install that package.
(iii) If there is no sufficient space in the system, the package will not be installed.
(iv) If the package is not properly downloaded, then the package will not be installed.

20. If the patch is not applied successfully what will you do?

(i) Check whether the patch is installed properly or not by # rpm -qa <patch name> command.
(ii) Check the /var/log/yum.log file to verify or see why the patch is not successfully installed..
If any possible to resolved those issues, resolve and remove that patch with

 # rpm -e <patch name> command.
(iv) If any reboots required to effect, then reboot the system.
(v) Again add that patch by # rpm -ivh <patch name> command.
(vi) Then check the patch by # rpm -qa <patch name> command

Other useful yum commands :

 # yum repoinfo (to list all the information on all the repositories)
 # yum repoinfo <repo id> (to list all the information on specified repository)
 # yum install <package name> -y (to download and install the package and y means yes)
 # yum install <package name> -d (to download the package)
 # yum erase or remove <package name> -y(to remove or uninstall the package and y means yes)
 # yum list installed (to display the list of all installed packages)
 # yum list available (to list all the available packages to be installed)
 # yum list all | less (to list all the installed and not installed packages)
 # yum search <package name> (to search a particular package is available or not)
 # yum info <package name> (to display the information on that package)
 # yum update <package name> (if the update version of the specified package is available, then update that package)
 # yum update all (to update all the packages nothing but whole system will be updated)
 # yum downgrade <package name>
(to revert back ie., go back to previous version of that package if new version is not working properly)
 # yum history (to display the yum history)
 # yum history info < id > (to display the information of that history id)
 # yum history undo < id > (to remove that history id)
 # yum history undo < id > (to redo the above removed history id)
 # yum grouplist (to display the list of group packages)
 # yum groupinstall <package name> (to install the group package)
 # yum install@<group package name> (to install the group package in another way)
 # yum groupinfo <group package name> (to display the group package information)
 # yum grouplist hidden (to list all the group packages names including installed or not installed and hidden group packages)
 # yum-config-manager disablerepo=<repo id>
(to disable the yum repository. So, we cannot install any package from the repository)
 # yum clean all (to clear the history, if we disable the repository id, then we have to clean the history, then only it will disable the repository)
 # yumdownloader <package name> (to download the package from the repository, and the downloaded location is the present working directory)
 # man yum.conf (to see the manual pages on yum configuration file)
 # yum-config-manager --add-repo=http://content.example.com/rhel7.0/x86_64/dvd (then the yum repository will be created automatically with .repo file also. And this works only in RHEL - 7)
 # subscription-manager register --username=<user name> --password=<password>
(to register our product with RHN--Redhat Network. The user name and passwords will be provided by the Redhat when we purchase the software)
 # subscription-manager unregister --username=<user name> --password=<password> (to unregister our product with RHN--Redhat Network. The user name and passwords will be provided by the Redhat when we purchase the software)

Chapter#11 – Backup and Restore

1. What is backup and what is purpose of the backup?

Copying files from local disk to any removable media is called backup.
In information technology, a backup or the process of backing up is making copies of data which may be used to restore the original after an event of data loss. Backup has two distinct purposes.
The primary purpose is to recover data after its loss due to deletion or corruption. Data loss is very common in IT industry. The second purpose of backup is to recover data from an earlier time.
Backup is the most important job of a system administrator, as a system admin it is our duty to take backup of the data every day. Most companies have gone out of the market because of poor backup planning or policy.

2. What is recovery or restore?

Copying files from any removable media to local disk is called recovery or restore. Backup will be helped in hardware failure or software failure or system crashed.

3. What are the backup tools available in the IT industry?

Platform	***Backup Tools***
Windows	*ntbackup*
Linux	*tar, cpio, dd, dump, restore*
3rd party	*Veritas netbackup, Amanda and Tivoli*

4. What is tar and Explain it or how to take a backup using tar?

Archiving means collection of files and directories and to make a single file nothing but compression. tar means tape archiving. It is an archive file. By using tar command we can take a backup of files and directories. It cannot support file systems backup and also not support for large files more than 80GB. tar will not skip any single file including bad blocks also.

Full syntax of tar :

 # tar <options><destination file name with path><source file or directory with path>

The options are, -c -----> create
-v -----> verbose
-f -----> file name
-t -----> listing
-tv ----> long listing
-x -----> extract
-w ---->interactive
-C -----> specific location (Capital C)
-u -----> update means adding new contents to the existing tar file
--update -----> " "
--delete -----> deletes the contents from the tar file
-p ----> preserve the old permissions of the files/directories when extracting the tar file
-z ----> gzip (gun zip) compression
-j ----> bzip2 (bun zip) compression
-J ----> xz compression (from RHEL - 7)

Examples:

 # tar -cvf /root/etc.tar /etc/ (to copy all the files and directories from /etc and make a single file and place in the /root/etc.tar file)*
 # tar -tvf /root/etc/tar (to long listing the contents of the /root/etc.tar file)
 # tar -xvf /root/etc.tar -C /root1/ (to extract and copy the files in /root1/ location)
 # tar -xf /root/etc.tar (to list the contents of the tar file)
 # tar -f /root/etc.tar --update or -u <file name or directory> (to add the new contents to the existing tar file)
 # tar -f /root/etc.tar --delete<file name or directory> (to delete the file from the tar)
 # tar -u /root/etc.tar /var (to add the /var contents into the /root/etc.tar file)
 # tar -cvf mytar.tar / --xattrs (to archive the contents along with SELinux and ACL permissions)
 # du -h /root/etc.tar (to see the size of the tar compressed file)

5. What are the compressing & uncompressing tools available for tar and explain them?

Compressing Tools	***Uncompressing Tools***
# gzip (.gz)	*# gunzip*
# bzip2 (.bz2)	*# bunzip2*
# xz (RHEL - 7)	*# unxz*

 # gzip <tar file name> (to compress the size of the tar file and the output file is .tar.gz)
 # gunzip < .gz compressed file name>(to uncompress the compressed tar file and the output is .tar only)
 # bzip2 <tar file name> (to compress the size of the tar file and the output is .tar.bz2)
 # bunzip2 < .bz2 compressed file name>(to uncompress the compressed file and the output is .tar only)

6. What is scp, rsyncand how to use it?

scp means secure copy. ie., ssh + cp = scp which is used to copy the files/directories into remote system. scp will copy files/directories into remote system blindly ie., if the file already exits, it will over write that file.So, scp will take more time to copy when compared to # rsync tool.
 # scp <file name><user name>@ <IP address of the remote system>:<location to be copied>
 # scp anaconda root@192.168.1.1:/root (to copy anaconda file into /root of the remote system)*
 # scp -r /etc/ root@192.168.1.1:/raju (to copy /etc/ directory into /raju of remote system)
#scp -av /raju root@192.168.1.1:/root (to copy /raju into /root of the remote system)
 # scp -r root@192.168.1.1 :/etc /home (to copy /etc of the remote into /home of the local system)
rsync is also used to copy files/directories into remote systems. rsync tool will compare the new files or directories and copy only the changed or modified contents of the files into remote system. So, it takes less time to copy when compared to # scp tool.
 # rsync -av root@192.168.1.1:/etc /home (to copy /etc directory changed contents into /home)
rsync options are, -a -----> all (copy the file with all permissions except SELinux and ACL permissions) -aA -----> synchronize ACL permissions
-aAx ----> synchronize ACL and SELinux permissions also.

7. What is cpio and how to take a backup and restore using cpio?

cpio means copy input and output. It supports any size of the file system. It skips the bad blocks also.

Syntax of cpio with full options :

 # ls <source file name> |cpio <options>><destination file name> (to take a backup of the source directory and stored the backup into destination directory)

The options are, *-t -----> to list the cpio contents*
-i -----> to restore the cpio backup
-v -----> to display on the screen ie., verbose
-o -----> to take a backup

Examples :
 # ls | cpio -ov > /opt/root.cpio (to take a backup of root directory and stored in /opt)
 # cpio -iv < /opt/root.cpio (to restore the backup)
 # ls /etc | cpio -ov > /opt/etc.cpio (to take a backup of the /etc directory and stored in /opt)
 # cd /etc (go to that /etc directory)
*# rm -rf * (to remove all the contents from /etc)*
 # cpio -iv < /opt/etc.cpio (to restore the /etc contents from the cpio backup)

8. What is dd and how to take a backup and restore using dd?

dd means disk to disk backup. Using dd command we can take a backup of the data from one disk to another disk. It copies the data in byte to byte. It can take a backup of the disk including bad blocks. # dd if = <disk 1> of = <disk 2> (to take a backup from disk 1 and stores in disk 2)
 # dd if = /dev/zero of = /root/raju bs = 1M count = 2048 (to create an empty file with 2GB size)
 # dd if = /dev/sda of = /root/mbr.bak bs = 1 count = 512 (to take the backup of /dev/sda Master Boot Record)
 # dd if = /root/mbr.bak of = /dev/sdb(to restore the MBR from backup to second disk /dev/sdb)
 # dd if = /dev/sda1 of = /dev/sdb1 (to take a backup of the entire /dev/sda1 disk partition)
 # dd if = /dev/sdb1 of = /dev/sda1 (to restore the /dev/sda1 contents from the above backup)
 # dd if = /dev/sda of = /dev/sdb (to take a backup of the entire /dev/sda disk into /dev/sdb)
 # dd if = /dev/cdrom of = /root/rhel6.iso (to create a ISO image file of the CD/DVD)

9. What is dump and how to take a backup and restore using dump and restore?

dump is a command used to take a backup of file systems only. We cannot take a backup of files and directories. We cannot take a backup of disk to disk backup. It is not recommended to take a backup on mounted file systems. So, unmount the file system and then take a backup is recommended. By default dump is not available in the system. so, first install the dump package and then execute the dump
 # yum install dump -y (to install the dump package)*

The syntax for dump :

 # dump <options><destination file name><source file name>(to take a backup of the file systems)
The options are, -0----->full backup
-(1 - 9) -----> incremental backups
-u -----> update the /etc/dumpdates file after successful dump
-v -----> verbose
-f ----->make the backup in a file
-e -----> exclude inode number while backing up

 # dump -0uvf /opt/full.dump /coss (to take a full backup of the /coss file system and copied it in /opt)
 # dump -1uvf /opt/full.dump /coss
(to take a backup modified files from the last full backup nothing but incremental backup)
 # dump -2uvf /opt/full.dump /coss
(to take a backup modified files from the last incremental level -1 backup)

The syntax for restore :

 # restore <options><dump backup file> (to restore the backup contents if that data is lost)

The options are,
-f -----> used to specify the dump or backup file
-C -----> used to compare the dump file with original file
-v -----> verbose
-e -----> exclude the inode number
-i -----> restore in interactive mode

The commands in interactive mode are,

restore> ls -----> list the files and directories in the backup file
restore> add ----> add the files from dump file to current working directory
restore> cd -----> change the directory
restore> pwd ---> displays the present working directory
restore> extract ----> extract the files from the dump file
restore> quit ---> to quit from the interactive mode

 # restore -tf /opt/full.dump (to list the dump file contents)
 # restore -rf /opt/full.dump (to restore the dump file contents)

10. How many types of backup available?

There are mainly three types of backups available.
(i) Full backup (Entire file system backup)
(ii) Incremental backup (backup from the last full backup or incremental backup)
(iii) Cumulative or differential backup (backup from last full backup or cumulative backup)

11. What is the difference between incremental and differential backup?

Incremental backup :
Taking a backup from the last full backup or last incremental backup

Differential backup :
Taking a backup from last full backup or last cumulative or differential backup

12. Which file will update when backing up with dump command?

/etc/dumpdates *file will be updated when backing up with dump command.*

13. What are the dump devices?

(i) Tape drives
(ii) Disks (local disks)
(iii) Luns (network disks)

14. What is snap shot?

(i) The point - in - time copy of the file system is called the snap shot.
(ii) It provides online backup solution of the file system.
(iii) We can take a backup while the file system is mounted and it is in multi-user mode.
(iv) It occupied only as much disk space as the file system ie., being captured.
(v)We can also create backup, delete, query temporary (read-only)snap shots using fssnap command.

15. What are the differences between tar and cpio commands?

(i) By tar we can take backup upto 80GB size of file systems , but using cpio there is no limit.
(ii) In tar the backup is in archive format ie., in compressed state, but in cpio there is no compression.
(iii) In both the types only the whole backup is possible.

16. How to take a backup on production servers?

(i) Normally in backup environment we have 3 servers.
(a) Master server (production servers -- 1 or 2 no's).
(b) Media server (backup server -- 1 or 2 no's).
(c) Client server (Normal system)
(ii) Backups can be taken in types.
(a) Application Backup (Normally application users will take these types of backups)
(b) File system Backup (O/S backup, System Administrators will take these types of backups)
(c) Database Backup (DBA users will take these types of backups)
(iii) Normally backup is automated through some backup tools like Veritas Net backup, IBM Tivoli and Autosys.
(iv) Using cron tool also we can take backup. But cron will not inform the failed backup. The other tools will inform by sending messages like why the backup is failed, when and where it is failed, ..etc.,
(v) On production servers the backup will follow the procedure,
(a) Master server deport from production.
(b) Import the master server on Media server.
(c) Then Master server will join with the Media server.
(d) Sync the data with the Master server.
(e) Take a backup from Master server and store the copy on Media server.
(f) Split the Master server from Media server.
(g) Deport the Master server from Media server.
(h) Import the Master server on production.
(i) Join the Master server with production.

17. What is your company's backup policy?

(i) By dump command we can take backups on disks, tapes and takes full, incremental and differential or cumulative backups.
(ii) level 0 -- Full backup (monthly once)
level 3 -- Performed on every Monday (Incremental from last full or last incremental backup)
level 4 -- Performed on every Tuesday (Incremental from last level 3 backup)
level 5 -- Performed on every Wednesday (Incremental from last level 4 backup)
level 6 -- Performed on every Thursday (Incremental from last level 5 backup)
level 7 -- Performed on every Friday (Incremental from last level 6 backup)
level 8 -- Performed on every Saturday (Incremental from last level 7 backup)
level 2 -- Performed on every Sunday (differential or cumulative backup from last full backup, ie., from Monday to Saturday)

18. What is the information is stored in /etc/dumpdates file?

/etc/dumpdates file records the backup information if -u option is used with dump command to take a backup. In this file each line tells the file system that was backed up, last level of backup, the date, day and time of the backup.

Chapter#12 – Managing Installed Services

1. What is service or deamon?

Service or deamon is program that stats at background and continuously run in the background. The service or deamon is ready for input or monitor the changes in our computer and respond to them. For example the Apache server has a deamon called httpd that listens on port no. 80 on our computer and when it receives a request for a page it sends the appropriate data back to the client machine.
Example : apache, samba, NFS, FTP, ...etc.,

2. What are the commands used to control the services?

service :

This controls the starting and stopping the services during session and these settings will not be saved. We can start the Apache service in this way, but it will not start on booting time. Using this method the service will continue to run on upto next boot but from next boot the service will not be started automatically.

chkconfig :

This controls which services are set to start at boot time. These settings will be saved and applied at next boot. Changing these settings will not start the service immediately and it will just flag them to be started from the next boot.

3. What are the differences between RHEL -6 and RHEL-7 services?

RHEL -6	***RHEL -7***
*(a) The parent process ie., the starting process is **initd** and it's process id (pid) is 1.*	*(a) The parent process ie., the starting process is **systemd** and it's process id (pid) is 1.*
*(b) There two commands for starting the services . They are called **# service** and **# chkconfig***	*(b) Here only one command is used to start the service. That is **# systemctl***
*(c) **# service** command is used to start or stop the services temporarily and **# chkconfig** is used to start or stop the services at next booting time.*	*(c) **# systemctl** is the command to start or stop the services temporarily or next booting time.*
*(d) **/etc/init.d** is the location for all the services.*	*(d) **/usr/lib/systemd/system** is the location for all the services.*
(e) # service <service name> <start/stop/restart/reload/status >	*(e) # systemctl <start/stop/restart/reload/ status ><service name>*

4. What are the differences between initd and systemd deamons?

Initd	***systemd***
(a) It is the starting process in RHEL - 4, 5 and 6.	*(a) It is starting process in RHEL - 7.*
(b) It's process id (pid) is 1.	*(b) It's process id (pid) is 1.*

(c) It will take more time to the system and services.	*(c) It will take less time to start the system and services when compared to RHEL - 6.*
(d) It will start the services one by one.	*(d) It will start the services parallel not one by one.*
(e) All the linux services are ends with letter d. Example : sshd, httpd, crond, ...etc.,	*(e) All the linux services are ends with letter d.service Example : sshd.service, httpd.service, ...etc.,*

5. How to make the computer to boot fasterly?

Many services are required to run all the time however many can be turned off for both security reasons as running unnecessary services opens more doors into our computer but also for performance reasons. It may take much difference but our computer should boot slightly faster with less services it has to start on boot. So, one of the technique to start the system fast and maintain to improve security is turn off the unneeded services.

6. What are masking and unmasking the services?

Masking the services means hiding the services and unmasking the services means unhiding the services. The masking and unmasking are the new commands in RHEL - 7. If any two similar services (for example ntp and chrony) are there in a system, we cannot start the two services at a time. In these scenarios we go for mask and unmask commands.

 # systemctl mask sshd
(to hide the sshd service temporarily ie., we cannot start the services when we mask any service)
 # systemctl unmask sshd (to unhide the sshd service ie., we can start the service again)
** we can also use RHEL - 6 commands like as,*
 # service and # chkconfig , but these two commands will internally call the # systemctl commands only. So, in RHEL - 7 # systemctl command is the recommended one.
 # systemctl --failed --type=service (to check all the failed services)
 # systemctl --failed --type=process (to check all the failed processes)
** In RHEL - 6 service names ends with 'd' only, but in RHEL - 7 the service names ends with d.service and these are all text files only. So, in RHEL - 7 we can open and see all the system services and read their contents.*
 # ps (to see the active process in the system)
 # top (It will show a dynamic real-time view of a running system. ie., a summary of processes or threads currently managed by the Linux kernel)
 # kill (It sends the specified signal to the specified process or process group)
 # pkill (It will send the specified signal to each process instead of listing them on standard output)
 # pstree
(to show all the running processes as a tree structure. The tree is rooted either pid or init)
 # nice (to run a program with modified scheduling priority ie., it runs the process with an adjustable niceness)
 # renice (to alter the scheduling priority of one or more running processes)
 # pgrep (to list the process id's which matches with the pgrep argument)

RHEL - 6 commands :

 # service <service name> status (to check the status of the service)
 # service <service name> start (to start the service)
 # service <service name> stop (to stop the service)
 # service <service name> reload (to reload the service)
 # service <service name> restart (to restart the service)

** These above commands will change the service statuses temporarily. So if we want to change statuses of the process automatically from next boot onwards we have to enable those services as given below.*
 # chkconfig --list (to check the availability of the services in different run levels)
 # chkconfig --list <service name> (to check the availability of the service in different run levels)
 # chkconfig <service name> on (to make the service available after restart)
 # chkconfig <service name> off (to make the service unavailable after next boot)
 # chkconfig --level <1-6><service name><on/off>
(to make the service available or unavailable on the particular run level)
 # chkconfig --level 5 vsftpd on
(to make the vsftpd service available on run level 5)
 # chkconfig --level 345 vsftpd on
(to make the vsftpd service available on run levels 3, 4 and 5)

RHEL - 7 commands :
 # systemctl status <service name> (to check the status of the service)
 # systemctl start <service name> (to start the service)
 # systemctl stop <service name> (to stop the service)
 # systemctl reload <service name> (to reload the service)
 # systemctl restart <service name> (to restart the service)

** These above commands will change the service statuses temporarily. So if we want to change statuses of the process automatically from next boot onwards we have to enable those services as given below.*
 # systemctl enable <service name> (to make the service available at next boot)
 # systemctl disable <service name> (to make the service unavailable at next boot)
 # grep <string name><file name> (to display the specified string in that file)
 # grep -n <string name><file name> (to display the string with line no's)
 # grep -e <string name 1> -e <string 2><file name>
(to display 2 or multiple strings in that file)
 # grep -o <string name><file name>
(to display only that string in that file not whole the text of that file)
 # grep -v <string name><file name>
(to display all the strings except the specified one)
 # grep ^ this coss
(to display the line which is starting with the specified string)

Chapter#13 – Managing Process

1. What is process and explain it?

A process is a set of instructions which executes in the memory. It is created in the memory when a program or command is executed. Every process is identified by a unique no. ie., PID (Process ID). Several processes are started at boot time and which are running at background called deamons. The Linux kernel is used to communicate with the processes by their process ID's (PID's). Deamon is a process running in the background. These are handled by the system and process are handled by the users.

*The first process in RHEL - 6 is **initd** and it starts at boot time. It's process ID is 1 where as in RHEL - 7 the first process is **systemd** and it starts at boot time. To manage or to see the processes there are two commands.*

(i) # ps and (ii) # top

 # ps :

It is just a snap shot of the current status of the processes. It gives only one terminal information not all the terminals information.

 # top :

Using top command we can monitor the processes continuously. By default every 3 seconds it will refresh the data.

2. How many process are run generally on Linux and explain them?

There are generally three types of processes that run on Linux. They are,

(i) Interactive Processes

(ii) System Process or deamon

(iii) Automatic or batch.

Interactive Processes :

Interactive processes are those processes that are invoked by a user and can interact with the user. For example # vi or # vim are the interactive processes. Interactive processes may be run in foreground or background. The foreground process is the process that we are currently interacting with and is using the terminal as its stdin (standard input) and stdout (standard output). The background process is not interacting with the user and can be in one of two states, ie., paused or running.

System Processes or deamons :

Deamon is refer to processes that are running on the computer and provides services but do not interact with the console. Most server software is implemented as a deamon. For example Apache, samba, sshd are the deamons. Any process can become a deamon as long as it is run in the background and does not interact with the user.

Automatic processes :

Automatic processes are not connected to a terminal and these are queued into a spooler area where they wait to be executed on a FIFO (First In - First Out) basis. Such tasks can be executed using one of two criteria. At certain date and time : done using the "at" command.When the total system load is low enough to accept extra jobs : done using the " cron " command. By default tasks are put in a queue where they wait to be executed until the system load is lower than 0.8 and cron job processing is also used for optimizing system performance.

3. What is parent process?

The process which starts or creates another process is called the parent process. Every process will be having a parent process except initd process. The initd process is the parent process to all the remaining processes in Linux system because it is the first process which gets started by the kernel at the time of booting and it's PID is 1. Only after initd process gets started, the remaining processes are called by it, and hence it is responsible for all the remaining processes in the system. The parent process is identified by PPID (parent process ID).

4. What is child process?

A process which started or created by the parent process is called child process and it is identified by PID.

Useful # ps commands :

 # ps -a (it displays all the terminals processes information)
 # ps -au (it displays all the terminals processes information with user names)
 # ps -aux (it displays all the terminals processes information including background processes with user names)
** ? (question mark) if it is appeared at tty column, it indicates that is a background process.*
 # ps -ef (it displays the total processes information with parent process ID (PPID))
 # ps -P <process id> (it displays the process name if we know the process ID (pid))
 # pidof<process name> (to see the process ID of the specified process)
 # pidof initd (to see the process ID of the initd process)
 # pstree (to display the parent and child processes structure in tree format)
 # ps -u <user name> (to display all the processes of the specified user)
 # ps -u raju (to display all the processes of the user raju)
 # ps -G <group name> (to display all the processes that are running by a particular group)
 # ps -o pid, comm, %mem, %cpu (to display process id, command, %memory and %cpu utilization nothing but filtering the output)
 # ps -Ao pid, comm, %mem, %cpu(to display the same information as above but including some more information)
 # ps -o pid, comm, %mem, %cpu |sort -k <no.> -r |head -n 10 (to display which process is utilizingmore memory or cpu in reverse order where -k means field, <no.> means field no. and -r reverse order)
 # ps -o pid, comm, %mem, %cpu |sort -k 3 -r |head -n 10 (to display the process which occupies more memory and cpu utilization in reverse order)
 # ps -aux |grep firefox (to check whether the firefox is running or not)
 # pgrep -U <user name> (to display all the process ID's only for that user)
** To communicate with the processes*
 # kill and # pkill commands are used.
 # kill -----> It will kill the processes using PID's.
 # pkill -----> It will kill the processes using process names.
** We can also give some signals while using the above commands and we get the signals information by*
 # kill -l command. This command will list all the signals with no's and there are 64 signals to pass.

5. What is signal in Process management?

Signals are a way of sending simple messages to processes. Most of these messages are already defined and however signals can only be processed when the process is in user mode. Every signal has a unique signal name. Each signal name is a macro which stands for a positive integer. Signals can be generated by the process itself or they can be sent from one process to another. A variety of signals can be generated or delivered and they have many uses for programmers.

6. What are the important signals in process management?

1.SIGHUP -----> to reload (read the configuration and load)
2.SIGINT -----> to interrupt from the keyboard (nothing but Ctrl + c)
3.SIGQUIT -----> to quit the process from keyboard (nothing but Ctrl + l)
9.SIGKILL -----> to kill the process forcefully (nothing but unblockable)
15. SIGTERM -----> wait for completing the process and then terminate (terminate gracefully)
18. SIGCONT -----> to continue or resume the process if it is stopped
19. SIGSTOP -----> to terminate the process (If it is not stopped the process we cannot continue or resume that process by Ctrl + c or Ctrl + z)
20. SIGHTSTP ----> to stop the process (nothing but Ctrl + z)
** But the most commonly used signals are 1, 9, 15 and 20.*
** The default signal is 15 (gracefully) when we not specified any signal.*
 # kill - <signal><process ID> (to kill the specified process using kill signal)
 # kill -9 1291 (to kill the process which has the PID as 1291)
** If we not specified the signal no. then the default signal 15 will effect.*
 # kill 1291 (to kill the process 1291 with default signal)
 # pkill -u <user name> (to kill all the processes of the specified user)
 # pkill -u raju (to kill all the processes of the user raju)
 # pkill -9 firefox (to kill the firefox process)

7. How many process states are there?

There are six process states and they are,
(i) Running process (the process which is in running state and is indicated by " r ").
(ii) Sleeping process (the process which is in sleeping state and is indicated by " s ")
(iii) Waiting process (the process which is in waiting state and is indicated by " w ").
(iv) Stopping process (the process which is in stopping state and is indicated by " T ").
(v) Orphan process (the process which is running without parent process and is indicated by " o ").
(vi) Zombie process (the process which is running without child process and is indicated by " Z ").

8. What is Orphan process?

The processes which are running without parent processes are called Orphan processes. Sometimes parent process closed without knowing the child processes. But the child processes are running at that time. These child processes are called Orphan processes.

9. What is Zombie process?

When we start parent process, it will start some child processes. After some time the child processes will died because of not knowing the parent processes. These parent processes (which are running without child processes) are called Zambie processes. These are also called as defaunct processes.

10. How to set the priority for a process?

Processes priority means managing processor time. The processor or CPU will perform multiple tasks at the same time. Sometimes we can have enough room to take on multiple projects and sometimes we can only focus on one thing at a time. Other times something important pops up and we want to devote all of our energy into solving that problem while putting less important tasks on the back burner.
In Linux we can set guidelines for the CPU to follow when it is looking at all the tasks it has to do. These guidelines are called niceness or nice value. The Linux niceness scale goes from -20 to 19. The lower the number the more priority that task gets. If the niceness value is higher number like 19 the task will be set to the lowest priority and the CPU will process it whenever it gets a chance. The default nice value is 0 (zero).By using this scale we can allocate our CPU resources more appropriately. Lower priority programs that are not important can be set to a higher nice value, while the higher priority programs like deamons and services can be set to receive more of the CPU's focus. We can even give a specific user a lower nice value for all his/her processes so we can limit their ability to slow down the computer's core services. There are two options to reduce/increase the value of a process. We can either do it using the nice or renice commands.

Examples *:*

 # nice -n <nice value range from -20 to 19><command>(to set a priority to a process before starting it)
 # nice -n 5 cat > raju (to set the medium priority to cat command)
 # ps -elf (to check the nice value for that command)

* *To reschedule the nice value of existing process, first check the PID of that process by*

 # ps -elf *command and then change the niceness of that command by*
 # renice <nice value (-20 to 19)>< PID > *command.*
 # renice 10 1560 (to reschedule the PID 1560)

11. What is top command and what it shows?

top is a command to see the processes states and statuses information continuously until we quit by pressing " q ". By default top command will refresh the data for every 3 seconds.
When we need to see the running processes on our Linux in real time, the top command will be very useful. Besides the running processes the top command also displays other information like free memory both physical and swap.
The first line shows the current time, "up 1 day" shows how long the system has been up for, "3 user" how many users login, "load average : 0.01, 0.00, 0.23" the load average of the system 1, 5 and 15 minutes.
The second line shows the no of processes and their current states.
The third line shows CPU utilization details like % of the users processes, % of the system processes, % of available CPU and % of CPU waiting time for I/O (input and output).
The fourth and fifth lines shows the total physical memory in the system, used physical memory, free physical memory, buffered physical memory, the total swap memory in the system, used swap memory, free swap memory and cached swap memory, ... etc.,
From sixth line onwards the fields are as follows.

PID	*Process ID*
USER	*Owner of the process ie., which user executed that process*
PR	*Dynamic Priority*
NI	*Nice value, also known as base value*
VIRT	*Virtual size of the task includes the size of processes executable binary*

RES	*The size of RAM currently consumed by the task and not included the swap portion*
SHR	*Shared memory area by two or more tasks*
S	*Task Status*
% CPU	*The % of CPU time dedicated to run the task and it is dynamically changed*
% MEM	*The % of memory currently consumed by the task*
TIME+	*The total CPU time the task has been used since it started. + sign means it is displayed with hundredth of a second granularity. By default, TIME/TIME+ does not account the CPU time used by the task's dead children*

COMMAND *Showing program name or process name.*

** While running the top command, just press the following keys woks and the output will be stored in real time.*

1	*----->*	*2nd CPU information*	*Shift + >*	*----->*	*Page up*
h	*----->*	*Help*	*Shift + <*	*----->*	*Page down*
Enter	*----->*	*Refresh immediately*	*n*	*----->*	*Number of tasks*
k	*----->*	*Kill the process*	*u*	*----->*	*user processes*
M	*----->*	*Sort by memory usage*	*P*	*----->*	*Sort by CPU usage*
T	*----->*	*Sort by cumulative time*	*z*	*----->*	*Color display*
r	*----->*	*To reschedule the priority by renice*	*d----->*		*Change the delay time (refresh time)*
b	*----->*	*Highlight the running process*	*W----->*		*Write the information in **/root/.toprc** file*
q	*----->*	*quit the top command*			

The status of the processes :

r	*----->*	*Running process*	*s*	*----->*	*Sleeping process*
z	*----->*	*Zombie process*	*T*	*----->*	*Stopped process*
D	*----->*	*Uninterrupted sleeping process*	*R <*	*----->*	*High priority*
N >	*---->*	*Low priority*	*o*	*----->*	*Orphan process*
+	*----->*	*Foreground process*	*?*	*----->*	*Background process*

 # renice -n 10 5453 *(to change the specified running process priority on line)*

 # nice -n -15 firefox *(to start the firefox process with priority level -15)*

12. How to solve the issue if the CPU utilization is 99% ?

(i) First check which process and who executed that process is consuming more CPU utilization or memory utilization by executing # top command.

(ii) Then inform to those users who executed that process though mail, message or raising the ticket.

(iii) If those users are not available or not responding to our mail then we have to change the priority of that process using # renice command.

(iv) Before changing the process priority level , we have to get or take approval from our team lead or project manager.

13. How to check the wwn no. of lun?

(i) First install sysutils package to execute the commands to know the wwn number by executing command,

 # yum install sysutils -y

(ii) # systool -c fs_host -v |grep "port-name" *(to check the wwn number)*

14. How to remove the page caches and other caches?

 # sysnc ; echo 2 > /proc/sys/vm/drop_caches (to remove the page caches)
 # sysnc ; echo 3 > /proc/sys/vm/drop_caches (to remove all types of caches like dent cache, page caches and others)

15. What is "sosreport" and how to generate it?

***Sosreport** is a command in linux (**RHEL / CentOS**) which collects **system configuration** and diagnostic information of your linux box like running kernel version, loaded modules, and system and service configuration files. This command also runs external programs to collect further information, and stores this output in the resulting archive.*
Sosreport is required when you have open a case with redhat for technical support. Redhat support Engineers will require sosreport of your server for troubleshooting purpose.
*To run sosreport , **sos** package should be installed. Sos package is part of default installation in most of linux. If for any reason this package is no installed , then use below yum command to install **sos package** :*
 # yum install sos -y
Generate the sosreport :
Open the terminal and type sosreport command :
 # sosreport
*This command will normally complete within a **few minutes**. Depending on local configuration and the options specified in some cases the command may take longer to finish. Once completed, sosreport will generate a compressed a file under **/tmp** folder. Different versions use different compression schemes (**gz, bz2, or xz**). The file should be provided to Redhat support representative (normally as an attachment to an open case).*
***Note:** sosreport requires root permissions to run.*
Different Options used in sosreport command :
*The sosreport command has a **modular structure** and allows the user to enable and disable modules and specify module options via the command line. To **list available modules** (plug-ins) use the following command:*
 # sosreport -l
*To **turn off** a module include it in a comma-separated list of modules passed to the -n/–skip-plugins option. For instance to disable both the kvmand amd modules:*
 # sosreport -n kvm,amd
*Individual modules may provide additional options that may be specified via the **-k option.** For example on Red Hat Enterprise Linux 5 installations the sos rpm module collects "rpm -Va" output by default. As this may be **time-consuming** the behaviour may be disabled via:*
 # sosreport -k rpm.rpmva=off

16. What is the command to see the complete information on virtual memory?

 # vmstat is the command to the complete information on virtual memory like no of processes, memory usage, paging memory, block I/O (input /output), traps, disk and CPU activity.
 # vmstat 2 10 (It will give the report for every 2 seconds upto 10 times)
The fields are, r -----> how many waiting processes
b -----> how many processes are busy
swapd -----> how much virtual memory used

free -----> how much memory is freely available
buffer -----> how much temporary memory using
caching-----> how much caching still using
swapin -----> how much data transferred from RAM to swap
swapout ---> how much data transferred from swap to RAM
bi -----> how much block input
bo -----> how much block output
system in ---> the no. of interrupts
system cs ---> the no. of contexts changed

 # vmstat -a (to see the active and inactive processes)
 # vmstat -d (to see the statistics of the disk used)
 # cat /proc/meminfo (to see the present memory information)

17. What is the command to see the I/O statistics?

 # iostat (to see the Input and Output statistics in the Linux system)
** This command is used to monitoring the system input, output statistics and processes transfer rate.*
** It is also used to monitor how many kilo bytes read per second and how many kilo bytes read and write, shows CPU load average statistics since the last reboot in first line and most current data is shown in the second line.*

18. How many CPUs are there in the system?

 # cat /proc/cpuinfo *command will show no. of CPUs, no. of cores, no. of threads, no. of sockets and the CPU architecture, ...etc., information.*
 # nproc *command will give the no. of CPUs present in the system.*
 # lscpu *command will give the information the architecture of the CPU (x86_64 or x86_32), no. of cores, no. of threads, no. of sockets, cache memory sizes (L 1, L 2, L 3, ...etc) , CPU speed and the vendor of the CPU.*

19. How to send the processor into offline?

 # ls -l /sys/devices/system/cpu is the command to see the no. of processors present in the system.
 # echo 0 > /sys/devices/system/cpu/cpu4/online is the command to send the CPU4 into offline.
 # grep "processor" /proc/cpuinfo or # cat /sys/devices/system/cpu/offline are the command to see the processor status whether offline.

20. How to send the processor into online?

 # ls -l /sys/devices/system/cpu is the command to see the no. of processors present in the system.
 # echo 1 > /sys/devices/system/cpu/cpu4/online is the command to send the CPU4 into offline.
 # grep "processor" /proc/cpuinfo or
 # cat /sys/devices/system/cpu/online are the command to see the processor status whether online.

21. How to clear /var and /tmp directories?

(i) Copy all the entries of those directories into a separate locations.
(ii) Redirect the null values in /var and /tmp directories by executing the below commands.
 # cat /dev/null > /var (to nullifying the /var directory)
 # cat /dev/null > /tmp (to nullifying the /tmp directory)

22. How to troubleshoot if df -k is giving error?

(I) First check which file system is giving error by # df -k command then see whether any files are opened or not.If opened then close those files by informing those teams which are using that file system.
(ii) Unmount that file system by taking approval from higher authorities and run fsck on that file system, then normally it will be solved if we run fsck command.
(iii) If not solved even though we run fsck then delete or remove that file system, recreate that file system, mount that file system and restore the data from recent backup.

23. What are the differences between a deamon and a process?

(i) Deamon is a service to provide some services to the users, where as a process is to do some particular tasks.
(ii) We can enable or disable the deamon, but we cannot disable or enable the process.
(iii) We can do start or stop the deamon, but we cannot start or stop the process. We only kill the process.
(iv) We can enable or disable to start the deamons at boot time as per our requirement, ie., on demand is possible, but it is not possible if is a process.
(v) Deamon is a background process where as process is a foreground process.

24. What is command to check the load average?

 # uptime is the command to check the system load, present time, from how many hours the system is running and load average.
** The load average shows three fields. The 1st field shows the load average from 1 minute, 2nd field shows the load average from 5 minutes and 3rd field shows the load average from 15 minutes.*

25. How to assign or shift the process to the particular CPU?

*(i) First install **util-linux** package by **# yum install util-linux -y** command.*
*(ii) Check the specified process is assigned to which processor ie., which CPU by **# taskset -p <pid>** command.*
*(iii) Then shift the process to another available CPU by **# taskset -cp <cpu -list><pid>** command.*
Examples:

```
# taskset -p 2125                (to check which processor is assigned to that process ID)
# taskset -cp 0, 4 2125          (to shift the process to the CPUs 0 and 4)
# taskset 0 firefox              (to assign the firefox process to the CPU 0)
```

26. How to limit the CPU usage of a linux process?

(a) First install the cpulimit package by # yum install cpulimit -y command.
** This package is not available in normal Linux packages and it is available in EPEL (Extra Packages for Enterprise Linux). So, first we have to enable the EPEL repository in our system by following steps.*
(i) # yum install epel-release -y (to install the epel-release package in RHEL - 7)
(ii) # rpm -Uvh http://mirrors.kernel.org/fedora-epel/6/i386/epel-release-6-8.noarch.rpm (to install the EPEL package in RHEL - 6)
(ii) # rpm -Uvh http://mirrors.kernel.org/fedora-epel/5/i386/epel-release-5-4.noarch.rpm (to install the EPEL package in RHEL - 5)
(iii) # rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-5 (to import the gpg key if it ask when executing the above command in RHEL - 5)

(iv) # rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6 (to import the gpg key if it ask when executing the above command in RHEL - 6)

(v) # rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7 (to import the gpg key if it ask when executing the above command in RHEL - 7)

(vi) # yum repolist (to check EPEL repolist)

(b) # cpulimit -p <PID> -l 10(to see the CPU usage of that process and limit the CPU usage to 10%)

(c)# cpulimit -e /usr/local/bin/myprog -l 20(to limit the CPU usage of this command to 20%)

27. How to capture the network traffic?

 # tcpdump *is the command to capture and analyze the network traffic. By using this command we can also troubleshoot the network problems.*

Examples :

 # tcpdump (to capture and analyze the network traffic)

 # tcpdump -i eth0 (to capture the network traffic from eth0 continuously and Ctrl + c to exit)

 # tcpdump -c 30 -i eth0 (to capture the network traffic from eth0 upto 30 packets only)

 # tcpdump -w /root/tcp.pcap -i eth0 to capture the network traffic from eth0 and write that in /root/tcp.pcap file)

 # tcpdump -t t t -r /root/tcp.pcap (to read the contents of the above captured file)

 # tcpdump -i eth0 port 22 (to capture the network traffic from eth0 of ssh traffic)

 # tcpdump -i eth0 dst 172.25.0.11 and port 22
(to capture the network traffic from 172.25.0.11 system of ssh traffic)

28. What is SAR utility and how to use it?

SAR stands for System Activity Report. Using SAR we can check the information of CPU usage, memory, swap, I/O, disk I/O, networking and paging. We can get the information of the present status and post status (history using the data) upto last 7 days because HISTORY=7 is there in the configuration file. The log messages are stored in /var/log/sa/sa1, /var/log/sa/sa2, /var/log/sa/sa3, ...etc., (where 1, 2, 3, ...etc., are dates). The SAR configuration is stored in /etc/sysconfig/sysstat file. In this file the HISTORY=7 default option will be there. So, we can change the default 7 days to our required value.

Before using the SAR utility first we should install the SAR utility package by ***# yum install sysstat* -y*** *command.*

Examples :

 # sar 2 10 (It will give the system report for every 2 seconds upto 10 times)

 # sar -p 2 10 (to see the CPU utilization for every 2 seconds upto 10 times)

 # sar -p ALL -f /var/log/sa/sa25 (to check the CPU utilization on 25th day of the current month)

 # sar -p ALL -f /var/log/sa/sa10 -s 07:00:00 -e 15:00:00 (to check the CPU utilization on 10th day of the current month from 7:00 to 15:00 hrs. where -s means start time -e end time)

 # sar -r 2 10 (to see the memory utilization for every 2 seconds upto 10 times)

 # sar -r -f /var/log/sa/sa14 (to check the memory utilization on 14th day of the current month)

 # sar -r -f /var/log/sa/sa10 -s 07:00:00 -e 15:00:00 (to check the memory utilization on 10th day of the current month from 7:00 to 15:00 hrs. where -s means start time -e end time)

 # sar -S 2 10 (to see the swap utilization for every 2 seconds upto 10 times)

 # sar -S -f /var/log/sa/sa25 (to check the swap utilization on 25th day of the current month)

 # sar -S -f /var/log/sa/sa10 -s 07:00:00 -e 15:00:00
(to check the swap utilization on 10th day of the current month from 7:00 to 15:00 hrs. where -s means start time -e end time)
 # sar -q 2 10 (to see the load average for every 2 seconds upto 10 times)
 # sar -q -f /var/log/sa/sa14 (to check the load average on 14th day of the current month)
 # sar -q -f /var/log/sa/sa10 -s 07:00:00 -e 15:00:00
(to check the load average on 10th day of the current month from 7:00 to 15:00 hrs. where -s means start time -e end time)
 # sar -B 2 10 (to see the paging information for every 2 seconds upto 10 times)
 # sar -d 2 10 (to see the disk usage for every 2 seconds upto 10 times)
 # sar -m 2 10 (to see the power management for every 2 seconds upto 10 times)
 # sar -b 2 10 (to see the disk input and output statistics for every 2 seconds upto 10 times)

29. What are the port no. for different services?

The Port no. list :

FTP (For data transfer)	20	HTTP	80
FTP (For connection)	21	POP3	110
SSH	22	NTP	123
Telnet	23	LDAP	389
Send Mail or Postfix	25	Log Server	514
DNS	53	HTTPS	443
DHCP (For Server)	67	LDAPS (LDAP + SSL)	636
DHCP (For Client)	68	NFS	2049
TFTP (Trivial File transfer)	69	Squid	3128
Samba shared name verification	137	Samba Data Transfer	138
Samba Connection Establishment	138	Samba Authentication	445
MySQL	3306	ISCSI	3260

** Ping is not used any port number. It is used ICMP (Internet Control Message Protocol) only.*

Other useful commands :
 # uptime (to see from how long the system is running and also gives the load average report)
** The load average is having 3 fields. 1 - present status, 2 - 5 minutes back and 3 - 15 minutes back.*
 # iostat 5 2 (to monitor the input and output statistics for every 5 seconds upto 10 times)
 # nproc (to check how many processors (CPUs) are there in the system)
 # top 1 (to see the no. processors (CPUs) are there in the system)
 # iptraf (to monitor the TCP or network traffic statistics in graphical mode)
** Before using this command install the iptraf package by # yum install iptraf* -y command.*
 # iftraf -ng -f eth0 (to see the IP traffic statistics in graphical mode)

 # lscpu (to see the no. of CPUs present in the system)
 # lsusb (to see the no. of USB devices present in the system).
 # lsblk (to see all the partitions or block devices information)
 # cat /etc/redhat-release (to see the RHEL version of system)
 # dmidecode
(to see the complete hardware information of the system)
 # dmidecode -t memory (to see the memory information of the system)
 # dmidecode -t bios (to see the system's bios information)
 # dmidecode -t system (to see the system's information)
 # dmidecode -t processor
(to see the processor's (CPU's) information of the system)
 # dmidecode -t 1 (to check the System's Serial No. information)
 # dmidecode -t 4 (to see the processor's (CPU's) information)
 # dmidecode -t 16 (to check the Max. RAM capacity of the system)
 # dmidecode -t 17 (to check how much RAM the system is using)
 # pidstat
(to monitoring the individual tasks currently being managed by the Linux kernel)
 # nfsiostat (to monitor the NFS input and output statistics)
 # cifsiostat (to monitor the Samba input and output statistics)
 # stat <file name or directory name> (to see the statistics of the file or directory)
 # strings <command name> (to read the binary language of the command)
 # find / -nouser -o -nogroup
(to see the files which are no belongs to any user and any group)
 # systemctl -t help (to see the list of systemd objects that are available)
 # systemctl -l help (to see the list of unit names)
 # systemctl list-dependencies <service name> (to see the dependent services in a tree manner)
 # sleep <seconds>& (to run the sleep processes at background)
 # jobs (to see the background jobs which were sent by the user)
 # fg % < Job ID > (to get back the background job to foreground job)
 # Ctrl + z (to stop the process)
 # bg % < Job ID > (to restart the process again at background)

** When there are stopped jobs and want to exit from the terminal then, a warning message will be displayed. If we try again to exit from the terminal,then the stopped or suspended jobs will be killed automatically.*

Chapter#14 – FTP(File Transfer Protocal)

1 What is FTP?

FTP stands for File Transfer Protocol used to transfer files from one host to another host over a TCP-based network.

2. How ftp works?

FTP is built on client-server architecture and utilizes separate control and data connection between the client and server. FTP users may authenticate themselves using a clear-text sign-in protocol but can connect anonymously if the server is configured to allow it.

Usually, the FTP server, which stores files to be transferred, uses two ports for the transferring purpose. One port for commands and another port for sending and receiving data. Requesting from client computers are received at the port 21 of server. ie., it is exclusively reserved for sending commands, therefore it is called the Command Port. Once an incoming request is received, the data requested or uploaded by the client computer is transferred through a separate port 22 and referred as Data Port. At this point, depending on the Active or Passive mode of the FTP connection, the port number used for the Data Transfer Varies.

3. What is Active FTP?

In Active FTP connection, the connection is initiated by the Client, and the data connection is initiated by the Server. And as the server actively establishes the data connection with the client, hence it is called the Active FTP. Here the client opens up a port higher than 1024 and it connects to the server through port 21. Then the server opens its port 20 to establish a data connection.

4. What is Passive FTP?

In Passive FTP connection, both command and data connections are established by the client. In this the server acts as entirely passive, that's why it is called the Passive FTP. Here the server listens for incoming requested connections from client through port 21 and the client also initiates the data connection at port 20.

5. What is the main difference between the Active FTP and Passive FTP?

The main difference between the Active FTP and the Passive FTP is based on who initiates the data connection between the server and the client. If the data connection is initiated by the server, that is called Active FTP and if the data connection is initiated by the client, that is called Passive FTP.

6. What is the profile for FTP server?

(i) It is used for uploading and downloading the files and directories cannot be downloaded.
(ii) The FTP server packageis vsftpd.
(iii)The FTP client packages are ftp and lftp.
(iv) The FTP server deamon is vsftpd (Very Secure FTP deamon)
(v) The FTP scripting file is /etc/initd/vsftpd
(vi) Port numbers 20 for data connection and 21 for FTP command connection.
(viii) The document root for FTP is /var/ftp

(viii) The FTP home directory is /var/ftp
(ix) The FTP configuration files are,
(a) /etc/vsftpd/vsftpd.conf
(b) /etc/vsftpd/user_list
(c) /etc/vsftpd/ftpuser
(d) /etc/pam.d/vsftpd

7. How to configure the FTP server?

(i) Install the FTP package by # yum install vsftpd -y command.*
(ii) Goto FTP document root directory and create some files by # cd /var/ftp/pub
 # touch f(1..10}
(iii) Restart the FTP service or deamon by # service vsftpd restart command in RHEL - 6.
 # systemctl restart vsftpd command in RHEL - 7.
(iv) Make the FTP service or deamon enable even after reboot the server by
 # chkconfig vsftpd on command in RHEL - 6 and # systemctl enable vsftpd command in RHEL - 7.
(v) Add the FTP service to the IP tables (RHEL - 6) and Firewalld (RHEL - 7).

RHEL - 6 :

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 21 -j ACCEPT
# iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 21 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 20 -j ACCEPT
# iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 20 -j ACCEPT
```

RHEL - 7 :

```
# firewall-cmd --permanent -add-service=ftp command in RHEL - 7.
# firewall-cmd --complete-reload command in RHEL - 7.
```

8. How to configure the FTP client and how to connect the ftp server?

*(i) Go to the client machine and install the **FTP** and **Lftp** packages.*
 # yum install ftp lftp* -y*
(ii) Connect the FTP server from client.
 # ftp <FTP server IP address or server host name>

Example : # ftp 172.25.9.11 or ftp://server.example.com
Username : ftp
Password : <press enter key>
ftp > ls (to see the files in the FTP document root directory)

(iii) We can also connect the FTP server through browser.
(i) Open the web browser and type in address bar as,
ftp://172.25.9.11 or ftp://server.example.com

9. How to configure the Secure FTP server?

(i) Open the FTP configuration file by # vim /etc/vsftpd/vsftpd.conf command.
(ii) Go to line no : 12 and type as, ananymous_enable=no (save and exit the file)

** ananymous_enable=yes (by default)*
It means anybody can login to the FTP server without any username and password.
If ananymous_enable=no, then we must provide the username and passwords when it prompts.
(iii) Restart the ftp deamon by # service vsftpd restart command in RHEL - 6 or
 # systemctl restart vsftpd command in RHEL - 7.
(iv) Assign the FTP user password by # passwd ftp (type and retype the ftp user password)
(v) Go to client side and connect the FTP server by # ftp 172.25.9.11 command.

10. How to configure the FTP server to upload the files feature?

(i) Open the FTP configuration file by # vim /etc/vsftpd/vdftpd.conf command.
(ii) Go to line no : 19 and type as, writable_enable=yes
(iii) Go to line no : 29 and type as, anon_upload_enable=yes (save and exit the file)
(iv) Make the uploaddirectory in /var/ftp/pub directory by # mkdir /var/ftp/pub/upload
(v) Change the group of the upload directory as ftp by # chgrp ftp upload command.
(vi) Change the permissions of the upload directory by # chmod 775 upload command.
(vii) To permanently add the ftp service to SELinux policy by
 # getsebool -a | grep ftp (to check the SELinux Booleans for FTP service)
 # setsebool -p allow_ftpd_anon_write on
 # chcon -t public_content_rw_t upload (to add read-write context of the upload directory)
 # setsebool -p ftp --full-access=1 command or # setenforce=0 command to disable the SELinux.
(viii) Restart the ftp deamon by # service vsftpd restart command in RHEL - 6 or
 # systemctl restart vsftpd command in RHEL - 7.

11. How to deny the particular system to use the FTP server?

(i) Open the /etc/hosts.deny file and put an entry of system which one to deny the ftp service.
 # vim /etc/hosts.deny (goto last line and type as below)
vsftpd : 172.25.9.10 (to deny 172.25.9.10 system)
vsftpd : ALL (to deny all the systems)
*vsftpd : ALL EXCEPT *.example.com*
(to deny all the systems except example.com domain systems)
(save and exit the file)
(ii) Restart the ftp deamon by
(iii) # service vsftpd restart command in RHEL - 6 or
 # systemctl restart vsftpd command in RHEL - 7.
** Now 172.25.9.10 system will not access the FTP services.*
** If we put an entry in /etc/hosts.allow file as, ALLOW ALL EXCEPT 172.25.5.10 then, except 172.25.5.10 system all the systems can avail the FTP service.*

12. How to change the ownership of the uploaded file in FTP?

If we upload or download any files the files owner and group are ftp only. We can change the ownership of the uploaded or downloaded files as follows.
(i) Open the FTP configuration file by # vim /etc/vsftpd/vsftpd.conf command.
(ii) Go to line no : 48 and type as, chown_upload=yes
(iii) Go to line no : 49 and type as, chown_username=<user name>
(iv) We can display the banner when we connect the FTP server by uncomment on line no : 86 and

type as, ftp_banner=" Welcome to Hyderabad "

(v) We can limit the FTP maximum connections at a time to 5 by put an entry in configuration file as,

max_clients=5 (save and exit the file)

(v) Restart the ftp deamon by # service vsftpd restart command in RHEL - 6 or

 # systemctl restart vsftpd command in RHEL - 7.

13. How to deny specific users to access the ftp services?

(i) Open the FTP users file by # vim /etc/vsftpd/ftpusers command.

(ii) Enter the user names whom to deny FTP services. For example as follows,

root

raju

junnu

(save and exit the file)

(ii) Restart the ftp deamon by

 # service vsftpd restart command in RHEL - 6 or

 # systemctl restart vsftpd command in RHEL - 7.

14. What is LFTP and how to configure LFTP?

LFTP is also used to upload or download the files. But, by using LFTP we can login to the FTP server without password because It will not ask any passwords. To use LFTP we have to install the LFTP package on server.

(i) Install the LFTP package by # yum install lftp -y command.*

(ii) Restart the lftp deamon by # service lftpd restart command in RHEL - 6 or

 # systemctl restart lftpd command in RHEL - 7.

(iii) Go to client system and access the LFTP server by,

 # lftp 172.25.9.11 (to connect the LFTP server)

lftp> cd pub (to move to the pub directory)

lftp> get f1 (to download the f1 file)

lftp> mget f2 f3 f4 f5 (to download the f2 f3 f4 and f5 multiple files at a time)

lftp> put f9 (to upload the f9 file)

lftp> mput f10 f11 f12 (to upload the f10 f11 f12 multiple files at a time)

lftp> quit (to quit the ftp server)

** In LFTP " Tab " key works as usual but in FTP " Tab " will not work.*

15. How to allow the root user to access the FTP server?

By default root user is blocked to access the FTP server. To allow the root user to access the FTP server follow the below steps.

(i) Open the /etc/vsftpd/user_list file by # vim /etc/vsftpd/user_list command.

(ii) Go to root user line and comment on that line. For example

 # root

(save and exit the file)

(iii) Open the /etc/vsftpd/ftpuser file by # vim /etc/vsftpd/ftpuser command.

(iv) Go to root user line and comment on that line. For example

 # root (save and exit the file)

(v) Restart the ftp deamon by

 # service vsftpd restart command in RHEL - 6 or
 # systemctl restart vsftpd command in RHEL - 7.
** Even though we changed the above, the root user cannot access the FTP server because the home directory context is not added. we can solve this as follows.*
(vi) # getsebool -a | grep ftp (to check the SELinux Boolean of the root home directory)
(vii) # setsebool -p ftp_home_dir on (to change the Boolean of the root home directory)
** Now go to client system and try to login the FTP server as root user. Here we can access the FTP server.*

16. What are the difference between FTP and LFTP servers?

(i)The user name and password are required to access the FTP server but LFTP does not requires passwords.
*(ii) In ftp>prompt the **" Tab "** key will not work but in lftp> prompt the **" Tab "** key will work as usual.*

Other useful FTP Commands :

 # ftp 172.25.9.11 (to access the FTP server provide FTP user name and password)
ftp > ls (to see all the files and directories in FTP root directory)
ftp > !ls (to see the local nothing present working directory files)
ftp > pwd (to see the FTP present working directory)
ftp > !pwd (to see the local file system's present working directory)
ftp > get <file name> (to download the specified file)
ftp > mget <file 1><file 2><file3> (to download multiple files at a time)
ftp > cd /var/ftp/pub/upload (to move to upload directory)
ftp > put <file name> (to upload the specified file into the FTP upload directory)
ftp > lcd /root/Downloads (to change to the local /root/Download directory)
ftp > help (to get the help about FTP commands)
ftp > bye or quit (to quit or exit from the FTP server)
 # lftp 172.25.9.11 (to access the LFTP server without asking any passwords)

Chapter#15 – NFS(Network File System)

1. What is NFS? Explain it.

NFS stands for Network File system and it is way to share the local hard drive files between machines which are NFS compatible. That means we share the files between Linux and Unix machines but not between Linux and windows systems. NFS is used upd protocol.
Normally the NFS server exports one or more directories to the client system and the client system mount one or more of the shared directories called mount points. After the NFS is mounted, all I/O operations are written back to the server, and all the clients notice the change. A manual refresh is not needed because the client access the remote file systems same as local file system because access does not requires the IP address, user name and password. However we can provide the security using the kerberos security.

2. What are the disadvantages of NFS?

(i) NFS does not support cross plat forms. ie., it will not support the sharing the files between Linux and Windows systems.
(ii) NFS does not support encryption of the data and it supports only plain text format.
(iii) NFS does not support TCP Wrappers, ie., NFS does not support /etc/hosts.allow and /etc/hosts.deny, because there is no libwrap.so module is not loaded with NFS service.
(iv) NFS does not support authentication. So, to overcome this problem kerberos security system is used.

3. What is the profile of NFS?

Package	*:*	*nfs**
Services	*:*	*nfs (in RHEL - 6)*
		nfs-server, nfs-secure-server (nfs with kerberos) (both for NFS server)
		nfs-secure (for NFS client) (these three services are in RHEL - 7)
Script	*:*	*/etc/init.d/nfs*
Port numbers	*:*	*2049 (for NFS server) and below 1024 (for NFS client)*
Configuration Files	*:*	*/etc/exports and /etc/sysconfig/nfs*
Other Important Files	*:*	*/var/lib/nfs/etab and /var/lib/nfs/rmtab*
Versions	*:*	*NFS - 3 (default in RHEL - 5) but it supports NFS - 4*
		NFS - 4 (default in RHEL - 6) but It also supports NFS - 3
		NFS - 4 (default in RHEL - 7) but it also supports NFS - 3
Protocol	*:*	*udp protocol*

4. What are the background deamons for NFS and explain them?

There are 6 background deamons for NFS.
(i) rpc . mountd :
This deamon is responsible for executing mount and unmount requests by the client.
(ii) rpc . nfsd : This deamon responds to clients requests for file access.
(iii) rpc . rquotad : This deamon is responsible for enabling quotas on NFS shared devices.
(iv) rpc . statd : This deamon is used to see the statistics about NFS server from NFS client when

executing the commands # netstat or # nfsstat (to see the I/O statistics of NFS)
(v) rpc . lockd : This deamon manages file locks and releases incase of client disconnected.
(vi) rpc . idmapd : This deamon is responsible for mapping user id and group id towards themselves.

5. What are the difference between NFS 3 and NFS 4?

In NFS 3 there is no security to protect the data, but in NFS 4 there is a kerberos security to protect the data.
In NFS 3 there is no ACL permissions on the shared directory, but in NFS 4 there is an ACL permissions on the shared directory.

6. In how many ways we can mount the NFS shared directory?

In order to access the NFS shared data, we have to mount that shared directory on local mount point. The mounting can be direct mount (manual mount) and indirect mount (auto mount).
Direct mount :
First create the local mount point and then mount that shared NFS directory on our local systems mount point by # mount <server host name or IP address> : <shared directory with full path><mount point> command. But this is temporary mount and we can mount it permanently by put an entry in /etc/fstab file.
Example :
 # mount 172.25.9.11:/product /mnt/nfs
(to mount the directory /product on /nfs mount point temporarily)
 # vim /etc/fstab (open this file and put an entry of mount point to mount permanently)
172.25.9.11:/product /mnt/nfs nfs defaults 0 0 (save and exit this file)

Indirect mount :
This method is used to mount the NFS share by using the Autofs service. Autofs uses the automount daemon to manage our mount points by only mounting them dynamically when they are accessed. Autofs consults the master map configuration file /etc/auto.master to determine which mount points are defined. It then starts an automount process with the appropriate parameters for each mount point. Each line in the master map defines a mount point and a separate map file that defines the file systems to be mounted under this mount point.

For example, the /etc/auto.misc file might define mount points in the /mnt directory; this relationship would be defined in the /etc/auto.master file.
Each entry in auto.master has three fields. The first field is the mount point. The second field is the location of the map file, and the third field is optional. The third field can contain information such as a timeout value.

For example, to mount the directory /product on the remote machine server9.example.com at the mount point /mnt/nfs on your machine, add the following line to auto.master:
/mnt /etc/auto.misc --timeout 60
Next, add the following line to /etc/auto.misc:
nfs -rw server9.example.com:/product
The first field in /etc/auto.misc is the name of the /mnt subdirectory.

This subdirectory is created dynamically by automount. It should not actually exist on the client machine. The second field contains mount options such asrw for read and write access. The third field is the location of the NFS export including the hostname and directory.
The directory /mnt must be exits on the local file system. There should be no sub directories on the local file system.
To start the autofs service, at a shell prompt, type the following command:
 # servive autofs restart
To view the active mount points, type the following command at a shell prompt:
 # service autofs status
If you modify the /etc/auto.master configuration file while autofs is running, you must tell the automount daemon(s) to reload by typing the following command at a shell prompt:
 # service autofs reload

7. How to configure NFS server?

(i) First install the NFS package by # yum install nfs -y command.*
(ii) Create the NFS shared directory on server system by # mkdir /public command.
(iii) Modify the permissions of the /public directory by # chmod 777 /public command. (These permissions may be changed depend on it's requirement)
(iv) Modify the SELinux context of the /public directory if SELinux is enabled by executing the below command. # chcon -t public_content_t /public
(v) create some files in the /public directory by # touch f{1..10} command.
(vi) Open the file NFS configuration file and put an entry of the NFS shared information by # vim /etc/exports command and type as an entry like <shared directory name><to whom to export the shared directory> (<permissions>, sync)
For example,
*# vim /etc/exports /public *.example.com (ro/rw, sync)*
(save and exit the file)

- *Where *.example.com means the shared directory can be exported to all the systems of the example.com domain.*
- *Permissions like ro (read only) or rw (read & write) and sync means the data will always be synced.*

/public desktop9.example.com (rw, sync) (to export the /public to desktop 5 system only)
*/public *.example.com (ro, sync) (export to the entire example.com domain with read only)*
/public 172.25.0.0/24 (rw, sync) (export to 172.25.0.0 network only with read and write)
/public server [0 - 20].example.com (rw, sync) (export to server0 to server20 in example.com domain with read and write)
/public 172.25.0.10 (rw, sync) (export to 172.25.0.10 network only with read and write)

Common Mount permission options :

rw	*read/write permissions*
ro	*read-only permissions*
insecure	*Allows the use of ports over 1024*

sync	*Specifies that all changes must be written to disk before a command completes*
no_wdelay	*Forces the writing of changes immediately*
root_squash	*Prevents root users*

(vii) Export the above shared directory to the defined client systems by # exportfs -rv command.
(viii) Restart the NFS services by following the commands in RHEL - 6 and RHEL - 7.
 # service rpcbind restart (to restart the rpcbind service in RHEL - 6)
 # service nfs restart (to restart the NFS service in RHEL - 6)
 # systemctl restart nfs-server (to restart the NFS service in RHEL - 7)
(ix) Make the NFS service permanently boot at next boot time onwards as follows.
 # chkconfig rpcbind on (to on the rpcbind service in RHEL - 6)
 # chkconfig nfs on (to on the nfs service in RHEL - 6)
 # systemctl enable nfs-server (to enable the nfs-server in RHEL - 7)
(x) Export the NFS shared directory as follows.
 # exportfs -rv
(xi) Enable the NFS service to the IP tables and Firewall in RHEL - 6 and RHEL - 7 as follows.
In RHEL - 6 :
(i) # setup
(a) Select Firewall Configuration.
(b) Select Customize (Make sure firewall option remain selected).
(c) Select NFS4 (by pressing spacebar once).
(d) Select Forward and press Enter.
(e) Select eth0 and Select Close button and press Enter.
(f) Select ok and press Enter.
(g) Select Yes and press Enter.
(h) Select Quit and press Enter.

(ii) Now open/etc/sysconfig/iptables file and add the following rules under the rule for port 2049 and save file.

```
-A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 32803 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 32769 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 662 -j ACCEPT
```

(iii) Restart the IP tables service by # service iptables restart command.
(iv) Make the IP tables service as permanent from next boot onwards as follows.
 # chkconfig iptables on

The following commands could be helpful for troubleshooting :

# mountstats	*Shows information about mounted NFS shares*
# nfsstat	*Shows statistics of exported resources*
# nfsiostat	*Shows statistics of NFS mounted shares*

In RHEL - 7 :

 # firewall-cmd --permanent -add-service=nfs (to enable the nfs service at firewall)
 # firewall-cmd --permanent -add-service=mountd (to enable the mountd service at firewall)
 # firewall-cmd --permanent -add-service=rpc-bind (to enable the rpc-bind service at firewall)
 # firewall-cmd --complete-reload (to reload the firewall)

8. What are requirements for NFS client?

(i)NFS server IP address or hostname.
(ii) Check the NFS shared name.
(iii) Create the local mount point.
(iv) Mount the NFS shared name on the local mount point.
(v) Go to mount point (local mount point) and access the NFS shared data.

9. How to access the NFS shared directory from the client?

(i) On Client system, install the nfs-utils package by # yum install nfs-utils -y command.*
(ii) Check the exported NFS shared directory by # showmount -e <IP address or hostname of the server>
Example : # showmount -e 172.25.9.11 or # showmount -e server9.example.com
(iii) Create one mount point to mount the NFS shared directory by
 # mkdir /<mount point> command.
Example : # mkdir /mnt/nfs
(iv) Mount the NFS shared directory on the above created mount point.
 # mount <IP address or server hostname> : <NFS shared directory><mount point>
Example : # mount 172.25.9.11:/public /mnt/nfs or
 # mount server9.example.com:/public /mnt/nfs
** These are temporary mount only. ie., If the system is rebooted these are unmounted automatically and we have to mount again after the system is rebooted.*
(v) So, if we want to mount it permanently, then open /etc/fstab file and put an entry of the mount point. # vim /etc/fstab (to open the file)
<IP address or server hostname> : <shared name><mount point><file system> defaults 0 0
Example : 172.25.9.11:/public /mnt/nfs nfs defaults 0 0 (or)
server9.example.com:/public /mnt/nfs nfs defaults 0 0 (save and exit the file)
(vi) Mount all the mount points as mentioned in the above /etc/fstab file by # mount -a command.
(vii) # df -hT command is used to check all the mounted partitions with file system types.

10. Why root user cannot create the files in the NFS shared directory and how to make him to create the files?

The root user normally has all the permissions, but in NFS root user is also becomes as a normal user. So, the root user having no permissions to create the files on the NFS shared directory.
The root user becomes as nfsnobodyuser and group also nfsnobody due to root_squash permission is there by default. So, if we want to make the root user to create file on the NFS shared directory, then go to server side and open the /etc/exports file and type as below,

<shared name> <domain name or systems names>(permissions, sync, no_root_squash)
*Example : /public *.example.com(rw, sync, no_root_squash) (save and exit the file)*
 # exportfs -rv (to export the shared directory)
 # service nfs restart (to restart the NFS service in RHEL - 6)
 # systemctl restart nfs-server (to restart the NFS service in RHEL - 7)

11. What are the disadvantages of the direct or manual mounting?

*(i) Manual mounting means, we have to mount manually, so it creates so many problems. For example if NFS service is not available then, **# df -hT** command will hang.*
*(ii) If the NFS server is down while booting the client, the client will not boot because it searches for NFS mount point as an entry in **/etc/fstab** file.*
(iii) Another disadvantage of manual mounting is it consumes more memory and CPU resources on the client system.So, to overcome the above problems normally indirect or automount is used using Autofs tool.

12. What is secure NFS server and explain it?

*Secure NFS server means **NFS server with Kerberos security**. It is used to protect the NFS exports. Kerbebors is a authentication tool to protect the NFS server shares. It uses the krb5p method to protect by authentication mechanism and encrypt the data while communication.*
For this one key file is required and this should be stored in each and every client which are accessing the nfs secure directory. Then only Kerberos security will be available. This key file should be stored in /etc/krb5.keytab file. For example the following command will download and store the keytab.
 # wget http://classroom.example.com/pub/keytabs/server9.keytab -O /etc/krb5.keytab (where O is capital)

13. How to configure the secure NFS server?

(i) Install the NFS package.
 # yum install nfs -y*
(ii) Create a directory to share through NFS server.
 # mkdir /securenfs
(iii) Modify the permissions of shared directory.
 # chmod 777 /securenfs
(iv)Change the SELinux context of the directory if the SELinux is enabled.
 # chcon -t public_content_t /securenfs
(v) Open the NFS configuration file and put an entry of the shared directory.
 # vim /etc/exports
*/securenfs *.example.com(rw,sec=krb5p) (save and exit the file)*
(vi)Download the keytab and store it in /etc/krb5.keytb file.
 # wget http://classroom.example.com/pub/keytabs/server9.keytab -O /etc/krb5.keytab

(vii)Export the shared the directory.

 # exportfs -rv

(viii) Restart and enable the NFS services in RHEL - 6 and RHEL - 7.

 # service nfs restart (restart the NFS service in RHEL - 6)

 # service nfs-secure-server restart (restart the secure NFS service in RHEL - 6)

 # chkconfig nfs on (enable the NFS service in RHEL - 6)

 # systemctl restart nfs-server (restart the NFS service in RHEL - 7)

 # systemctl restart nfs-secure-server (restart the secure NFS service in RHEL - 7)

(ix) Enable the IPtables or firewall to allow NFS servicein RHEL - 6 and RHEL - 7 as follows.

In RHEL - 6 :

(i) # setup

(a) Select Firewall Configuration.

(b) Select Customize (Make sure firewall option remain selected).

(c) Select NFS4 (by pressing spacebar once).

(d) Select Forward and press Enter.

(e) Select eth0 and Select Close button and press Enter.

(f) Select ok and press Enter.

(g) Select Yes and press Enter.

(h) Select Quit and press Enter.

(ii) Now open /etc/sysconfig/iptables file and add the following rules under the rule for port 2049 and save file.

```
-A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 32803 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 32769 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 662 -j ACCEPT
```

(iii) Restart the IP tables service by # service iptables restart command.

(iv) Make the IP tables service as permanent from next boot onwards as follows.

 # chkconfig iptables on

In RHEL - 7 :

 # firewall-cmd --permanent -add-service=nfs (to enable the nfs service at firewall)

 # firewall-cmd --permanent -add-service=mountd (to enable the mountd service at firewall)

 # firewall-cmd --permanent -add-service=rpc-bind (to enable the rpc-bind service at firewall)

 # firewall-cmd --complete-reload (to reload the firewall)

14. How to access the secure NFS server on client side?

(i) Install the nfs-utils package.

 # yum install nfs-utils -y*

(ii) Download the same key tab and store it in /etc/krb5.keytab file.

 # wget http://classroom.example.com/pub/keytabs/desktop9.keytab -O /etc/krb5.keytab

(iii) Check the shared NFS directory.

 # showmount -e server9.example.com

(iv) Restart the secure NFS service on client side.

 # service nfs-secure restart (restart the secure NFS client service in RHEL - 6)

 # systemctl restart nfs-secure (restart the secure NFS client service in RHEL - 7)

(v) Create the mount point on client system. # mkdir /mnt/nfssecure

(vi) Mount the NFS shared directory on the local mount point temporarily.

 # mount server9.example.com:/securenfs /mnt/nfssecure

(vii) Open /etc/fstab file and put an entry of the NFS shared mounting details to mount it permanently.

 # vim /etc/fstab

server9.example.com:/securenfs /mnt/nfssecure nfs defaults,sec=krb5p 0 0

(save and exit the file)

(viii) Mount all the file systems which are having the entries of the /etc/fstab file.

 # mount -a

(ix) Check all the mounted file systems with file system type on client system.

 # df -hT

15. How to mention the NFS version while configuring?

(i) Open /etc/sysconfig/nfs file by # vim /etc/sysconfig/nfs command.

(ii) Go to line no. 13 and edit the line as below,

RPCNFSDARGS=" - 4.2 "

(iii) Save and exit this file.

16. How to add the LDAP user shared directory and how the LDAP user access that directory on client?

(i) Create a sub-directory in /securenfs directory.

 # mkdir /securenfs/secure

(ii) Change the ownership of the above sub directory to LDAP user.

 # chown ldapuser9 /securenfs/secure

(iii) Assign the full permissions on that directory to LDAP user.

 # setfacl -m u : ldapuser9 : rwx /securenfs/secure

(iv) Change the SELinux context of that directory if SELinux is enabled.

 # chcon -t public_content_t /securenfs/secure

(v) Re-export the secure NFS shared directory.

 # exportfs -rv

(vi) Restart the NFS services.

 # service nfs restart (restart the NFS service In RHEL - 6)

 # service nfs-secure-server restart (restart the secure NFS service In RHEL - 6)

 # systemctl restart nfs (restart the NFS service In RHEL - 7)

 # systemctl restart nfs-secure (restart the secure NFS service In RHEL - 7)

On Client side :

(i) Login as LDAP user on local system through ssh.

(ii) # ssh ldapuser9@localhost (type yes and press Enter if it asks (yes/no))

(ii) Type the password as kerberos if it asks the LDAP user password.

(iii) Go to that secure NFS shared mount point and access the contents.

$ cd /mnt/nfssecure	*(to access the mount point)*
$ ls	*(to see the contents in that)*
$ cd secure	*(to access the sub directory)*
$ ls	*(to see the contents in that)*
$ exit	*(to exit or logout from ssh)*

17. What are the advantages of NFS?

(i) NFS allows multiple computers can use same files, because all the users on the network or domain can access the same data.
(ii) NFS reduces the storage costs by sharing applications on computers instead of allocating local disk space for each user application.
(iii) NFS provides data consistency and reliability, because all users can read same set of files.
(iv) NFS supports heterogeneous environments which are compatible to NFS.
(v) NFS reduces System Administration overhead.

18. Remote user cannot mount the NFS shared directory. How to resolve this?

(i) First check the user belongs to the same domain as the NFS shared or not. ie., the user's system domain and NFS shared system domain should communicate.
(ii) Check the user's system is pinging or not.
(iii) Check the user's name is present, not present or disabled to access the NFS server.
(iv) Check the mounted file system is shared or not.
(v) Check all the NFS server and client deamons are running or not.
(vi) Check all the network connections are properly established or not.
(vii) Check whether the NFS service is running or not in server's current run level.
(viii) Check whether the NFS server is running or hung or shutdown.
(ix) Check both NFS server and NFS client systems network routers, network connections and IP addresses.
(x) Check the mount point is correct or not, paths are correct or not and files are there or not.
(xi) Check the NFS shared directory and mount point details are correct or not in /etc/fstab file.
(xii) Check the keytabs are downloaded and stored properly in ***/etc/krb5.keytab*** *file on both NFS server and client.*
(xii) Finally check whether the NFS port no. 2049 is running or not and make sure that the IP tables or firewall should not block the NFS service.

19. NFS server and NFS client configurations are OK, but at client it is not showing anything. How *to resolve?*

(i) The rpcbind may be failed.
(ii) The server is not responding.
(iii) NFS client may be failed at reboot.
(iv) The NFS service is not responding.
(v) The deamons on both systems may not be running.
(vi) Network may be failed on both server and client or any one system.
(vii) May be server and client are not in the same domain or not pinging.
(viii) The server may be in hung or shutdown state.

20. What is Autofs ?

Autofs is service that can automatically mount the shared directory on demand and will automatically unmount the shared directory if it is not accessed within the specified timeout period. The default timeout period is 5 minutes or we can specify the timeout period in /etc/auto.master file.

21. What are the advantages of the Autofs?

(i) Shares are accessed automatically and transparently when a user tries to access any files or directories under the designated mount point of the remote file system to be mounted.
(ii) Booting time is significantly reduced because no mounting is done at boot time.
(iii) Network access and efficiency are improved by reducing the number of permanently active mount points.
(iv) Failed mount requests can be reduced by designating alternate servers as the source of a file system.
(v) Users do not need to have root privilegesto mount or unmount the mount point.
(vi) We can reduce the CPU and memory utilizations because autofs will not mount permanently.
(vii) We can also reduce hard disk utilization because permanent mount points occupies the hard disk space.

22. What are the minimum requirements for Autofs?

(i) autofs package.
(ii) autofs deamon.
(iii) One shared directory.
(iv) One mount point.
(v) Two configuration files are,
(a) /etc/auto.master
(b) /etc/auto.misc

23. How to configure Autofs?

*(i) Install the autofs package by **# yum install autofs* -y** command.*
(ii) Open /etc/auto.master file by # vim /etc/auto.master and at last type as below.
< Client's local mount point> /etc/auto.misc --timeout=60

***Example** :*

/mnt /etc/auto.misc (save and exit this file)
*(* Where timeout=60 means, if the directory is not used for 60 seconds then the shared directory is unmounted automatically. And the default is 5 minutes.)*
(iii) Open /etc/auto.misc file by # vim /etc/auto.misc and types as below.
< Client temporary mount point >-<permissions><IP address or hostname of the server> : <shared name>

***Example** :*

nfs -ro (or) -rw classroom.example.com:/public (save and exit this file)
*(* where -ro means read-only and -rw means read-write)*
(iv) Restart the autofs service in RHEL -6 and RHEL - 7.
 # service autofs restart (restart the autofs service in RHEL - 6)
 # chkconfig autofs on (enable the autofs service at next boot in RHEL - 6)
 # systemctl restart autofs (restart the autofs service in RHEL - 7)
 # systemctl enable autofs (enable the autofs service at next boot in RHEL - 7)
(iv) Goto the Client local mount point which is entered in /et/auto.master file by

 # cd <mount point> command.
Example :
 # cd /mnt
(v) Goto the Client temporary mount point which is entered in /etc/auto.misc file as below.
 # cd /mnt/<temporary mount point>
Example :
 # cd nfs
 # pwd (the output is /mnt/nfs)

24. What is LDAP server?

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.LDAP is lighter because in its initial version it did not include security features.

25. What is LDAP client?

LDAP Client is a network user creation and activity. LDAP user means network user. Network user means login the user through network. If a user wants to login to the remote system, the LDAP user should be created and login to the remote system through LDAP account.
Upto RHEL -5 for this NIS (Network Information System) is used. From RHEL - 6 onwards LDAP is using. The main feature of the LDAP is to share the users information in network.

26. What are the requirements of LDAP and explain it?

(i) Packages.
(a) authconfig-gtk (to configure the LDAP client)
(b) sssd (system security service deamon)
*(ii) LDAP client configuration file is **/etc/ldap.conf***
*(iii) LDAP kerberos configuration file is **/etc/krb5.conf***
(iv) sssd (systems security service deamon) deamon.
(v) LDAP port no. is 389.
(vi) sssd deamon responsibility is retrieving and caching the authentication information.
*(vii) The configuration file of sssd is **/etc/sssd/sssd.conf***
(ix) Through NIS the data is transferred in plain text format.
So, there is no security. But LDAP will transfer the data in encrypted format. So, the data will be in secured way.
(ix) LDAP is used by default sssd ie., kerberos.

27. What are the requirements for LDAP client?

*(i) **dc** (domain controller)*
***Example :** If the domain is example.com then dc=example, dc=com*
*(ii) **ldap server***
***Example :** ldap://classroom.example.com*
*(iii) **Authentication certificate (example-ca.crt)** is located in **http://classroom.example.com/pub** directory.*

28. How to configure the LDAP client?

(i) Create the LDAP user.
(ii) Configure the kerberos.
(iii) configure the NFS automount to share the LDAP user's home directory.
So, LDAP + NFS + sssd is the LDAP system.
* *LDAP is used share the user name and password to remote system.*
* *sssd is used to authenticate in secured communication.*
* *NFS is used to share the user's home directory to remote system.*

Steps :

(i) Install the LDAP + kerberos packages by the following commands.
 # yum groupinstall directory -y (installation in RHEL - 6)*
 # yum install authconfig-gtk sssd* -y (installation in RHEL - 7)*
* *The LDAP packages are different in RHEL - 6 and RHEL - 7 but, the configuration of LDAP is same in both the versions.*
(ii) Create the LDAP users and passwords in the LDAP server.
(iii) Configure the LDAP user's authentication by # system_config_authentication command in Graphical user interface.
(iv) The above command will display the configuration window and in that select and type the option as below.
User Account Database = LDAP
LDAP search base on = dc=example, dc=com
LDAP server = ldap://classroom.example.com/
Enable TLS to encrypt = Click on Download CA Certificate button and then enter the url as, http://classroom.example.com:/pub/example-ca.crt
Authentication Method = LDAP Password (then click on Apply button)
(v) Check whether the LDAP user is configured or not by # getent password ldapuser9 command.

29. How to mount the LDAP user's home directory automatically when demand using Autofs tool?

(i) Install the autofs package by # yum install autofs -y command.*
(ii) Open the /etc/auto.master file by # vim /etc/auto.master command and type as below.
/home/guests /etc/auto.misc (save and exit this file)
(iii) Open the /etc/auto.misc file by # vim /etc/auto.misc command and type as below.
ldapuesr9 -rw classrrom.example.com:/home/guests/ldapuser9 (save and exit this file)
(iv) Restart the autofs services.
 # service autofs restart (restart the autofs service in RHEL - 6)
 # chkconfig autofs on (enable the autofs service at next boot in RHEL - 6)
 # systemctl restart autofs (restart the autofs service in RHEL - 7)
 # systemctl enable autofs (enable the autofs service at next boot in RHEL - 7)
(v) Check whether the LDAP user is able to login or not.
 # su - ldapuser9 (to switch to ldapuser9)
$ pwd (to see the present working directory)
* *The output of the above command is /home/guests/ldapuser9*
$ ls (to see the files in LDAP user's home directory)
$ exit (to exit or logout of the LDAP user)

Chapter#16 – Samba Server

1. What is Samba and explain it?

(i) An open source implementation of the SMB file sharing protocolthat provides file and print services to SMB/CIFS clients. Samba allows a non-Windows server to communicate with the same networking protocol as the Windows products.
(ii) Samba allows Linux computers to share files and printers across a network connection by using SMB protocol. Samba will support DFS, NFS, ufs file systems to share files and directories. That's why Samba is used to share files and directories between different platforms.
(iii) Samba will support printer sharing and it requires authentication.

2. What are the differences between Samba and NFS?

(i) Samba supports to all O/S platforms, whereas NFS will support the same platforms only.
(ii) There is a security in Samba because Samba requires authentication, whereas in NFS there is no security if there is no kerberos because NFS does not requires authentication.
(iii) Samba will support printer sharing, whereas NFS will not support printer sharing.

3. What are the different file systems for sharing different O/S?

(i) Windows --- Windows -----> Distributed File system (DFS)
(ii) Linux --- Linux -----> Network File system (NFS)
(iii) Unix --- Unix -----> Network File system (NFS)
(iv) Apple MAC --- Apple MACs -----> Apple File sharing Protocol (AFP)
(v) Windows --- Linux -----> Common Internet File system (CIFS)

4. What are the requirements or what is the profile of Samba?

(i) Packages : samba for samba server and samba-client* for samba client*
(ii) Deamons : smbd and nmbd for RHEL - 6 where as smbd is for Samba server deamon and nmbd is for Netbios service deamon. smb and nmb for RHEL - 7 where as smb is for Samba server deamon and nmb is for Netbios service deamon.
(iii) Scripting files : /etc/init.d/smb and /etc/init.d/nmb
(iv) Port number : 137 ---> to verify the share name, 138 ---> to data transfer, 139 ---> to connection establish and 445 ---> for authentication
(v) Log file : /var/log/samba
(vi) Configuration : /etc/samba/smb.conf
(vii) File systems : CIFS (Common Internet File system)

5. How to configure the Samba server?

(i) Install the samba package by # yum install samba -y command.*
(ii) Create a samba shared directory by # mkdir /samba command.
(iii) Modify the permissions of the above samba shared directory.

```
# chmod 777 /samba
```

(iv) Modify the SELinux context of the samba directory if SELinux is enabled.

```
# chcon -t samba_share_t /samba
```

(v) Create the samba user and assign the password for the samba user.

 # useradd raju (to create the samba user)

 # smbpasswd -a raju (to assign the samba password for the user raju)

(vi) Assign the ACL permissions (like read, write and execute) to the above shared directory if it is necessary.

 # setfacl -m u : <user name> : rwx <samba shared name>

Example : # setfacl -m u:raju:rwx /samba

(vii) Open the samba configuration file and put an entries of the Samba configuration.

 # vim /etc/samba/smb.conf

Go to last line and copy the last 7 lines and paste them at last. And then modify as below.

[samba] (this is the samba shared name)

comment = public stuff (this is a comment for samba)

path = /samba (share directory name with full path)

public = yes (means no authentication)

= no (means requires authentication)

writable = yes (in read-write mode)

= no (in read only mode)

printable = no (printing is not available)

= yes (printing is available)

write list = raju (to give the write permission to user raju)

= + <group name> (to give the write permission to the group)

valid users = raju, u2 or @group 1, @group 2 (to give the authentication to the users or groups)

hosts allow = IP 1 or IP 2 or host 1 or host2 or <host network ID> or <host network ID> (to share the directory to IP 1 or IP 2 or host 1 or host2)

work group = <windows work group name> (to share the directory to the windows work group)

create mask = 644 (the files created by samba users with 644 permission)

directory mask = 744 or 755 (the directories created by samba users with 744 or 755 permissions)

(save and exit the configuration file)

(viii) Verify the configuration file for syntax errors by # testparm command.

(ix) Restart the samba deamons in RHEL - 6 and RHEL - 7.

 # service smbd nmbd restart (to restart the samba services in RHEL - 6)

 # chkconfig smbd nmbd on (to enable the samba services at next boot in RHEL - 6)

 # systemctl restart smb nmb (to restart the samba services in RHEL - 7)

 # systemctl enable smb nmb (to enable the samba services at next boot in RHEL - 7)

(x) Add the samba service to IP tables and Firewall.

 # setup (then select Firewall configuration option to add the service to IP tables in RHEL - 6)

 # service iptables restart

(to restart the IP tables in RHEL - 6)

 # firewall-cmd --permanent --add-service=samba (to add the samba service to firewall in RHEL - 7)

 # firewall-cmd --complete-reload (to reload the firewall in RHEL - 7)

6. How to access the samba share directory at client side?

(i) Install client side samba packages by ***# yum install samba-client* cifs-utils -y*** *command.*

(ii) Check the samba shared directory names from client side.

 # smbclient -L //<host name or IP address of the server> *(then it will ask password, here don't enter any password because it does not require any password)*

***Example :**# smbclient -L //server9.example.com or 172.25.9.11*

(iii) connect the samba server with user credentials and access the samba shared directory.

***# smbclient //<host name or IP address of the server>/<shared directory name> -U <samba user name>**(Where U is Capital Letter and we have to enter the user's samba password)*

***Example :** # smbclient //server9.example.com/samba -U raju (then smb :/> prompt appears)*
smb:/> ls (to see the contents of the samba shared directory)
smb:/> pwd (to see the present working directory)
smb:/> ! ls (to see the client's local directory contents)
smb:/> get <file name> (to download the specified file from samba server)
smb:/> mget <file 1><file 2><file 3><file4> ... (to download multiple files from samba server)
smb:/> put <file name> (to upload the specified file to the samba server)
smb:/> put <file 1><file 2><file 3><file 4> ... (to upload multiple files to the samba server)
smb:/> exit (to exit from the samba server)

7. How to mount the samba shared directory permanently?

(i) Create the mount point for the samba shared directory.
 # mkdir /mnt/samba
(ii) Put an entry of the mount point details in /etc/fstab file.
 # vim /etc/fstab
//<samba server host name or IP address>/<shared directory name><mount point> cifs defaults , username=<samba user name>, password=<user's samba password> 0 0

Example : //server9.example.com/samba /mnt/samba cifs defaults, username=raju, password=<samba password> 0 0 (save and exit this file)
(iii) Mount all the mount points which are having entries in /etc/fstab file.
 # mount -a
(iv) Check all the mount points by # df -hT command.

8. How to mount the samba shared directory using credential file?

(i) Create one file and put an entries of the user name and password details.
 # vim /root/smbuser
username=raju
password=<user's samba password>
(save and exit the file)
(ii) Open /etc/fstab file and put an entries of the above credential details of user.
 # vim /etc/fstab
//server9.example.com/samba /mnt/samba cifs credentials=/root/smbuser, multiuser, sec=ntlmssp 0 0
(save and exit this file)

9. How to access the samba share directory if it already mounted?

(i) Go to Client system and switch to samba user.

 # su - raju
$ cd /mnt/samba
$ ls (permission denied message will be displayed)
$ cifscreds add <host name or IP address of the samba server>

(to add cifs credentials to the server)
$ ls (to see the contents of the samba shared directory)

10. How to access the samba server from windows system?

(i) Goto Windows system, click on START button, click on Run and type as ***\\172.25.9.11\samba*** *command.*
(ii) Then provide samba user name and password if it prompts us.
(iii) Then see the contents of the samba shared directory.

Other useful commands *:*

 # smbpasswd -a <user name> (to add the samba password to the samba user)
 # smbpasswd -d <user name> (to disable the samba user's password)
 # smbpasswd -e <user name> (to enable the samba user's password)
 # smbpasswd -r <user name> (to remove the samba user's password)
 # smbpasswd -x <user name> (to delete the samba user's password)
 # smbpasswd -n <user name> (to set the samba user's password as null)
 # findsmb (to check how many samba servers are running in our network)
 # pdbedit (to check the available samba users who are accessing currently)
 # smbstatus (to check how many smb clients are connected to the samba server)
 # mount -t cifs //<host name or IP address of the samba server>/<shared direcotory><mount point> -o user=<user name>
(to mount the samba share directory on local mount point temporarily)

Example *: # mount -t cifs //172.25.9.11/samba /mnt/samba -o user=raju*

Chapter#17 – NTP (Netwotk Time Protocal)

1. What is NTP and Chrony?

NTP stands for Network Time Protocol in RHEL - 6 and Chrony is also a Network Time Protocol in RHEL - 7.These are used to synchronize the time on your Linux system with a centralized NTP or Chrony server.A local NTP or Chrony server on the network can be synchronized with an external timing source to keep all the servers in your organization in-sync with an accurate time.

2. What are the differences between NTP and Chrony?

NTP	Chrony
This is used in RHEL - 6.	This is used in RHEL - 7.
Package is ntp or system-config-date.	Package is chrony.
It's deamon is ntpd and Port number is 123.	It's deamon is chronyd and Port number is 123.
We have to install the package manually.	By default this package is installed.
# ntpq -p (to check ntp is configured or not).	# chronyc sources -v (to check chrony is configured or not).
Configuration file is /etc/ntp.conf	Configuration file is /etc/chrony.conf
Log file is /var/log/ntpstat	Log file is /var/log/chrony

3. How to configure the NTP and Chrony client?

NTP :

(i) Install the ntp package by # yum install ntp -y or # yum install system-config-date* -y command.*

(ii) open the configuration file by

 # system-config-date or

 # vim /etc/ntp.conf command.

(# system-config-date command is used to configure the NTP in graphical mode)

** Make a comment on line numbers 21, 22 and 23. Then go to line number 24 and type as below.*

server <ntp server host name> (save and exit this file)

Example : server classroom.example.com

(iii) Restart the ntpd service by # service ntpd restart command.

(iv) Enable the ntp service at next boot by # chkconfig ntpd on command.

(v) Check whether the NTP is configured or not by # ntpq -p command.

Chrony :

(i) Chrony package is not installed because by default it is installed. If it not installed then install the package by # yum install chrony -y command.*

(ii) Open the chrony configuration file by # vim /etc/chrony.conf command.

** Make a comment on line numbers 3, 4 and 5. Then go to line number 6 and type as below.*

server <ntp server host name> iburst
(save and exit this file)

Example : server classroom.example.com iburst

(iii) Restart the chrony service by
 # systemctl restart chronyd command.

(iv) Enable the chrony service at next boot by # systemctl enable chronyd command.
(v) Check whether the Chrony is configured or not by # chronyc sources -v command.
 # timedatectl
(to check whether the client's time is synchronized to the server's time)
 # timedatectl list-timezones (to list the different time zones)
 # timedatectl set-time <hh : mm : ss> (to set the time)
 # timedatectl set-timezone Asia/Kolkata
(to set the time zone in RHEL - 7)
 # tzselect Asia/Kolkata (to set the time zone in RHEL - 6)

Chapter#18 – DNS (Domain Naming System)

1. What is DNS?

*DNS stands for Domain Naming System. The **DNS**translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.*

DNS implements a distributed database to store this name and address information for all public hosts on the Internet. DNS assumes IP addresses do not change (are statically assigned rather than dynamically assigned).

2. What is DNS server and how it works?

In any network, the hosts primarily communicate between each other through IP addresses. For example, if my computer is doing a google search, my computer is actually communicating with the IP address of one of the web servers of google.com. However, even if the computer is efficient with numbers, humans on the other hand work better with names. For this reason, the TCP/IP protocol includes the Domain Name System (DNS) to link between IPs and computer names i.e. hostnames. The DNS is a distributed database of computers that is responsible for resolving hostnames against IP addresses and vice-versa.

Any DNS query involves two parts.

(i) The Resolver: The resolver forms up or initiates the query. The resolver itself does not run as a program. /etc/resolve.conf is an example of a resolver.

(ii) Name Server: The Name Server is the service running in the server that responds to the DNS query generated by the resolver i.e. answers to the question of the resolver.

The working DNS :

(i) The client initiates a query to find a domain example.com. The client sends the query to the DNS server of the ISP. (The DNS Server IP in the client computer is set as the IP address of the DNS Server of the ISP)

(ii) The DNS Server of the ISP first checks it's own cache to check whether it already knows the answer. But as the answer is not present, it generates another query. As the Top Level Domain of example.com is .com, so the DNS server queries the Internet Registration Authority to find who is responsible for example.com.

(iii) The Internet Registration Authority responds to the ISP by answering the query.

(iv) Once the ISP DNS Server knows the authoritative name servers, it contacts the authoritative name servers to find out the IP address for www.example.com i.e. the IP address of host www in the domain example.com.

(v) example.com responds to the ISP DNS Server by answering the query and providing the IP address of the web server i.e. www

(vi) The ISP DNS Server stores the answer in it's cache for future use and answers to the client by sending the IP address of the www server.

(vii) The client may store the answer to the DNS query in it's own cache for future use. Then the client communicates directly with the www server of domain example.com using the IP address.

(viii) The www server responds by sending the index.html page.

3. What is the format of the domain name?

Like a physical address, internet domain names are hierarchical way. If the Fully Qualified Domain Name is www.google.co.in , the www is the Hostname, google is the Domain, co is the Second Level Domain and in is the Top Level Domain.

4. What are the files we have to edit to configure the DNS?

There are four files to edit to configure the DNS. They are /etc/named.conf, /etc/named.rfc1912.zones, Forward Lookup Zoneand Reverse Lookup Zone. DNS provides a centralised database for resolution. Zone is storage databasewhich contains all the records.
Forward Lookup Zone is used to resolveHostnames to IP addresses.
Reverse Lookup Zone is used to resolve IP addresses to Hostnames.

5. What are the DNS record and explain them?

(i) SOA Record : (Start of Authority)
SOA contains the general administration and control information about the domain.
(ii) Host A Record :
(a) It is nothing but aForward Lookup Zone.
(b) It maps Hostname to IP address.
(iii) PTR : (Pointer Record)
(a) It is nothing but a Reverse Lookup Zone.
(b) It maps IP address to Hostname.
(iv) NS Record : (Name Server Record)
It stores the DNS server IP addresses.
(v) MX Record : (Mail Exchange Record)
It stores the records of the Mail Server IP address.
(vi) CNME Record :
It is nothing but Host's Canonical name allows additional names or aliases to be used locate a system.

6. What is the profile of the DNS?

Package	*:*	*bind and caching-name*
Script	*:*	*/etc/init.d/named*
Configuration file	*:*	*/etc/named.conf and /etc/named.rfc1912.zones*
Client's configuration file	*:*	*/etc/resolve.conf*
Document root	*:*	*/var/named/*
Log file	*:*	*/var/log/messages*
Deamon	*:*	*named*
Port number	*:*	*53*

7. How to configure the DNS server?

(i) Install the packages bind, caching-name for RHEL- 6 &bind, cashing-name and unbound for RHE - 7.
 # yum install bind caching-name* -y (to install the DNS packages for RHEL - 6)*
 # yum install bind caching-name* unbound* -y (to install the DNS packages for RHEL - 7)*
(ii) Change the hostname by adding fully qualified domain name and make it permanent.
 # hostname <fully qualified domain name> (to change the hostname in RHEL - 6)
 # hostname server9.example.com (example for setting hostname temporarily in RHEL - 6)
 # hostnamectl set <fully qualified domain name> (to change the hostname in RHEL - 7)

 # hostnamectl set server9.example.com (example for setting hostname temporarily in RHEL - 7)
 # vim /etc/hosts (open this file and go to last line and type as below in RHEL - 6 only)
<IP address> <fully qualified domain name> <hostname>
172.25.9.11 server9.example.com server9 (for example of the above syntax)
 # vim /etc/sysconfig/network
(open this file and go to last line and type as below in RHEL - 6 only)
HOSTNAME=<fully qualified domain name>
HOSTNAME=server9.example.com (for example of the above syntax)

(ii) Open the DNS main configuration file by # vim /etc/named.conf command.
** Go to line number 11 and edit this line as below.*
listen-on port 53 { 127.0.0.1; <server IP address>; };
Example : listen-on port 53 {127.0.0.1; 172.25.9.11; };
** Go to line number 17 and edit this line as below.*
allow-query { localhost; <Network ID>/<netmask>; };
Example : allow-query {localhost; 172.25.9.0/24; };
(save and exit this file)

(iii) Open the DNS zone reference file by # vim /etc/named.rfc1912.zones command
** Go to line number 19 and copy 5 lines and paste them at last of the file.*

```
zone "<domain name>" IN {
        type-master;
        file "<forward lookup zone file name>";
        allow-update { none; };
};
```

Example :

```
zone "example.com" IN {
        type-master;
        file "named.forward";
        allow-update { none; };
};
```

** Go to line number 31 and copy 5 lines and paste them at last of the file.*

```
zone "<Three octets of the DNS server IP address> . in . addr . arpa" IN {
        type-master;
        file "<reverse lookup zone file name>";
        allow-update { none; };
};
```

Example :

```
zone "9.25.172 . in . addr . arpa" IN {
        type-master;
        file "named.reverse";
        allow-update { none; };
};
```

(save and exit this file)

(iv) Copy /var/named/named.localhost file to /var/named/named.forward and edit as follows.
 # cp -p /var/named/named.localhost /var/named/named.forward
 # vim /var/named/named.forward
** Go to line number 2 and edit as follows.*

```
@ IN SOA <DNS server fully qualified domain name> . com root . <domain name> .
{
```

* Go to line number 8 and edit as follows.

NS <DNS server fully qualified domain name> .
A <DNS server IP address>

<DNS server fully qualified domain name> IN A <DNS server IP address>
<Client 1 fully qualified domain name> IN A <Client 1 IP address>
<Client 2 fully qualified domain name> IN A <Client 2 IP address>
<Client 3 fully qualified domain name> IN A <Client 3 IP address>
www IN CNAME<DNS server fully qualified domain name>

Example : The line number 2 should be edited as follows.

@ IN SOA server9.example.com. root.example.com. {
The line number 8 should be edited as follows.

NS server9.example.com.
A 172.25.9.11

server9.example.com. IN A 172.25.9.11
client9.example.com. IN A 172.25.9.10
client10.example.com. IN A 172.25.9.12
client11.example.com. IN A 172.25.9.13
www IN CNAME server9.example.com.
(save and exit this file)

(v) Copy /var/named/named.empty file to /var/named/named.reverse and edit as follows.

cp -p /var/named/named.empty /var/named/named.reverse
vim /var/named/named.reverse

* Go to line number 2 and edit as follows.

@ IN SOA <DNS server fully qualified domain name> . com root . <domain name> .
{

* Go to line number 8 and edit as follows.

NS <DNS server fully qualified domain name> .

<Last octet of the DNS server IP address> IN PTR <DNS server fully qualified domain name>
<Last octet of the Client 1 IP address> IN PTR <Client 1 fully qualified domain name>
<Last octet of the Client 2 IP address> IN PTR <Client 2 fully qualified domain name>
<Last octet of the Client 3 IP address> IN PTR <Client 3 fully qualified domain name>
<DNS server fully qualified domain name> IN A <DNS server IP address>
www IN CNAME<DNS server fully qualified domain name>

Example : The line number 2 should be edited as follows.

@ IN SOA server9.example.com. root.example.com. {
The line number 8 should be edited as follows.

NS server9.example.com.
11 IN PTR server9.example.com.
10 IN PTR client9.example.com.
12 IN PTR client10.example.com.
13 IN PTR client11.example.com.
server9.example.com. IN A 172.25.9.11
www IN CNAME server9.example.com. (save and exit this file)

(vi) Check the DNS configuration files for syntax errors.

 # named-checkconf /etc/named.conf

 # named-checkconf /etc/named.rfc1912.zones

 # name-checkzone <domain name><forward lookup zone>

Example : # named-checkzone example.com /var/named/named.forward

 # named-checkzone <domain name><reverse lookup zone>

Example : # named-checkzone example.com /var/named/named.reverse

(vii) Give full permissions to the forward and reverse lookup zones.

 # chmod 777 /var/named/named.forward

 # chmod 777 /var/named/named.reverse

(viii) Open /etc/sysconfig/network-scripts/ifcfg-eth0 and enter the DNS domain details if not present.

 # vim /etc/sysconfig/network-scripts/ifcfg-eth0 (go to last line and type as follows)

DNS 1=example.com

(save and exit this file)

(ix) Add the DNS server IP address in /etc/resolve.conf

 # vim /etc/resolve.conf

search <domain name>

namesever <IP address of the DNS server>

Example :

search example.com

nameserver 172.25.9.11

(save and exit this file)

(x) Restart the DNS server deamons.

 # service named restart (to restart the deamon in RHEL - 6)

 # chkconfig named on (to enable the deamon at next boot time in RHEL - 6)

 # systemctl restart named unbound (to restart the deamons in RHEL - 7)

 # systemctl enable named unbound (to enable the deamons at next boot time in RHEL -7)

(xi) Add the DNS service to the IP tables and Firewall.

 # setup (then select the Firewall configuration option and add DNS in RHEL - 6)

 # service iptables restart (to restart the IP tables in RHEL - 6)

 # service iptables save (to save the IP tables in RHEL - 6)

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

(to add the DNS service to firewall in RHEL - 7)

 # firewall-cmd --complete-reload (to reload the firewall in RHEL - 7)

(xi) Check whether the DNS is resolving or not.

 # dig <DNS server fully qualified name>

(to check the resolving from hostname to IP address)

 # dig -x <DNS server IP address> (to check the resolving from IP address to hostname)

Example : # dig server9.example.com

 # dig -x 172.25.9.11

(xii) Check the resolution with ping test.

 # ping -c3 <DNS server fully qualified domain name>

(to check the ping test with hostname)

 # ping -c3 <IP address of the DNS server> (to check the ping test with IP address)

Example :

 # ping -c3 server9.example.com

 # ping -c3 172.25.9.11

(xiii) Check the resolution with host command.

 # host <hostname> (to check the resolution with hostname)

 # host <IP address> (to check the resolution with IP address)

Example :

 # host server9.example.com

 # host 172.25.9.11

(xiv) Check the resolution with nslookup command.

 # nslookup <hostname> (to check the resolution with hostname)

 # nslookup <IP address> (to check the resolution with IP address)

Example :

 # nslookup server9.example.com

 # nslookup 172.25.9.11

8. How to configure the DNS client?

(i) First assign the static IP address to the client.

(ii) Set the hostname to the client.

(iii) Restart the network service by ***#service network restart*** *command.*

(iv) Open /etc/resolve.conf file and edit as below.

 # vim /etc/resolve.conf

search <domain name>

nameserver <DNS server IP address>

Example :

search example.com

nameserver 172.25.9.11 (save and exit this file)

(v) Check whether the DNS is resolving or not.

 # dig <DNS server fully qualified name> (to check the resolving from hostname to IP address)

 # dig -x <DNS server IP address> (to check the resolving from IP address to hostname)

Example : *# dig server9.example.com*

 # dig -x 172.25.9.11

 # dig client9.example.com

 # dig -x 172.25.9.10

(vi) Check the resolution with ping test.

 # ping -c3 <DNS client fully qualified domain name> (to check the ping test with hostname)

 # ping -c3 <IP address of the DNS server> (to check the ping test with IP address)

Example :

 # ping -c3 client9.example.com

 # ping -c3 172.25.9.10

 # ping -c3 server9.example.com

 # ping -c3 172.25.9.11

(vii) Check the resolution with host command.

 # host <hostname> (to check the resolution with hostname)

 # host <IP address> (to check the resolution with IP address)

Example :

 # host server9.example.com
 # host 172.25.9.11
 # host client9.example.com
 # host 172.25.9.10

(viii) Check the resolution with nslookup command.

 # nslookup <hostname> (to check the resolution with hostname)
 # nslookup <IP address> (to check the resolution with IP address)

Example :

 # nslookup server9.example.com
 # nslookup 172.25.9.11
 # nslookup client9.example.com
 # nslookup 172.25.9.10

9. How to configure the Secondary DNS server?

(i) Install the packages bind, caching-name for RHEL - 6 &bind, cashing-name and unbound for RHEL - 7.

 # yum install bind caching-name* -y (to install the DNS packages for RHEL - 6)*
 # yum install bind caching-name* unbound* -y (to install the DNS packages for RHEL - 7)*
(ii) Change the hostname by adding fully qualified domain name and make it permanent.
 # hostname <fully qualified domain name> (to change the hostname in RHEL - 6)
 # hostname server6.example.com (example for setting hostname temporarily in RHEL - 6)
 # hostnamectl set <fully qualified domain name> (to change the hostname in RHEL - 7)
 # hostnamectl set server6.example.com (example for setting hostname temporarily in RHEL - 7)
 # vim /etc/hosts (open this file and go to last line and type as below in RHEL - 6 only)
<IP address> <fully qualified domain name> <hostname>
172.25.6.11 server6.example.com server6 (for example of the above syntax)
 # vim /etc/sysconfig/network (open this file and go to last line and type as below in RHEL - 6 only)
HOSTNAME=<fully qualified domain name>
HOSTNAME=server6.example.com (for example of the above syntax)

(ii) Open the DNS main configuration file by # vim /etc/named.conf command.
** Go to line number 11 and edit this line as below.*
listen-on port 53 { 127.0.0.1; <server IP address>; };
Example : listen-on port 53 {127.0.0.1; 172.25.6.11; };
** Go to line number 17 and edit this line as below.*
allow-query { localhost; <Network ID>/<netmask>; };
Example : allow-query {localhost; 172.25.6.0/24; };
(save and exit this file)

(iii) Open the DNS zone reference file by # vim /etc/named.rfc1912.zones command
** Go to line number 19 and copy 5 lines and paste them at last of the file.*

```
zone "<domain name>" IN {
        type-slave;
        file "slaves/<forward lookup zone file name>";
        master { <Primary DNS server IP address; };
```

};
Example : zone "example.com" IN {
type-slave;
file "slaves/named.forward";
master { 172.25.9.11; };
};
* Go to line number 31 and copy 5 lines and paste them at last of the file.
zone "<Three octets of the DNS server IP address> . in . addr . arpa" IN {
type-slave;
file "slaves/<reverse lookup zone file name>";
master { <Primary DNS server IP address; };
};
Example : zone "9.25.172 . in . addr . arpa" IN {
type-slave;
file "slaves/named.reverse";
master { 172.25.9.11; };
};
(save and exit this file)

(iv) Copy /var/named/slaves/named.localhost to /var/named/slaves/named.forward and edit as follows.

mkdir /var/named/slaves
cp -p /var/named/slaves/named.localhost /var/named/slaves/named.forward
vim /var/named/slaves/named.forward
* Go to line number 2 and edit as follows.

@IN SOA <secondary DNS server fully qualified domain name> . com root . <domain name> . {

* Go to line number 8 and edit as follows.
NS <DNS server fully qualified domain name> .
A <DNS server IP address>

<secondary DNS server fully qualified domain name> IN A <secondary DNS server IP address>
<DNS server fully qualified domain name> IN A <DNS server IP address>
<Client 1 fully qualified domain name> IN A <Client 1 IP address>
<Client 2 fully qualified domain name> IN A <Client 2 IP address>
<Client 3 fully qualified domain name> IN A <Client 3 IP address>
www IN CNAME<DNS server fully qualified domain name>
Example : The line number 2 should be edited as follows.
@ IN SOA server6.example.com. root.example.com. {
The line number 8 should be edited as follows.
NS server6.example.com.
A 172.25.6.11
server6.example.com. IN A 172.25.6.11
server9.example.com. IN A 172.25.9.11

client9.example.com. IN A 172.25.9.10

client10.example.com. IN A 172.25.9.12
client11.example.com. IN A 172.25.9.13
www IN CNAME server6.example.com. (save and exit this file)

(v) Copy /var/named/slaves/named.empty file to /var/named/slaves/named.reverse and edit as follows.

cp -p /var/named/slaves/named.empty /var/named/slaves/named.reverse
vim /var/named/slaves/named.reverse
* Go to line number 2 and edit as follows.
@ IN SOA <secondary DNS server fully qualified domain name> . com root . <domain name> . {
* Go to line number 8 and edit as follows.
NS <secondary DNS server fully qualified domain name> .
<Last octet of the secondary DNS server IP address> IN PTR <secondary DNS server fully qualified domain name>
<Last octet of the DNS server IP address> IN PTR <DNS server fully qualified domain name>
<Last octet of the Client 1 IP address> IN PTR <Client 1 fully qualified domain name>
<Last octet of the Client 2 IP address> IN PTR <Client 2 fully qualified domain name>
<Last octet of the Client 3 IP address> IN PTR <Client 3 fully qualified domain name>
<secondary DNS server fully qualified domain name> IN A <secondary DNS server IP address>
www IN CNAME<secondary DNS server fully qualified domain name>

Example : The line number 2 should be edited as follows.
@ IN SOA server6.example.com. root.example.com. {
The line number 8 should be edited as follows.
NS server6.example.com.
11 IN PTR server6.example.com.
11 IN PTR server9.example.com.
10 IN PTR client9.example.com.
12 IN PTR client10.example.com.
13 IN PTR client11.example.com.
server6.example.com. IN A 172.25.6.11
www IN CNAME server6.example.com. (save and exit this file)

(vi) Check the DNS configuration files for syntax errors.

named-checkconf /etc/named.conf
named-checkconf /etc/named.rfc1912.zones
name-checkzone <domain name><forward lookup zone>
Example : # named-checkzone example.com /var/named/slaves/named.forward
named-checkzone <domain name><reverse lookup zone>
Example : # named-checkzone example.com /var/named/slaves/named.reverse

(vii) Give full permissions to the forward and reverse lookup zones.

chmod 777 /var/named/slaves/named.forward
chmod 777 /var/named/slaves/named.reverse

(viii) Open /etc/sysconfig/network-scripts/ifcfg-eth0 and enter the DNS domain details if not present.

vim /etc/sysconfig/network-scripts/ifcfg-eth0 (go to last line and type as follows)

DNS 1=example.com (save and exit this file)

(ix) Add the DNS server IP address in /etc/resolve.conf

vim /etc/resolve.conf
search <domain name>
namesever <IP address of the DNS server>
namesever <IP address of the secondary DNS server>

Example :
search example.com
nameserver 172.25.9.11
nameserver 172.25.6.11 (save and exit this file)

(x) Restart the DNS server deamons.

service named restart (to restart the deamon in RHEL - 6)
chkconfig named on (to enable the deamon at next boot time in RHEL - 6)
systemctl restart named unbound (to restart the deamons in RHEL - 7)
systemctl enable named unbound (to enable the deamons at next boot time in RHEL -7)

(xi) Add the DNS service to the IP tables and Firewall.

setup (then select the Firewall configuration option and add DNS in RHEL - 6)
service iptables restart (to restart the IP tables in RHEL - 6)
service iptables save (to save the IP tables in RHEL - 6)
firewall-cmd --permanent --add-service=dns
(to add the DNS service to firewall in RHEL - 7)
firewall-cmd --complete-reload (to reload the firewall in RHEL - 7)

(xi) Check whether the DNS is resolving or not.

dig <DNS server fully qualified name> (to check the resolving from hostname to IP address)
dig -x <DNS server IP address> (to check the resolving from IP address to hostname)

Example : # dig server6.example.com
dig -x 172.25.6.11

(xii) Check the resolution with ping test.

ping -c3 <secondary DNS server fully qualified domain name>(to check the ping test with hostname)
ping -c3 <IP address of the secondary DNS server> (to check the ping test with IP address)

Example :
ping -c3 server6.example.com
ping -c3 172.25.6.11

(xiii) Check the resolution with host command.

host <hostname> (to check the resolution with hostname)
host <IP address> (to check the resolution with IP address)

Example :
host server6.example.com
host 172.25.6.11

(xiii) Check the resolution with nslookup command.

nslookup <hostname> (to check the resolution with hostname)
nslookup <IP address> (to check the resolution with IP address)

Example :
nslookup server6.example.com
nslookup 172.25.6.11

Chapter#19 – DHCP (Dynamic Host Configuration Protocal)

1. What is DHCP and explain it?

DHCP stands for Dynamic Host Configuration Protocol. DHCP is a network protocol that enables the server to assign an IP addresses to the clients in the network automatically from a defined range of IP addresses ie., scope configured for a given network. DHCP allows a computer to join in an IP-based network without having a pre-configured IP address. DHCP is a protocol that assign unique IP addresses to devices, then releases and renews those addresses as devices leave and rejoin in the network. Internet Service Providers (ISPs) usually use DHCP to help customers join their networks with minimum setup effort required. Likewise, home network equipment like broadband routers offers DHCP support to joining home computers to Local Area Networks (LANs). In simple terms DHCP is used to assign the IP addresses to the remote hosts automatically. First client requests to the DHCP server, then DHCP server accepts the client's request and assign the next available IP address to the requested DHCP client.

2. How the DHCP works?

The process of requesting the IP address from the DHCP clients and assign the IP address by the DHCP server is called "D O R A".

(i) When we switch on the system with DHCP client, the client system sends the broadcast request looking for a DHCP server to answer. This process is called DISCOVER or DHCP DISCOVER.

(ii) The router directs the DISCOVER packet to the correct DHCP server.

(iii) The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER orDHCP OFFER packet with that address information. The server also configures the client's DNS servers, WINS servers, NTP serves and sometimes other services also.

(iv) Then the Client sends a REQUEST or DHCP REQUEST packet, letting the server know that it intends to use the address.

(v) Then the server sends an ACK or DHCP ACK packet, conforming that the client has been given a lease on the address for a server specified period of time.

3. What is the disadvantage to assign the Static IP address?

When a system uses a static IP address, It means that the system is manually configured to use a specific IP address. One problem with static assignment,which can result from user error or inattention to detail, occurs when two systems are configured with the same IP address. This creates a conflict that results in loss of service. Using DHCP to dynamically assign IP addresses to avoid these conflicts.

4. What is the profile of DHCP?

Package	*:*	*dhcp**
Script file	*:*	*/etc/init.d/dhcpd*
Configuration file	*:*	*/etc/dhcp/dhcpd.conf*
Deamon	*:*	*dhcpd*
Port numbers	*:*	*67 (dhcp server) and 68 (dhcp client)*
Log messages	*:*	*/var/log/messages*

5. How to configure the DHCP server?

(i) Assign a static IP address to the DHCP server.

(ii) Install the DHCP package by # yum install dhcp -y command.*

(iii) Open the DHCP configuration file by # vim /etc/dhcp/dhcpd.conf command. This file is empty and we have to copy the sample file from /usr/share/doc/dhcp-4.25/dhcpd.conf.example to the above location by # cp -p /usr/share/doc/dhcp-4.25/dhcpd.conf.example /etc/dhcp/dhcpd.conf

(iv) Now open the above DHCP configuration file by # vim /etc/dhcp/dhcpd.conf command.

** Go to line number 47 and edit that line as below.*

```
subnet <DHCP server Network ID> netmask <subnetmask of the this network> {
        range <starting IP address><ending IP address>;
default-lease-time 600;                 (the minimum lease time to the client in seconds)
max-lease-time 7200;                    (he maximum lease time to the client in seconds)
}
```

Example :

```
subnet 172.25.0.0 netmask 255.255.255.0 {
        range 172.25.9.50 172.25.9.100;
        default-lease-time 600;
        max-lease-time 7200;
}
```

** Go to line number 51 and edit that as below.*

```
option routes <DHCP server IP address>;
option broadcast-address <DHCP server broadcast address>;
```

Example :

```
option routes 172.25.9.11;
option broadcast-address 172.25.9.255;
                (save and exit this file)
```

(v) Restart the DHCP services in RHEL - 6 and RHEL - 7.

```
# service dhcpd restart                 (to restart the DHCP service in RHEL - 6)
# chkconfig dhcpd on                    (to enable the DHCP service at next boot in RHEL - 6)
# systemctl restart dhcpd               (to restart the DHCP service in RHEL - 7)
# systemctl enable dhcpd                (to enable the DHCP service at next boot in RHEL - 7)
```

(vi) Add the DHCP service to the IP tables and Firewall.

In RHEL - 6:

```
# iptables -A INPUT -p udp -i eth0 --deport 67 -j ACCEPT
# iptables -A INPUT -p tcp -i eth0 --deport 67 -j ACCEPT
# iptables -A INPUT -p udp -i eth0 --deport 68 -j ACCEPT
# iptables -A INPUT -p tcp -i eth0 --deport 68 -j ACCEPT
# iptables -A OUTPUT -p udp -i eth0 --deport 67 -j ACCEPT
# iptables -A OUTPUT -p tcp -i eth0 --deport 67 -j ACCEPT
# iptables -A OUTPUT -p udp -i eth0 --deport 68 -j ACCEPT
# iptables -A OUTPUT -p tcp -i eth0 --deport 68 -j ACCEPT
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=dhcp
# firewall-cmd --complete-reload
```

(vii) # cat /var/lib/dhcpd/dhcpd.lease (to see the DHCP lease message database on DHCP server)

6. How to configure the DHCP client?

(i) Change the IP addressing from static to dynamic if it is configured as static.

In RHEL - 6 :

 # setup

Network Configuration -----> Press Enter -----> Device Configuration -----> Select eth0 -----> Press Enter ----> Select Use DHCP -----> Press Spacebar -----> OK -----> Save ----->Save & Quit -----> Quit

 # service NetworkManager restart

 # service network restart

In RHEL - 7:

 # nmcli connection modify "System eth0" ipv4.method auto or dynamic

 # nmcli connection down "System eth0"

 # nmcli connection up "System eth0"

 # systemctl restart network

(ii) Open /etc/sysconfig/network-scripts/ifcfg-eth0 file and edit the BOOTPROTO line.

 # vim /etc/sysconfig/network-scripts/ifcfg-eth0

** Go to BOOTPROTO line and edit that line as below.*

BOOTPROTO=dhcp (save and exit this file)

(iii) Get the IP address from the DHCP server.

 # dhclient

 # ifdown eth0

 # ifup eth0

7. How to fix the IP address to the client every time it requests or how to configure the MAC *binding?*

*The process of assigning the same IP address (fixed IP address) to the DHCP client every time it booted is called **"MAC binding"**.*

*(i) Open the file /etc/dhcp/dhcpd.conf by **# vim /etc/dhcp/dhcpd.conf** command.*

** Go to line number 76 and 77 and edit those lines as below.*

```
host <dhcp client hostname> {
        hardware ethernet    <MAC address of the Client's NIC card>;
        fixed addresses      <IP address>;
}
```

Example :

```
host client 1 {
        hardware ethernet 2015:ac18::55;
        fixed addresses 172.25.9.150;
}
```

(save and exit this file)

(ii) Restart the DHCP services in RHEL - 6 and RHEL - 7.

 # service dhcpd restart (to restart the DHCP service in RHEL - 6)

 # chkconfig dhcpd on (to enable the DHCP service at next boot in RHEL - 6)

 # systemctl restart dhcpd (to restart the DHCP service in RHEL - 7)

 # systemctl enable dhcpd (to enable the DHCP service at next boot in RHEL - 7)

** Then the above MAC address of the system will get the same IP address every time it booted.*

Chapter#20 – Web Server Configuration(Apache)

1. What is Web server and explain it?

A Web server is a system that delivers content or services to end users over the Internet. A Web server consists of a physical server, server operating system (OS) and software used to facilitate HTTP communication. A computer that runs a Web site. Using the HTTP protocol, the Web server delivers Web pages to browsers as well as other data files to Web-based applications. The Web server includes the hardware, operating system, Web server software, TCP/IP protocols and site content (Web pages, images and other files). If the Web server is used internally and is not exposed to the public, it is an "intranet server" and if the Web server is used in the internet and is exposed to the public, it is an Internet server.

2. What is Protocol?

A uniform set of rules that enable two devices to connect and transmit the data to one another. Protocols determine how data are transmitted between computing devices and over networks. They define issues such as error control and data compression methods. The protocol determines the following type of error checking to be used, data compression method (if any), how the sending device will indicate that it has finished a message and how the receiving device will indicate that it has received the message. Internet protocols include TCP/IP (Transmission Control Protocol / Internet Protocol), HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol).

3. How a Web server works?

(i) If the user types an URL in his browsers address bar, the browser will splits that URL into a number of separate parts including address, path name and protocol.
(ii) A DNS (Domain Naming Server) translates the domain name the user has entered into its IP address, a numeric combination that represents the site's true address on the internet.
(iii) The browser now determines which protocol (rules and regulation which the client machine used to communicate with servers) should be used. For example FTP (File Transfer Protocol) and HTTP (Hyper Text Transfer Protocol).
(iv) The server sends a GET request to the Web Server to retrieve the address it has been given. For example when a user types http://www.example.com/Myphoto.jpg , the browser sends a GET Myphoto.jpg command to example.com server and waits for a response. The server now responds to the browser's requests. It verifies that the given address exist, finds the necessary files, runs the appropriate scripts, exchanges cookies if necessary and returns the results back to the browser. If it cannot locate the file, the server sends an error message to the client.
(v)Then the browser translates the data it has been given into HTML and displays the results to the user.

4. In how many ways can we host the websites?

IP based Web Hosting : IP based web hosting is usedIP address or hostname web hosting.
Name based Web Hosting : Hosting the multiple websites using single IP address. Port based Web Hosting : Web hosting using another port number ie., other than the default port number.
User based Web Hosting : We can host the Web sites using the user name and password.

5. What is Apache Web Server?

Apache is a open source web server. It is mostly used web server in the internet. httpd is the deamon that speaks the http or https protocols. It is a text based protocol for sending and receiving the objects over a network connection. The http protocol is sent over the wired network in clear text using default port number 80/tcp. To protect the website we can use https web server for data encryption.

6. What is the profile for Web server?

Package : httpd
script : /etc/init.d/httpd
Deamon : httpd
Configuration file: /etc/httpd/conf/httpd.conf (for http)
/etc/httpd/conf.d/ssl.conf (for https)
Document Root : /var/www/html
Log files : /var/log/httpd/access_log
/var/log/httpd/error_log
Port Number : 80/http and 443/https

** If we want to configure the httpd server, we have to follow the ISET rules. where I - Install, S - Start,*
E - Enable and T - Test.
** To access the websites using the CLI mode e-links, curl tools are used and to access the websites using the browser in Linux Firefox is used.*

7. How to make the http web server available to the cleint?

(a) First assign the static IP address and hostname to the server.
(b) Check whether the server package by # rpm -qa httpd command.*
(c) If not installed, install the web server package by # yum install httpd -y command.*
(d) Start the web server and enable web server service at next boot.
 # service httpd start (to start the webserver deamon in RHEL - 6)
 # chkconfig httpd on (to enable the service at next boot in RHEL - 6)
 # systemctl restart httpd (to start the webserver deamon in RHEL - 7)
 # systemctl enable httpd (to enable the service at next boot in RHEL - 7)
(e) Open the browser and access the web server document.
 # firefox (to open the firefox browser)
** Then in address bar type as http://localhost/manual and press Enter key.*

8. How to configure the IP based virtual host Web server?

(a) First assign the static IP address and hostname to the server.
(b) Check whether the server package by # rpm -qa httpd command.*
(c) If not installed, install the web server package by # yum install httpd -y command.*
(d) Check the configuration file to configure the http web server by # rpm -qac httpd command.
(e) If required open the web server document by # rpm -qad httpd command.
(f) Go to the configuration file directory by # cd /etc/httpd/conf.d
(g) Create the configuration for IP based hosting.
 # vim /etc/httpd/conf.d/ip.conf
<VirtualHost <IP address of the web server> : 80>

ServerAdmin root@<hostname of the web server>
ServerName <hostname of the web server>
DocumentRoot /var/www/html
</VirtualHost>

<Directory "/var/www/html">
AllowOverride none
Require All Granted
</Directory> (save and exit this file)

Example :

vim /etc/httpd/conf.d/ip.conf (create the configuration file)

<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
</VirtualHost>

<Directory "/var/www/html">
AllowOverride none
Require All Granted
</Directory>

(h) Go to document root directory and create the index.html file.

cd /var/www/html
vim index.html

<html>
<H1>
This is IP based Web Hosting
</H1>
</html> (save and exit this file)

(i) Restart the web server deamon.

service httpd start (to start the webserver deamon in RHEL - 6)
chkconfig httpd on (to enable the service at next boot in RHEL - 6)
systemctl restart httpd (to start the webserver deamon in RHEL - 7)
systemctl enable httpd (to enable the service at next boot in RHEL - 7)

(j) Add the service to the IP tables and firewall.

In RHEL - 6 :

iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
service iptables save
service iptables restart

In RHEL - 7 :

firewall-cmd --permanent --add-service=http
firewall-cmd --complete-reload

(k) Go to client system, open the firefox browser and type as http://server9.example.com in address bar and check the index page is displayed or not.

(l) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y                    (install the elinks package)
# elinks --dump server9.example.com         (access the index page)
```

9. How to configure the name based web hosting?

(a) Make a directory for virtual or named based hosting.

```
# mkdir /var/www/virtual
```

(b) Go to the configuration file directory by # cd /etc/httpd/conf.d

(c) Create the configuration for name based hosting.

```
# vim /etc/httpd/conf.d/virtual.conf
<VirtualHost <IP address of the web server> : 80>
ServerAdmin root@<hostname of the web server>
ServerName <virtual hostname of the web server>
DocumentRoot /var/www/virtual
        </VirtualHost>

        <Directory "/var/www/virtual">
AllowOverride none
Require All Granted
</Directory>                                (save and exit this file)
```

Example :

```
# vim /etc/httpd/conf.d/virtual.conf        (create the configuration file)
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName www9.example.com
DocumentRoot /var/www/virtual
        </VirtualHost>

        <Directory "/var/www/virtual">
AllowOverride none
Require All Granted
</Directory>
```

(d) Go to named based virtual directory and create the index.html file.

```
# cd /var/www/virtual
# vim index.html
        <html>
                <H1>
                        This is Name based Web Hosting
                </H1>
        </html>
(save and exit this file)
```

(e) Restart the web server deamon.

```
# service httpd start                       (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                        (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd                   (to start the webserver deamon in RHEL - 7)
```

 # systemctl enable httpd (to enable the service at next boot in RHEL - 7)

(f) Add the service to the IP tables and firewall.

In RHEL - 6 :

 # iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
 # iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
 # service iptables save
 # service iptables restart

In RHEL - 7 :

 # firewall-cmd --permanent --add-service=http
 # firewall-cmd --complete-reload

(g) Go to client system, open the firefox browser and type as http://www9.example.com in address bar and check the index page is displayed or not.

(h) We can also access the website using elinks CLI tool.

 # yum install elinks -y (install the elinks package)*
 # elinks --dump www9.example.com (access the index page)

10. How to configure the port based web hosting?

(a) Make a directory for port based hosting.

 # mkdir /var/www/port

(b) Go to the configuration file directory by # cd /etc/httpd/conf.d

(c) Create the configuration for port based hosting.

 # vim /etc/httpd/conf.d/port.conf
<VirtualHost <IP address of the web server> : 8999>
ServerAdmin root@<hostname of the web server>
ServerName <port based hostname of the web server>
DocumentRoot /var/www/port
</VirtualHost>

<Directory "/var/www/port">
AllowOverride none
Require All Granted
</Directory> *(save and exit this file)*

Example :

 # vim /etc/httpd/conf.d/virtual.conf (create the configuration file)
<VirtualHost 172.25.9.11:8999>
ServerAdmin root@server9.example.com
ServerName port9.example.com
DocumentRoot /var/www/port
</VirtualHost>

<Directory "/var/www/port">
AllowOverride none
Require All Granted
</Directory>

(d) Go to port based virtual directory and create the index.html file.

```
# cd /var/www/port
# vim index.html
        <html>
                <H1>
                        This is Port based Web Hosting
                </H1>
        </html>
```

(save and exit this file)

(e) Generally port based web hosting requires DNS server. So, we can solve this problem by the following way. For that open the /etc/hosts file enter the server name and IP addresses on both server and client.

```
# vim /etc/hosts
172.25.9.11     port5.example.com
```

(save and exit this file)

(f) By default the web server runs on port number 80. If we want to configure on deferent port number, we have to add the port number in the main configuration file.

```
# vim /etc/httpd/conf/httpd.conf
* Go to Listen : 80 line and open new line below this line and type as,
Listen : 8999
```

(save and exit this file)

(g) By default SELinux will allow 80 and 8080 port numbers only for webserver. If we use different port numbers other than 80 or 8080 then execute the following command.

```
# semanage port -a -t http_port_t -p tcp 8999
```

(h) Restart the web server deamon.

```
# service httpd start                   (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                    (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd               (to start the webserver deamon in RHEL - 7)
# systemctl enable httpd                (to enable the service at next boot in RHEL - 7)
```

(i) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 8999 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 8999 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --permanent -add-port=8999/tcp
# firewall-cmd --complete-reload
```

(j) Go to client system, open the firefox browser and type as http://port9.example.com in address bar and check the index page is displayed or not.

(k) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y                (install the elinks package)
# elinks --dump port9.example.com       (access the index page)
```

11. How to configure user authentication based web hosting?

It will ask user name and password to access this website. So, we have to provide http password.

(f) Go to the configuration file directory by # cd /etc/httpd/conf.d

(g) Create the configuration for user authentication based hosting.

```
# vim /etc/httpd/conf.d/userbase.conf
<VirtualHost <IP address of the web server> : 80>
ServerAdmin root@<hostname of the web server>
ServerName <hostname of the web server>
DocumentRoot /var/www/html
        </VirtualHost>

        <Directory "/var/www/html">
AllowOverride none
Require All Granted
AuthType Basic
AuthName "This site is protected"
AuthUserFile /etc/httpd/pass
Require User <user name>
</Directory>
        (save and exit this file)
```

Example :

```
# vim /etc/httpd/conf.d/userbase.conf                    (create the configuration file)
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
        </VirtualHost>

        <Directory "/var/www/html">
AllowOverride none
Require All Granted
AuthType Basic
AuthName "This site is protected"
AuthUserFile /etc/httpd/pass
Require User raju
</Directory>
```

(h) Go to document root directory and create the index.html file.

```
# cd /var/www/html
# vim index.html
        <html>
                <H1>
                        This is User Authentication based Web Hosting
                </H1>                   </html>
                (save and exit this file)
```

(i) Restart the web server deamon.

```
# service  httpd  start                    (to start the webserver  deamon  in  RHEL - 6)
# chkconfig  httpd  on                    (to enable the service at next boot  in  RHEL - 6)
# systemctl  restart  httpd               (to start the webserver  deamon  in  RHEL - 7)
# systemctl  enable  httpd                (to enable the service at next boot  in  RHEL - 7)
```

(j) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables  -A  INPUT  -i  eth0  -p  tcp  -m  tcp  --deport  80  -j  ACCEPT
# iptables  -A  OUTPUT  -i  eth0  -p  tcp  -m  tcp  --deport  80  -j  ACCEPT
# service  iptables  save
# service  iptables  restart
```

In RHEL - 7 :

```
# firewall-cmd  --permanent  --add-service=http
# firewall-cmd  --complete-reload
```

(k) Create the user and assign the http password.

```
# useradd  kvreddi
```

* Don't give the normal password because this user requires the http password.

```
# htpasswd  -c m  /etc/httpd/pass  <user name>
```

Example : `# htpasswd  -c m  /etc/httpd/pass  kvreddi`

(l) Go to client system, open the firefox browser and type as http://server9.example.com in address bar and check the index page is displayed or not. Then it asks password, so we have to provide http password.

(m)We can also access the website using elinks CLI tool.

```
# yum  install  elinks*  -y                    (install the elinks  package)
# elinks  --dump  server9.example.com          (access the index page)
```

* Then it asks password, so we have to provide http password.

12. How to restrict the web sites access from hosts or domains or networks?

(a) Go to the configuration file directory by `# cd /etc/httpd/conf.d`

(b) Create the configuration for IP based hosting.

```
# vim  /etc/httpd/conf.d/restrict.conf
<VirtualHost  172.25.9.11:80>
ServerAdmin  root@server9.example.com
ServerName  server9.example.com
DocumentRoot  /var/www/html
        </VirtualHost>
        <Directory  "/var/www/html">
AllowOverride  none
Require  All  Granted
Order  Allow,  Deny
Allow  from  172.25.9.0  or  172.25.0
                        (allows  172.25.9  network  or  172.25 network to access the websites)
Deny  from  .my133t.org
                        (deny  all the systems of  *.my133t.org  domain to access the websites)
</Directory>
```

13. How to Redirect the website?

* Redirecting means whenever we access the website, it redirects to another website.

(a) Go to the configuration file directory by # cd /etc/httpd/conf.d

(b) Create the configuration for redirect based hosting.

```
# vim /etc/httpd/conf.d/rediect.conf
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
Redirect / "http://www.google.com"
        </VirtualHost>
        <Directory "/var/www/html">
AllowOverride none
Require All Granted
</Directory>
        (save and exit this file)
```

(c) Go to document root directory and create the index.html file.

```
# cd /var/www/html
# vim index.html
        <html>
                <H1>
                        This is Redirect based Web Hosting
                </H1>
        </html>
```

(save and exit this file)

(d) Restart the web server deamon.

```
# service httpd start                    (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                     (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd                (to start the webserver deamon in RHEL - 7)
# systemctl enable httpd                 (to enable the service at next boot in RHEL - 7)
```

(e) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --complete-reload
```

(f) Go to client system, open the firefox browser and type as http://server9.example.com in address bar and check the redirection google web page is displayed or not.

(g) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y                 (install the elinks package)
# elinks --dump server9.example.com      (access the index page)
```

* This website redirects to the google website.

14. How to configure the website with alias name?

(a) Go to the configuration file directory by # cd /etc/httpd/conf.d

(b) Create the configuration for alias based hosting.

```
# vim /etc/httpd/conf.d/alias.conf
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
Alias /private /var/www/html/private
        </VirtualHost>
        <Directory "/var/www/html/private">
AllowOverride none
Require All Granted
</Directory>                                    (save and exit this file)
```

(c) Create private directory in /var/www/html.

```
# mkdir /var/www/html/private
```

(c) Go to document root private directory and create the index.html file.

```
# cd /var/www/html/private
# vim index.html
        <html>
                <H1>
                        This is Alias based Web Hosting
                </H1>
        </html>
```

(save and exit this file)

(d) Restart the web server deamon.

```
# service httpd start                    (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                     (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd                (to start the webserver deamon in RHEL - 7)
# systemctl enable httpd                 (to enable the service at next boot in RHEL - 7)
```

(e) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --complete-reload
```

(f) Go to client system, open the firefox browser and type as http://server9.example.com/privae in address bar and check the private or alias based web page is displayed or not.

(g) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y                 (install the elinks package)
# elinks --dump server9.example.com/private   (access the index page)
```

15. How to configure the directory based web hosting?

(a) Go to the configuration file directory by # cd /etc/httpd/conf.d

(b) Create the configuration for direct based hosting.

```
# vim /etc/httpd/conf.d/confidential.conf
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
        </VirtualHost>
        <Directory "/var/www/html/confidential">
AllowOverride none
Require All Granted
</Directory>
        (save and exit this file)
```

(c) Create confidentialdirectory in /var/www/html.

```
# mkdir /var/www/html/confidential
```

(c) Go to confidential directory and create the index.html file.

```
# cd /var/www/html/confidential
# vim index.html
        <html>
                <H1>
                        This is Alias based Web Hosting
                </H1>
        </html>
```

(save and exit this file)

(d) Restart the web server deamon.

```
# service httpd start                    (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                     (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd                (to start the webserver deamon in RHEL - 7)
# systemctl enable httpd                 (to enable the service at next boot in RHEL - 7)
```

(e) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --complete-reload
```

(f) Go to client system, open the firefox browser and type as http://server9.example.com/confidential in address bar and check the directory based web page is displayed or not.

(g) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y                 (install the elinks package)
# elinks --dump server9.example.com/confidential    (access the index page)
```

16. How to configure the web server to display the user defined home page not the index.html page?

Normally Apache will look the index.html as the home page by default. If the name changed it will display the home page without configure that one. For that we can do the above as follows.

(i) Go to configuration file directory by # cd /etc/httpd/conf.d command.

(ii) Create a userpage configuration file.

```
# vim userpage.conf
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
DirectoryIndex userpage.html
        </VirtualHost>

        <Directory "/var/www/html">
        AllowOverride none
        Require All Granted
        </Directory>
                                (save and exit this file)
```

(iii) Go to document root directory by # cd /var/www/html command.

(iv) # vim userpage.html

```
        <html>
                <H1>
                        This is userpage as home page web hosting
                </H1>
        </html>
                (save and exit this file)
```

(d) Restart the web server deamon.

```
# service httpd start                    (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                     (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd                (to start the webserver deamon in RHEL - 7)
# systemctl enable httpd                 (to enable the service at next boot in RHEL - 7)
```

(e) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --complete-reload
```

(f) Go to client system, open the firefox browser and type as http://server9.example.com in address bar and check the user defined web page is displayed or not.

(g) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y                 (install the elinks package)
# elinks --dump server9.example.com      (access the index page)
```

17. How to configure CGI based web hosting?

CGI content will change dynamically every time the client accessed it. Normal web server will not be used to support this type of web hosting. To access these dynamic pages, we have to configure the web server as ".wsgi" server. The following steps will configure the CGI web server.

(a) Install the CGI package by # yum install mod_wsgi -y command.*

(b) Download or create the CGI script file in web server's document root directory.

Example : # cp webapp.wsgi /var/www/html

(c) Create the configuration file for CGI based web hosting.

```
<VirtualHost 172.25.9.11:80>
ServerAdmin root@server9.example.com
ServerName webapp9.example.com
DocumentRoot /var/www/html
WSGIScriptAlias / /var/www/html/webapp.wsgi
</VirtualHost>
```

(d) Restart the web server deamon.

```
# service httpd start                (to start the webserver deamon in RHEL - 6)
# chkconfig httpd on                 (to enable the service at next boot in RHEL - 6)
# systemctl restart httpd            (to start the webserver deamon in RHEL - 7)
# systemctl enable httpd             (to enable the service at next boot in RHEL - 7)
```

(e) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 80 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --complete-reload
```

(f) Go to client system, open the firefox browser and type as http://webapp9.example.com in address bar and check the CGI based web page is displayed or not.

(g) We can also access the website using elinks CLI tool.

```
# yum install elinks* -y             (install the elinks package)
# elinks --dump webapp9.example.com  (access the index page)
```

18. What is secured web server?

Secured web server means normal Apache web server with SSL support. In normal web server the data communication is done in plain text format. So, there is no security for data because everyone can access the data. If we want to provide security to the data, then we have to configure the web server with SSL support.

19. What is the profile of secured web server?

Package	*:*	*mod_ssl*
Configuration file	*:*	*/etc/httpd/conf.d/ssl.conf*
Private key location	*:*	*/etc/pki/tls/private*
Public key location	*:*	*/etc/pki/tls/certs*

Authentication certificate: /etc/pki/tls/certs
Port number : 443
** Private key extention is " . key " and public key extention is " . crt "*

20. How to configure the secured web server?

(a) Install the web server and secure shell packages.
 # yum install httpd mod_ssl* -y command.*

(b) Download the private key and public certificates.
 # cd /etc/pki/tls/private
 # wget http://classroom.example.com/pub/tls/private/server<no.> . key
 # cd /etc/pki/tls/certs
 # wget http://classroom.example.com/pub/tls/certs/server<no.> . crt
 # wget http://classroom.example.com/pub/example-ca.crt

(c) Create the configuration file for secured web server.
 # vim /etc/httpd/conf.d/https.conf
<VirtualHost 172.25.9.11:443>
ServerAdmin root@server9.example.com
ServerName server9.example.com
DocumentRoot /var/www/html
</VirtualHost>

(d) We have to copy 7 lines from ssl.conf file to https.conf file.
 # vim -O ssl.conf https.conf
Copy the line numbers 70, 75, 80, 93, 100, 107, 116 copy and paste them in https.conf file.
So, after copied those line the https.conf file should be as below.
<VirtualHost 172.25.9.11:443>
ServerAdmin root@server9.example.com
ServerName server9.example.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
SSLCertificateFile /etc/pki/tls/certs/server9.crt
SSLCertificateKeyFile /etc/pki/tls/private/server9.key
#SSLCertificateChainFile /etc/pki/tls/certs/example-ca.crt
DocumentRoot /var/www/html
</VirtualHost>
<Directory "/var/www/html">
AllowOverride
Require All Granted
</Directory>
(save and exit this file)

(e) Go to document root directory by # cd /var/www/html command.
(f) # vim index.html

```
<html>
        <H1>
                This is a  secured  web hosting

        </H1>
</html>
```

(save and exit this file)

(g) Restart the web server deamon.

```
# service  httpd  start                    (to start the webserver  deamon  in  RHEL - 6)
# chkconfig  httpd  on                    (to enable the service at next boot  in  RHEL - 6)
# systemctl  restart  httpd               (to start the webserver  deamon  in  RHEL - 7)
# systemctl  enable  httpd                (to enable the service at next boot  in  RHEL - 7)
```

(h) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables  -A  INPUT  -i  eth0  -p  tcp  -m  tcp  --deport  443 -j  ACCEPT
# iptables  -A  OUTPUT  -i  eth0  -p  tcp  -m  tcp  --deport  443 -j  ACCEPT
# service  iptables  save
# service  iptables  restart
```

In RHEL - 7 :

```
# firewall-cmd  --permanent  --add-service=http
# firewall-cmd  --permanent  --add-service=https
# firewall-cmd  --complete-reload
```

(i) Go to client system, open the firefox browser and type as https://server9.example.com/ in address bar and check the secured web page is displayed or not.

21. How to generate our own private and public keys using crypto-utils package?

(i) Install the package by # yum install crypto-utils* -y command.

(ii) Create our own public and private keys by # genkey <hostname of the server> command.

Ex: #genkey server9.example.com (one window will be opened and we have to enter the details)

Click on Next ---> Don't change the default size ---> Next ---> No --->The keys are generated in their directories.

Other useful commands :

```
# httpd  -t                    (to check the web server configuration file for  syntax  errors)
```

Chapter#21 – Mail Server

1. What is mail server?

A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers. A client computer is normally the computer where you read your e-mails, for example your computer at home or in your office. Also an advanced mobile phone or Smartphone, with e-mail capabilities, can be regarded as a client computer in these circumstances.

2. How many types of mail servers available in Linux?

There are two types of mail servers.

(i) Sendmail server (default in RHEL - 5, available in 6 and 7)

(ii) Postfix (default in RHEL - 6 and 7)

These both mail server are used to send and receive the mails, but we cannot used both mail servers at a time ie., we have to use only one server at a time. These mail servers are used as CLI mode. Outlook express in windows is used to send or receive the mails. Thunderbird is used to send or receive the mails using GUI mode in Linux. # mail is the command used to send the mails in CLI mode.

3. What are MUA, MTA, SMTP, MDA and MRAs?

MUA :

MUA stands for Mail User Agent. It is the e-mail client which we used to create-draft-send emails. Generally Microsoft Outlook, Thunderbird, kmail, ...etc., are the examples for MUAs.

MTA :

MTA stands for Mail Transfer Agent. It is used to transfer the messages and mails between senders and recipients. Exchange, Qmail, Sendmail, Postfix, ...etc., are the examples for MTAs.

SMTP:

SMTP stands for Simple Mail Transfer Protocol. It is used to transfer the messages and mails between the MTAs.

MDA :

MDA stands for Mail Delivery Agent. It is a computer software component that is responsible for the delivery of e-mail messages to a local recipient's mailbox. Within the Internet mail architecture, local message delivery is achieved through a process of handling messages from the message transfer agent, and storing mail into the recipient's environment (typically a mailbox).

MRA :

MRA stands for Mail Retrieval Agent. It is a computer application that retrieves or fetches e-mail from a remote mail server and works with a mail delivery agent to deliver mail to a local or remote email mailbox. MRAs may be external applications by themselves or be built into a bigger application like an MUA. Significant examples of standalone MRAs include fetchmail, getmail and retchmail.

4. What is the profile of mail server?

Package : sendmail (in RHEL - 5, 6 and 7) or postfix (in RHEL - 6 and 7).
Configuration file : /etc/postfix/main.cf, /etc/dovecot/dovecot.conf
Log file : /var/log/mail.log
User's mails location : /var/spool/mail/<user name>
root user's mail location: /var/spool/mail/root
Deamons : postfix
Port number : 25

5. How to configure the mail server?

The pre-requisite for mail server is DNS. ie., Domain Naming System should be configured first.

(i) Check the hostname of the server by # hostname command.
(ii) Install the mail server package by # yum install postfix dovecot* -y command.*
(iii) Open the mail configuration file and at last type as below.

```
# vim /etc/postfix/main.cf
myhostname = server9.example.com
mydomain = example.com
myorigin = $mydomain
inet_interfaces = $myhostname, localhost
mydestination = $myhostname, localhost.$localdomain, localhost, $mydomain
home_mailbox = Maildir /                                   (save and exit this file)
```

(iv) Open the another configuration file and at last type as below.

```
# vim /etc/dovecot/dovecot.conf
protocols = imap pop3 lmtp                    (save and exit this file)
```

(v) Restart the mail server services.

```
# service postfix restart                  (to restart the postfix deamon in RHEL - 6)
# service dovecot restart                  (to restart the dovecot deamon in RHEL - 6)
# chkconfig postfix on                     (to enable the postfix deamon at next boot in RHEL - 6)
# chkconfig dovecot on                     (to enable the dovecot deamon at next boot in RHEL - 6)
# systemctl restart postfix doveco0t
        (to restart the postfix and dovecot deamons in RHEL - 6)
# systemctl enable postfix dovecot         (to enable the deamons at next boot in RHEL - 6)
```

(vi) Add the service to the IP tables and firewall.

In RHEL - 6 :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --deport 25 -j ACCEPT
# iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 25 -j ACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-port=25/tcp
# firewall-cmd --complete-reload
```

(vii) Send a test mail to the user.

```
# mail -s testmail kvreddi
Hi this is a test mail
ok bye... bye ....
```

(exit and send the mail by Ctrl + d)

(viii) Login as kvreddi user and check the mail.

```
# su - kvreddi
  $ ls
  $ cd Maildir
  $ ls
  $ cd new
  $ cat <mail name>
```

6. How to configure mail server as null client in RHEL - 7 ?

(i) Open the configuration file and at last type as below.

```
# vim /etc/postfix/main.cf
relayhost = [client9.example.com]
inet_interfaces = loopback-only
mynetworks = 127.0.0.0/8 [ : : 1]/128
myorigin = server9.example.com
mydestination =
local_transport = error : local delivery disabled
        (save and exit this file)
```

(ii) Restart the postfix deamons.

```
# systemctl restart postfix
# systemctl enable postfix
```

(iii) Add the postfix service to Firewall.

```
# firewall-cmd --permanent --add-port=25/tcp
# firewall-cmd --complete-reload
```

(iv) Send a test mail to the user.

```
# mail -s testmail kvreddi or # mutt -s testmail kvreddi
 Hi this is a test mail
 ok bye... bye ....
                        (exit and send the mail by Ctrl + d )
```

(v) Login as kvreddi user and check the mail.

```
# su - kvreddi
  $ ls
  $ cd Maildir
  $ ls
  $ cd new
  $ cat <mail name>
```

Other useful commands :

** To send a mail to the local system, no need to configure the mail server.*

** To send a mail to the remote system, then only we have to configure the mail server.*

```
# mail kvreddi@server9.example.com                    (to send the mail to the kvreddi user of the server9)
  type the message whatever you want                  (press Ctrl + d to exit and send the mail)
# su - kvreddi                                        (to switch to the kvreddi user)
$ mail                                                (to check the mails of the kvreddi user)
  N       abcd
```

N efgh
N ijkl
N mnop (there are four mails in the mail box)
& 1 (to read the 1st mail)

* If the mail is new one then 'N' letter is appears before the mail. If it is already seen then there is no letter before the mail.
* press 'q' to quit the mail utility.

mail or mutt -s " hello " <user name1><user name2><user name3>
type the matter whatever you want (press Ctrl + d to exit and send the mail to 3 users)
$ mail (to see all the mail in the mail box)
&<type the mail number> (to read the specified mail by it's number)
& r (to send the replay mail to that user)
& p (to send the mail to the printer for printing)
& w (to write the contents of the mail into a file, ie., save the contents of the mail ina file)
& q (to quit the mail box)
& d (to delete the mail)
& d <mail number> (to delete the specified mail by it's number)
& d 1-20 (to delete the mails from 1 to 20 numbers)
# mail -s "hello" <user name>@<servername> . <domain name>
(to send the mail to the remote system)
mailq (to see the mails in the queue)

* If the mail server is not configured or not running, then the sent mails will be in the queue.

mail -s "hello" <user name1><user name2><<File name>
(send the mail with attached file to the 2 users)
postfixcheck (to verify the mail configuration file for syntax errors)

Chapter#22 – iSCSI (Remote Storage)

1. What is storage?

The memory where we can store the data, such as files, directories, ...etc., is called the storage.
Storage is mainly two types. (i) Local storage and (ii) Remote Storage.

*(i) **Local storage** :*

Local storage is a storage which is directly connected to our system and ready to use.

Example : Local hard disk, local pen drive, DAS (Direct Access Storage) ... etc.,

(ii) Remote storage :

The storage which is not connected to our system directly but allotted some space to our system in remote location is called remote storage.

Example : iSCSI (Internet Small Computer System Interface), SAN (Storage Area Network), NAS (Network Area Storage)

2. What is iSCSI and explain it?

iSCSI is a way of connecting storage devices over a network using TCP/IP. It can be used over a local area network (LAN), a wide area network (WAN), or the Internet.
iSCSI devices are disks, tapes, CDs, and other storage devices on another networked computer that you can connect to. Sometimes these storage devices are part of a network called a Storage Area Network (SAN). In the relationship between our computer and the storage device, our computer is called an initiator because it initiates the connection to the device, which is called a target.
iSCSI provides Remote Block or File Storage. Most data centers keep their storage in centralised SAN racks. iSCSI provides an inexpensive alternative to proprietary SAN hardware.

3. What is the terminology of iSCSI?

iSCSI supports sending SCSI commands from clients (initiators) over IP to SCSI storage devices (targets) on remote systems (servers). iqn is a iSCSI qualified name or number.
The format of iqn is "iqn.yyyy-mm.<domain name in reverse order>label is used to identify initiators And targets communicate through port number 3260.

4. What is the profile of iSCSI?

Package : iscsi (for RHEL-6), target* (for RHEL-7 server) and iscsi-utils* (for RHEL-7 Client)*
Configuration files:/etc/tgt/target.conf (for RHEL - 6) and /etc/target/saveconfig.json (for RHEL - 7)
Deamons : tgtd (for RHEL-6) and target (for RHEL-7 server) and iscsi, iscsid (for RHEL-7)
Port number : 3260

5. How to configure the iSCSI server?

(i) Create one partition and create the LVM with that partition.

 # fdisk <device name>
: n (new partition) ---> Enter ---> Enter ---> Enter ---> +<size in MB/GB/TB> ---> w (write the changes into the disk)
 # partprobe (to write the changes into the partition table)
 # pvcreate <disk partition name> (to create the physical volume)
 # vgcreate <physical volume name> (to create the volume group)

 # lvcreate -s <extent size> -n <logical volume name><vg name> (to create the logical volume)

(ii) Install the iSCSI package by # yum install scsi-target-utils -y command in RHEL - 6 or
Install the iSCSI package by # yum install target -y command in RHEL - 7.*

(iii) Start the iSCSI deamon and enable the deamon at next boot time.
 # service tgtd restart (to start the iSCSI deamon in RHEL - 6)
 # chkconfig tgtd on (to enable the iSCSI deamon at next boot in RHEL - 6)
 # systemctl start target (to start the target deamon in RHEL - 7)
 # systemctl enable target (to enable the target deamon at next boot in RHEL - 7)

(iii) Configure the iSCSI storage.
In RHEL - 6 :

```
#vi /etc/tgt/targets.conf
    default-driver iscsi
      <target iqn.2015-06.com.example:server9.target1>
    backing-store <iSCSI partition name>
   write-cache off
 </target>
```

In RHEL - 7 :

 # targetcli (to get the configuration window and displays "/>" prompt appears)
/> ls (to see the configuration contents)
/> /backstores/block create <block storage name><the above created volume name> (create the block storage)
/> /iscsi create iqn.2015-06.com.example:server9 (to create the lun number not the lun name)
/> /iscsi/iqn.2015-06.com.example:server9/tpg1/acls create iqn.2015-06.com.example:server9 (to create the alias name for client side lun number)
/> /iscsi/iqn.2015-06.com.example:server9/tpg1/luns create /backstores/block/<block storage name> (to create the lun using the block storage device)
/> /iscsi/iqn.2015-06.com.example:server9/tpg1/portals create <IP address of the server> (to allot the above created lun to the IP address and port number, ie., 3260)
/> saveconfig (to save the iSCSI configuration into the configuration file)
/> exit (to exit from the configuration window)

(iv) Restart the iSCSI deamons after the configuration of iSCSI or target.
 # service tgtd restart (to start the iSCSI deamon in RHEL - 6)
 # chkconfig tgtd on (to enable the iSCSI deamon at next boot in RHEL - 6)
 # systemctl restart target (to start the target deamon in RHEL - 7)
 # systemctl enable target (to enable the target deamon at next boot in RHEL - 7)
(vi) # tgt-admin --show (to check the iSCSI configuration in RHEL - 6)

(vii) Add the iSCSI service and port number to the IP tables and firewall.
In RHEL - 6 :

```
# iptables-I INPUT -p tcp-m tcp --dport3260 –jACCEPT
# iptables-O OUTPUT -p tcp-m tcp --dport3260 -jACCEPT
# service iptables save
# service iptables restart
```

In RHEL - 7 :

```
# firewall-cmd --permanent --add-port=3260/tcp
# firewall-cmd --complete-reload
```

6. How to configure the iSCSI client?

(i) Install iscsi-initiator-utils package on the client by

 # yum install iscsi-initiator-utils -y command in RHEL-6.*

 # yum install iscsi-utils -y command in RHEL - 7.*

(iv) Discover the target LUN's exported by server using following command. It will provide iqn name with of LUN associated with given ip address.

 # iscsiadm -m discovery -t sendtargets -p <IP address of the server> (in RHEL - 6)

 # iscsiadm --mode discoverydb --type sendtargets --portals <IP address of the server) (in RHEL - 7)

(v) Open the iscsi initiator file and put an entry of the above discovered lun number in RHEL - 7

 # vim /etc/iscsi/initiatorname.iscsi (go to last line and type as below)

Initiatorname=iqn.2015-06.com.example:server9 (save and exit this file)

(iv) Restart and enable the iSCSI client side deamons.

 # service iscsi restart (to restart the iscsi client deamon in RHEL - 6)

 # chkconfig iscsi on (to enable the iscsi client deamon at next boot in RHEL - 6)

 # systemctl restart iscsid iscsi (to restart the iscsi client deamons in RHEL - 7)

 # systemctl enable iscsid iscsi (to enable the iscsi client deamons at next boot in RHEL - 7)

(v) To connect iSCSI target we can use following command , we need to mention server ip and iqn name.

In RHEL - 6 :

 # iscsiadm -m node -T iqn.2015-06.com.example:server9.target1–p <IP address of the server>login

In RHEL - 7 :

 # iscsiadm --mode node --targetname iqn.2015-06.com.example:server9 --portal <IP address of the server> : 3260 --login

(vi) Check the new remote disk name by # fdisk -l command.

(vii) Create the required size partition using # fdisk, # partprobe commands.

(viii) Create the required type of file systems by # mkfs.ext4 <above created partition name> command.

(ix) Create a mount point for the above file system by # mkdir /mnt/iscsi command.

(x) Open the /etc/fstab file and put en entry of the above file system information.

 # vim /etc/fstab

<partition name> or <UUID> /mnt/iscsi ext4 _netdev 0 0 (save and exit this file)

(x) Mount the all the partitions which are having entries in /etc/fstab file by

 # mount -a command.

(xii) Check all the mounted file systems by # df -hT command.

(xiv) To disconnect iSCSI target we can use following commands.

Don't forget that logout from the target.

In RHEL - 6 :

 # iscsiadm -m node -T iqn.2015-06.com.example:server9.target1–p <IP address of the server>logout

In RHEL - 7 :

 # iscsiadm --mode node --targetname iqn.2015-06.com.example:server9 --portal <IP address of the server> : 3260 --logout

(xiv) Restart the client system by # init 6 command.

(xv) After reboot check the remote file system by # df -hT command.

Chapter#23 – MySQl Server or MariaDB

1. What is MySQL or MariaDB?

MySQL or MariaDB is a database software to create and maintain the databases.
Upto RHEL - 6 the database software is MySQL and from RHEL - 7 onwards the database software is MariaDB.If we want to do any transactions or database operations, we have to open the mysql > or mariadb > prompt. In MySQL or MariaDB all the database operation commands will end with a " ; " (semicolon).

2. What is the profile of MySQL or MariaDB?

Package : mysql (in RHEL - 6) and mariadb* (in RHEL - 7)*
Version : 5.0 (in RHEL - 6) and 5.5 (in RHEL - 7)
Deamons : mysqld (in RHEL - 6) and mariadb (in RHEL - 7)
Configuration file: /etc/my.cnf
Installation Commands : mysql_secure_installation

3. How to configure MySQL or MariaDB?

(i) Install the MySQL or Mariadb software packages.
 # yum groupinstall mysql -y (to install MySQL in RHEL - 6)*
 # yum groupinstall mariadb (to install Mariadb in RHEL - 7)*
(ii) Restart the mysqld and mariadb deamons.
 # service mysqld restart (to start the mysqld deamon in RHEL - 6)
 # chkconfig mysqld on (to enable the mysqld deamon at next boot in RHEL - 6)
 # systemctl restart mariadb (to start the mysqld deamon in RHEL - 7)
 # systemctl enable mariadb (to enable the mysqld deamon at next boot in RHEL - 7)
(iii) Check the mysql port is listening or not.
 # netstat -ntulp | grep mysql (it works in both RHEL - 6 & 7)
Where n -----> network t -----> tcp protocol u -----> udp protocol
l -----> listening or not and p -----> port number
(vi) If we want to configure the database as localhost ie., database will not be available to remote systems.
 # vim /etc/my.cnf (open this file and go to 2nd line, create an empty line and type as below)
skip-networking=1 (save and exit this file)
(v) Restart the mysqld and mariadb deamons.
 # service mysqld restart (to start the mysqld deamon in RHEL - 6)
 # chkconfig mysqld on (to enable the mysqld deamon at next boot in RHEL - 6)
 # systemctl restart mariadb (to start the mysqld deamon in RHEL - 7)
 # systemctl enable mariadb (to enable the mysqld deamon at next boot in RHEL - 7)
(vi) Install the database engine. (it works in both RHEL - 6 & 7)
 # mysql_secure_installation
Enter current root password : (here do not enter any passwords and just press the Enter Key)
Set root password [y/n] : y
Remove ananymous users [y/n] : y

Disallow root login remotely [y/n] : y
Remove test database and access to it [y/n] : y
Reload the privilages tables now [y/n] : y

(vii) Login into the mysql server as a root user.
 # mysql -u root -p (where u -----> user and p -----> using password)
(we have to enter the password for root user)

(viii) See the default databases.
mysql > show databases; (in RHEL - 6)
mariadb > show databases; (in RHEL - 7)

(ix) Exit from the database by mysql > exit; (in RHEL - 6) and mariadb > exit; (in RHEL - 7)

4. *How to create a database, create tables, enter the data into the tables and access that data?*

(i) Login into the database server by # mysql -u root -p command.

(ii) Create the database and connect the databases.
mysql or mariadb > create database <database name>; (to create the database)
mysql or mariadb>show databases; (to see all the databases in the server)
mysql or mariadb > use <database name>; (to connect to the specified database)

(iii) Create a table, enter the data and query the data.
mysql or mariadb > create table <table name> (field name1 data type (size),
field name2 data type (size),
field name3 data type (size));
Example : mysql or mariadb > create table mydetails (Name varchar (30), status varchar (10),
Address varchar (50), phone int (10));

(iv) See the structure of the table.
mysql or mariadb >describe<table name>; (to see the structure of the table)
Example : mysql or mariadb > describe mydetails;

(v) Insert or enter the data into the table.
mysql or mariadb > insert into mydetails values ("Kvreddi", "Single", Hyderabad", 9848750755);

(vi) Query the table to get the data.
*mysql or mariadb >select * from mydetails; (to see all the records of the tables)*
mysql or mariadb > select name, phone from mydetails; (to select the wanted data ie., filtering the data)

5. **How to take a backup of the database, drop the database and restore the database using backup?**

To take a backup or restore of the database first we should comeout from the database server and then take a backup or restore the backup.

(i) Exit the from the database server.
mysql or mariadb > exit;

(ii) Take a backup of the database.
 # mysqldump -u root -p <database name>><file name with full path>
Example : # mysqldump -u root -p mydetails > /root/mydetails.bak

(iii) Delete the database from the database server.
mysql or mariadb >drop database <database name>;
Example : mysql or mariadb > drop database mydetails;

(iv) Restore the deleted database using the backup copy.

mysql or mariadb >exit;
 # mysql -u root -p <database name><<backup file name with path>
Example : # mysql -u root -p mydetails < /root/mydetails.bak

6. How to create the user in the database and make the user to do transactions or operations?

(i) To create the user in the database first login to the database and then create the user.
mysql or mariadb > create user <user name>@<host name> identified by "<password>";
Example : mysql or mariadb > create user kvreddi@localhost or server9.example.com identified by "kvreddi123";

(ii) Make the user to do transactions on the database. (nothing but granting the permission)
mysql or mariadb > grant select, insert, update, delete on <database name>. to <user name>;*
or
mysql or mariadb > grant all on <database name> . to <user name>;*
Example : mysql or mariadb > grant select, insert, update, delete on mydetails . to kvreddi;*
or mysql or mariadb > grant all on mydetails . to kvreddi;*
*(where database . * means granting permissions on all the contents like tables, indexes, views, synonyms and others)*

7. How to update the table in the database with new data?

mysql or mariadb > update <table name><field name>=<new value> where <primary key field name>="<value>";
Example : mysql or mariadb > update mydetails name="bangaram" where name='kvreddi';

8. How to delete the table from the database?

mysql or mariadb > drop table <table name>;
Example : mysql or mariadb > drop table mydetails;

9. How to connect the remote database from our system?

 # mysql -u root -h <host name> -p (here we have to enter the password)
Example : # mysql -u root -h server9.example.com -p
(If the database is configured as localhost database, then server will not allow remote database connections and Permission denied message will be displayed on the screen)

10. How to add mysqld service to IPtables and mariadb service to firewall?

In RHEL - 6 :
 # iptables -A INPUT -i eth0 -p tcp -m tcp --deport 3306 -j ACCEPT
 # iptables -A OUTPUT -i eth0 -p tcp -m tcp --deport 3306 -j ACCEPT
 # service iptables save
 # service iptables restart
 # chkconfig iptables on
In RHEL - 7 :
 # firewall-cmd --permanent --add-port=3306
 # firewall-cmd --complete-reload

Chapter#24 – Log Server and Log Files

1. What is log server?

A log server represents a central log monitoring point on a network, to which all kinds of devices including Linux or Windows servers, routers, switches or any other hosts can send their logs over network. By setting up a log server, you can filter and consolidate logs from different hosts and devices into a single location, so that you can view and archive important log messages more easily.
On most Linux distributions, rsyslog is the standard syslog daemon that comes pre-installed. Configured in a client/server architecture, rsyslog can play both roles; as a syslog server rsyslog can gather logs from other devices, and as a syslog client, rsyslog can transmit its internal logs to a remote syslog server. When logs are collected with syslog mechanism, three important things must be taken into consideration:
Facility level: what type of processes to monitor
Severity (priority) level: what type of log messages to collect
Destination: where to send or record log messages

2. What is the profile of log server?

This is also called as rsyslog server. The requirements are given below.

(i)	*Package*	*:*	*rsyslog**
(ii)	*Deamon*	*:*	*rsyslog*
(iii)	*Port No.*	*:*	*514*
(iv)	*Configuration file*	*:*	*/etc/rsyslog.conf*

3. How to configure the log server?

(i) Install rsyslog package by # yum install rsyslog -y command.*
(ii) Open the log server configuration and file and edit as per requirements.
 # vim /etc/rsyslog.conf
Go to line no. : 15 & 16 and uncomment on those lines. (save and exit this file)
(iii) Restart the log server deamon in RHEL - 6 and RHEL - 7.
 # service rsyslog restart (to restart the log server deamon in RHEL - 6)
 # chkconfig rsyslog on (to enable the log server deamon at next boot in RHEL - 6)
 # systemctl restart rsyslog (to restart the log server deamon in RHEL - 7)
 # systemctl enable rsyslog (to enable the log server deamon at next boot in RHEL - 7)
(iv) Verify whether the log server is listening or not.
 # netstat -ntulp | grep 514
(v) Add the log server service to IPtables.
 # iptables -A INPUT -p tcp -m tcp --deport 514 -j ACCEPT (to add the incoming port no. to Iptables in RHEL - 6)
 # iptables -A INPUT -p udp -m udp --deport 514 -j ACCEPT (to add the incoming port no. to Iptables in RHEL - 6)
 # iptables -A OUTPUT -p tcp -m tcp --deport 514 -j ACCEPT (to add the outgoing port no. to Iptables in RHEL - 6)
 # iptables -A OUTPUT -p udp -m udp --deport 514 -j ACCEPT (to add the outgoing port no. to Iptables in RHEL - 6)

 # firewall-cmd --permanent -add-port=514/tcp (to add the 514 tcp port no. to the firewall)
 # firewall-cmd --permanent -add-port=514/udp (to add the 514 udp port no. to the firewall)
 # firewall-cmd --complete-reload (to reload the firewall configuration)

4. How to configure the client system to send log messages to the log server?

(i) Open the log server configuration file by # vim /etc/rsyslog.conf command.
(ii) Go to line no. 90 and type as below.
**.*@<log server IP address> : 514*
*Example : *.* @172.25.9.11:514 (save and exit this file)*
(iii) Restart the log server deamons in RHEL - 6 and RHEL - 7.
 # service rsyslog restart (to restart the log server deamon in RHEL - 6)
 # chkconfig rsyslog on (to enable the log server deamon at next boot in RHEL - 6)
 # systemctl restart rsyslog (to restart the log server deamon in RHEL - 7)
 # systemctl enable rsyslog (to enable the log server deamon at next boot in RHEL - 7)

* *Then all the log messages are stored in /var/log/secure location.*
* *To monitor all the messages on the server by # tailf /var/log/secure command.*
* *Open the /etc/rsyslog.conf file and type as below to store all the client's log messages in remote log server only.*

 # vim /etc/rsyslog.conf
**.* /var/log/secure*
(save and exit this file)

* *Then restart the log server deamons in RHEL - 6 and RHEL - 7.*
 # service rsyslog restart (to restart the log server deamon in RHEL - 6)
 # systemctl restart rsyslog (to restart the log server deamon in RHEL - 7)

5. What is log file?

Log file is file that contains messages about that system, including the kernel, services and applications running on it, ...etc., There are different log files for different information. These files are very useful when trying to troubleshoot a problem with systems.
Almost all log messages are stored in /var/log directory. Only root user can read these log messages. We can use less or more commands to read these log files. The messages will be generated only when rsyslog service is running, otherwise the log messages will not be generated.

The different types of log files and their locations :
/var/log/messages -----> System and general messages and DHCP log messages.
/var/log/authlog -----> Authentication log messages.
/var/log/secure -----> Security and authentication and user log messages.
/var/log/maillog -----> Mail server log messages.
/var/log/cron -----> Cron jobs log messages.
/var/log/boot.log -----> All booting log messages.
/var/log/httpd -----> All Apache web server log messages.
/var/log/mysqld.log -----> Mysql database server log messages.
/var/log/utmp or /var/log/wtmp -----> All the user's login messages.
/var/log/Qmail -----> Qmail log messages.
/var/log/kernel.log -----> All kernel related log messages.

/var/log/samba -----> All samba server log messages.
/var/log/anakonda.log -----> Linux installation log messages.
/var/log/lastlog -----> Recent login information for all users.
 # lastlog (to see the log messages of the above log file)
/var/log/yum.log -----> All package installation log messages generated by
 # yum or # rpm commands.
/var/log/cups -----> All printer and printing related log messages.
/var/log/ntpstat -----> All ntp server and services log messages.
/var/log/spooler -----> Mail, printer and cron jobs spooling messages.
/var/log/sssd -----> System security service deamon log messages.
/var/log/audit.log -----> SELinux log messages.
 # dmesg (to see the boot log messages)
 # tailf or # tail -f /var/log/secure (to check or watch the log files continuously)
 # vim /etc/rsyslog.conf (we can change the log messages default destinations)
** Whenever we change the contents of the /etc/rsyslog.conf file, then we have to restart the rsyslog service.*
** There are 7 types of priority messages. We can change the default destination of those log files. For that open rsyslog server configuration file and we have enter the rules as follows.*
 # vim /etc/rsyslog.conf
<priority type> . <priority name> <new destination of the log files> (save and exit this file)
 # logger <type any text> (to send that text into /var/log/messages files and to test whether logging service is running or not)
 # logrotate (to create the log files with datewise)
** Generally in log messages the fields are,*
Date & Time : From which system : command name or change : Execution of the command
 # yum install tmpwatch -y
(to install the tmpwatchpackage to execute the below command)
 # tmpwatch (to monitor the /tmp directory)
 # logwatch (to monitor the log messages)
 # yum install watch -y (to install the watch package to execute the below command)
 # watch <command> (to watch the specified command results continuously)
 # mkdir mode=755 /ram (to give the permissions to the directory while creating that directory)
 # journalctl (it tracks all the log files between two different timings and save by default in /run/log location)
** /run/log is mounted on tmpfs file system ie., if the system is rebooted the whole information in that location will be deleted or erased..*

Chapter#25 – Configuring IP tables and Firewalls

1. What are IPtables or firewalls?

IP tables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action. IP tables almost always comes pre-installed on any Linux distribution. We can update/Reinstall the IP tablespackage by # yum install iptables -y command.*

2. What are the types of firewalls?

There are four types of firewalls.

(i) ***Packet firewalls*** *:*

It works atPhysical, Data Link and Network Layers.
It works fast and efficiently.
It treats each packet in isolation.

Statefull firewalls *:*

It identifies a packets connection state.
It maintains packets history in the state tables.

(iii) ***Application layer firewalls*** *:*

It inspects and filter packets on OSI layer upto Application Layer.
It identifies if protocols are being misused.

(iv) ***Proxies firewalls*** *:*

It acts as an intermediary.
It operates at Application Layer.
It won't allow direct connections.

3. What are the tables maintained by IP tables?

Normally IP tables maintain 3 tables.

(i) ***INPUT table:***

This chain handles all packets that are addressed to your server and also to control the behaviour For incoming connections. For example, if a user attempts to SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.

(ii) ***OUTPUT table*** *:*

This chain contains rules for traffic created by your server. This chain is used for outgoing connections.

For example, if you try to ping ***google.com****, iptables will check its output chain to see what the rules are regarding ping and* ***google.com****before making a decision to allow or deny the connection attempt.*

(iii) ***FORWARD table*** *:*

This chain is used for incoming connections that aren't actually being delivered locally. Think of a router – data is always being sent to it but rarely actually destined for the router itself; the data is just forwarded to its target. Unless you're doing some kind of routing, NATing, or something else on your system that requires forwarding, you won't even use this chain.This chain is used to deal with traffic destined for other servers that are not created on your server. This chain is basically a way to configure your server to route requests to other machines.

4. What are the meanings of REJECT, DROP and ACCEPT ?

REJECT *:*

REJECT means server receives the FTP request from the specified IP address and rejects that request and also send the acknowledgement.

DROP *:*

DROP means server receives the FTP requests from the specified IP address and drop the request without sending any acknowledgement.

ACCEPT *:*

ACCEPT means server receives the FTP requests from the specified IP address and allow that system for FTP services.

5. What is the configuration file of IP tables and what are the options available in IP tables command?

/etc/sysconfig/iptables *is the configuration file of IP tables.*

 # iptables <options><chain> firewall-rule *(to execute the IP tables)*

The options are as follows.

-A -----> Add or append the rule.
-p -----> Indicates the protocol for that rule (tcp, udp, icmp, ...etc.;).
-s -----> Indicates the source of the packet (IP address, Network ID or Hostname).
-d ----->Indicates the destination of the packet.
-j -----> 'Jump to target' indicates the interface through which the incoming packets are coming through the INPUT , FORWARD and PREROOTING chain.
-o -----> 'Output Interface' indicates the interface through which the outgoing packets are sent through the INPUT, FORWARD and PREROOTING chain.
-sport or -source-port -----> Source port for -p tcp or -p udp.
-dport or -destination-port -----> Destination port for -p tcp or -p udp.

6. How to allow a ping from outside to inside and inside to outside?

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

7. In how many ways can we protect the network?

There are 4 ways to protect the network.

(i) SELinux
(ii) IP tables
(iii) Firewalld
(iv) TCP wrappers
IP tables and firewalld both are used to protect our systems services from outside. But we can use only one way at a time.

8. How to configure the firewalld?

(i) Install the firewalld package by ***# yum install firewalld* -y*** *command.*
(ii) Check whether the firewalld package is installed or not by ***# rpm -qa firewalld*** *command.*
(iii) Check the status of the firewalld by executing the below commands.
 # systemctl status firewalld *or* ***# firewall-cmd --status***

Examples of IP tables commands :

 # service iptables status (to check the IP tables status)
 # service iptables start (to start the IP tables)
 # service iptables stop (to stop the IP tables)
 # service iptables restart (to restart the IP tables)
 # service iptables save (to save the iptable rules permanently)
 # chkconfig iptables on (to enable the iptables at next boot)
 # chkconfig iptables off (to disable the iptables at next boot)
 # iptables -A INPUT -i eth0 -p tcp --deport 22 -j ACCEPT (to add the rules to the existing iptables to allow ssh)

where -A ---> Add or append a rule to the INPUT chain for incoming traffic.
-i eth0 ---> Incoming packets through the interface eth0 will be verified against this added new rule.
-p tcp -deport 22 ---> protocol is tcp and the destination port is 22.
-j ACCEPT ---> Accept the packet.

 # iptables -A INPUT -p tcp -m state --state NEW -m tcp --deport 80 -j ACCEPT (to allow http traffic)

 # iptables -A INPUT -s 9.9.9.9 -p tcp -m state --state NEW -m tcp --deport 443 -j ACCEPT (to allow https traffic)

 # iptables -A INPUT -i eth0 -p tcp --deport 22 -m state --state NEW, ESTABLISHED -j ACCEPT and # iptables -A INPUT -o eht0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT (to allow ssh input and output on port number 22 through a device eth0)

 # iptables -A IN PUT -p udp -m state --state NEW -m udp --deport 161 -j ACCEPT (to allow SNMP traffic through port number 161)

 # iptables -P INPUT DROP (to block the input traffic)
 # iptables -P FORWARD DROP (to block the forward traffic)
 # iptables -p OUTPUT DROP (to block the output traffic)
(where P is capital letter)
 # iptables -A INPUT -s 9.9.9.9 -j DROP (to block the 9.9.9.9 input traffic)
 # iptables -L (to see the list of the IP tables)
 # iptables -F (to flush the iptable rules nothing but deleting all the rules)

* Don't run this command on production servers or real time environment.

iptables -save > /root/iptables (to save all the existing iptables rules as backup copy in /root/iptables file)

iptables -F (to delete all iptables rules)

iptables -restore < /root/iptables (to restore the IP tables from the backup file)

iptables -I INPUT -s <IP address> -p tcp --deport 21 -j <REJECT> or <DROP> or <ACCEPT> (to REJECT or DROP or ACCEPT the FTP requests from the specified IP address system)

iptables -I INPUT -s <IP address>/<net mask as 8/16/24> -p tcp --deport 21 -j <REJECT> or <DROP> or <ACCEPT>
(to REJECT, DROP or ACCEPT the FTP requests from all the systems in that network)

iptables -I INPUT -s <IP address>/<net mask as 8/16/24> -p tcp -j <REJECT> or <DROP> or <ACCEPT>
(to REJECT, DROP or ACCEPT all the requests from the specified system all the systems in that network)

watch -d -n 5 free (to repeat a free command for every 5 seconds)

* Default is for every 2 seconds. -d option highlights the change. Press Ctrl+c to quit from the above command.

ping -a 192.168.10.1 (to ping the IP address with audiable ping ie., it makes noises)

shred -n 5 trail.txt (to over write the trail.txt file five times default is 3 times)

shred -u 5 trail.txt (to remove a file after over writing)

* This **shed** tool may not work in journaling or RAID file systems.

file <file name> (to know what type file is that)

mtr <IP address> (to check the connection between the source and the destinations)

* The above command gives the report continuously until the user press Ctrl+c.

htop (it is an improved **top** command and it allows to scroll vertically or horizontally)

logsave filelist.txt ls -l (to capture the output of any command and stores it in a file along with the starting and ending time of the command)

look "printf" avltree.c (to display all the lines in a file that start with a particular string and performance of this command is more than grep)

stat <file name> (to display the status of a file or file system like absolute path of the files, the no of blocks used by the file, the I/O block size, inode access specifier, access time, time of modification, ...etc)

mc (it is a powerful text based file manager and it is a directory browsing tool and allows to see thecontents of the archived files, ...etc.;)

* In RHEL - 6 we have to write the rules and regulations to allow or deny the system but, in RHEL - 7 we have enable or disable the firewalld options only.

firewall-config (to manage the firewalld services using graphical user mode)

firewall-cmd --get-zones (to display all available zones)

firewall-cmd --get-default-zone (to check the default zone, the default zone is **public zone**)

firewall-cmd --set-default-zone=work (to activate the work zone, nothing but changing default zone temporarily)

 # firewall-cmd --permanent --set-default-zone=work (to set the default zone as work permanently)
 # firewall-cmd --get-activate-zones
(to display which zone is an active with IP address and interface eth0)
 # firewall-cmd --add-service=172.25.0.0/24 --zone=public
(to add the source to the public zone temporarily)
 # firewall-cmd --get-activate-zone (to see the default zone which is activated)
 # firewall-cmd --permanent -add-source=172.25.0.0/24 --zone=public
to add the IP address to public zone permanently)
 # firewall-cmd --remove -souce =172.25.0.0/24 --zone=public
(to remove the iP address from public zone temporarily)
 # firewall-cmd --permanent --remove-source=172.25.0.0/24 --zone=public
(to remove the iP address from public zone permanently)
 # firewall-cmd --add-interface=eth1 --zone=public
(to change the interface or add interface to the public zone temporarily)
 # firewall-cmd --permanent --add-interface=eth1 --zone=public
(to change the interface or add interface to the public zone permanently)
 # firewall-cmd --get-active-zones (to see the activated zones)
** All rules what we have written are temporary. If the system is rebooted then all changed values are revert back to it's previous state*
** To make the changed values permanent then, add* ***--permanent*** *to all the commands set of firewalld.*
 # firewall-cmd --reload (to apply the changed rules immediately)
 # firewall-cmd --permanent --add-service=sshd (to add the sshd service to firewall permanently)
 # firewall-cmd --list-services (to list all the firewall added services)
 # firewall-cmd --list-all (to list all the all the firewall added services with detailed information)
 # firewall-cmd --permanent --remove-service=sshd (to remove sshd service from firewall permanently)
 # firewall-cmd --permanent --add-port=22/tcp (to add the port number 22 with tcp protocol to firewall permanently)
 # firewall-cmd --permanent --remove-port=22/tcp (to remove the port number 22 permanently)
 # firewall-cmd --complete-reload (first it unload all the firewall settings and again reload the firewall settings completely)

Chapter#26 – TCP Wrappers

1. Firewalld will protect all the services.

** TCP WRAPPER will also protect the services, but it can support for only limited services. And it can protect the services which are having the* ***libwrap.so*** *module is loaded for that service.*

** So, TCPWRAPPER does not support to protect all the services except* ***libwrap.so*** *module loaded.*

 # ldd (this command is used to check the modules which are loaded for this services)

 # ldd <service name with full path> (to display all the loaded modules of the specified service)

 # ldd /usr/sbin/sshd (to display all the loaded modules of the sshd service)

 # ldd /usr/sbin/sshd | grep -i libwrap.so (to check whether libwrap.so module is loaded or not)

2. To configure the TCPWRAPPER :

(i) Open /etc/hosts.deny or /etc/hosts.allow file by ***# vim /etc/hosts.deny or hosts.allow*** *commands.*

** The above files are to be edited or modified to enable or disable the tcpwrapper services the users.*

 # vim /etc/hosts.deny (Go to last line and type as below)

sshd : 172.25.9.11 or system9.example.com *(to deny the specified host or hostname)*

sshd : ALL *(to deny all the clients)*

sshd : ALL EXCEPT *.eample.com *(to deny all the clients except all the systems of example.com domain)*

(ii) save and exit this file.

(iii) Open ***/etc/hosts.allow*** *by* ***# vim /etc/hosts.allow*** *command and go to last line and type as below.*

sshd : 172.25.9.11 172.25.6.11 *(to allow 2 systems only)*

(iv) save and exit this file.

** If the client system's entry is there in both /etc/hosts.deny and /etc/hosts.allow files, then the TCPWRAPPER will look /etc/hosts.allow file first. Then it will look /etc/hosts.deny file. If there is an entry in both the files, then it will allow the system because based on the above rule first it will read /etc/hosts.allow file and allow the system. It won't read the /etc/hosts.deny file.*

Chapter#27 – Virtualization

1. What is virtualization?

Virtualization allows multiple operating system instances to run concurrently on a single computer;it is a means of separating hardware from a single operating system. Each "guest" OS is managed bya Virtual Machine Monitor (VMM), also known as a hypervisor. Because the virtualization system sitsbetween the guest and the hardware, it can control the guests' use of CPU, memory, and storage,even allowing a guest OS to migrate from one machine to another.

2. What are types of virtualizations available in Linux?

RHEL - 5 :
xen
64 bit
VT-Enabled
Intel/AMD
2 GB RAM
6 GB Hard disk

RHEL - 6 & 7 :
kvm
64 bit
VT-Enabled
Intel/AMD
2 GB RAM
6 GB Hard disk

3. What are the packages of virtualization and how to install the packages?

(i) qemu (It is used to provide user level KVM virtualization and disk image also)
(ii) virt (It is used to provide virtualization software)
(iii) libvirt (It is used to provide the libraries for virtualization software)
(iv) python (This package provides the host and server libraries for interacting with Hypervisor and Host system)
 # yum install qemu virt* libvirt* python* -y (to install the virtualization softwares)*

4. How to start the virtualization manager and how to create a new virtual machine?

(i) Go to Applications -----> System Tools -----> Virtual Machine Manager
(ii) Vitual Machine Manager is used to check and displays the available virtual machines. It is also used to create the new virtual machines.
(iii) To create a new virtual machine first click on monitor icon, then enter the virtual machine name, Select Local and Select Forward.
(iv) Click on Browse Local, Select the guest O/S " . iso " image file and Select Forward.

5. What are the packages of Virtualization Hypervisor and how to install the packages?

(i) "virtualization hypervisor" (provides the foundation to host virtual machines includes the libvirt and qemu- kvm package)
(ii) "virtualization client" (provides the support to install and manage virtual machines includes virsh, virt-install, virt-manager, virt-top and virt-viewer packages)
(iii) "virtualization tools" (provides tools for offline management of virtual machines includes the libguestfs package)
(iv) "virtualization platform" (provides an interface to access and control virtual machines includes the libvirt, libvirt-client and virt-who packages)

Installation of Virtualization Hypervisor :

 # yum group install "virtualization hypervisor" "virtualization client" "virtualization tools" "virtualization platform" -y

6. How to create a storage pool and volume using virsh tool?

(i) View all the available storage pools by ***# virsh pool-list*** *command.*

(ii) Create a storage pool directory by ***# mkdir /var/lib/libvirt/<pool name>*** *command.*

(iii) Define the storage pool directory by

 # virsh pool-define-as <pool name> dir ----/var/lib/libvirt/<pool name> *command.*

(iv) Start the virtual storage pool by ***# virsh pool-start <pool name>*** *command.*

(v) To see the specified storage pool information by ***# virsh pool-info <pool name>*** *command.*

(vi) Create the storage pool volume with specified size by ***# virsh vol-create-as <pool name><pool volume><size in MB/GB/TB>*** *command.*

(vii) To see the list of all available storage pool volumes by ***# virsh vol-list <pool name>*** *command.*

Other useful commands :

# lscpu	*(to list the CPU information)*
# cat /proc/cpuinfo	*(to display the CPU information)*
# virsh start <virtual machine name>	*(to start the virtual machine)*
# virsh shutdown<virtual machine name>	*(to shutdown the virtual machine)*
# virsh destroy <virtual machine name>	*(to delete the virtual machine)*
# virsh suspend <virtual machine name>	*(to pause the virtual machine)*
# virsh resume <virtual machine>	*(to start the paused virtual machine)*
# virsh net-list	*(to see all the available virtual machines)*
# virsh net-define /root/<virtualnetname.xml>	*(to define a virtual network using xml file)*
# virsh net-autostart <virtualnet name>	*(to set the virtual network autostart at reboot)*
# virsh net-start <virtual net name>	*(to start the virtual network)*
# rht-vmctl fullreset all	*(to reset all the virtual machines as new machines)*
# rht-vmctl reset server	*(to reset the server virtual machine)*
# rht-vmctl reset client	*(to reset the client virtual machine)*
# pushcourse all <system hostname>	*(to send the server and client virtual machines to the specified system)*

Chapter#28 – RedHat Cluster

1. How can you define a cluster and what are its basic types?

A cluster is two or more computers (called nodes or members) that work together to perform a task.
There are four major types of clusters:
Storage
High availability
Load balancing
High performance

2. What is Storage Cluster?

Storage clusters provide a consistent file system image across servers in a cluster, allowing the servers to simultaneously read and write to a single shared file system.
A storage cluster simplifies storage administration by limiting the installation and patching of applications to one file system.
The High Availability Add-On provides storage clustering in conjunction with Red Hat GFS2

3. What is High Availability Cluster?

High availability clusters provide highly available services by eliminating single points of failureand by failing over services from one cluster node to another in case a node becomes inoperative.
Typically, services in a high availability cluster read and write data (via read-write mounted file systems).
A high availability cluster must maintain data integrity as one cluster node takes over control of a service from another cluster node.
Node failures in a high availability cluster are not visible from clients outside the cluster.
High availability clusters are sometimes referred to as failover clusters.

4. What is Load Balancing Cluster?

Load-balancing clusters dispatch network service requests to multiple cluster nodes to balance the request load among the cluster nodes.
Load balancing provides cost-effective scalability because you can match the number of nodes according to load requirements. If a node in a load-balancing cluster becomes inoperative, the load-balancing software detects the failure and redirects requests to other cluster nodes.
Node failures in a load-balancing cluster are not visible from clients outside the cluster.
Load balancing is available with the Load Balancer Add-On.

5. What is a High Performance Cluster?

High-performance clusters use cluster nodes to perform concurrent calculations.
A high-performance cluster allows applications to work in parallel, therefore enhancing the performance of the applications. High performance clusters are also referred to as computational clusters or grid computing.

6. How many nodes are supported in Red hat 6 Cluster?

A cluster configured with qdiskd supports a maximum of 16 nodes. The reason for the limit is because of scalability; increasing the node count increases the amount of synchronous I/O contention on the shared quorum disk device.

7. What is the minimum size of the Quorum Disk?

The minimum size of the block device is 10 Megabytes.

8. What is the order in which you will start the Red Hat Cluster services?

In Red Hat 4 :

 # service ccsd start
 # service cman start
 # service fenced start
service clvmd start (If CLVM has been used to create clustered volumes)
 # service gfs start
 # service rgmanager start

In RedHat 5 :

 # service cman start
 # service clvmd start
 # service gfs start
 # service rgmanager start

In Red Hat 6 :

 # service cman start
 # service clvmd start
 # service gfs2 start
 # service rgmanager start

9. What is the order to stop the Red Hat Cluster services?

In Red Hat 4 :

 # service rgmanager stop
 # service gfs stop
 # service clvmd stop
 # service fenced stop
 # service cmanstop
 # service ccsd stop

In Red Hat 5 :

 # service rgmanager stop
 # servicegfsstop
 # service clvmd stop
 # servicecman stop

In Red Hat 6 :

 # service rgmanagerstop
 # service gfs2 stop
 # service clvmdstop
 # service cman stop

10. What are the performance enhancements in GFS2 as compared to GFS?

Better performance for heavy usage in a single directory
Faster synchronous I/O operations
Faster cached reads (no locking overhead)
Faster direct I/O with preallocated files (provided I/O size is reasonably large, such as 4M blocks)
Faster I/O operations in general
Faster Execution of the df command, because of faster statfs calls
Improved atime mode to reduce the number of write I/O operations generated by atime when compared with GFS
GFS2 supports the following features.
extended file attributes (xattr)
the lsattr() and chattr() attribute settings via standard ioctl() calls
nanosecond timestamps
GFS2 uses less kernel memory.
GFS2 requires no metadata generation numbers.
Allocating GFS2 metadata does not require reads. Copies of metadata blocks in multiple journals are managed by revoking blocks from the journal before lock release.
GFS2 includes a much simpler log manager that knows nothing about unlinked inodes or quota changes.
The gfs2_grow and gfs2_jadd commands use locking to prevent multiple instances running at the same time.
The ACL code has been simplified for calls like creat() and mkdir().
Unlinked inodes, quota changes, and statfs changes are recovered without remounting the journal.

11. What is the maximum file system support size for GFS2?

GFS2 is based on 64 bit architecture, which can theoretically accommodate an 8 EB file system.
However, the current supported maximum size of a GFS2 file system for 64-bit hardware is 100 TB.
The current supported maximum size of a GFS2 file system for 32-bit hardware for Red Hat Enterprise Linux Release 5.3 and later is 16 TB.
NOTE: It is better to have 10 1TB file systems than one 10TB file system.

12. What is the journaling filesystem?

A journaling filesystem is a filesystem that maintains a special file called a journal that is used to repair any inconsistencies that occur as the result of an improper shutdown of a computer.
In journaling file systems, every time GFS2 writes metadata, the metadata is committed to the journal before it is put into place.
This ensures that if the system crashes or loses power, you will recover all of the metadata when the journal is automatically replayed at mount time.
GFS2 requires one journal for each node in the cluster that needs to mount the file system. For example, if you have a 16-node cluster but need to mount only the file system from two nodes, you need only two journals. If you need to mount from a third node, you can always add a journal with the gfs2_jadd command.

13. What is the default size of journals in GFS?

When you run mkfs.gfs2 without the size attribute for journal to create a GFS2 partition, by default a 128MB sizejournal is created which is enough for most of the applications

In case you plan on reducing the size of the journal, it can severely affect the performance. Suppose you reduce the size of the journal to 32MB it does not take much file system activity to fill an 32MB journal, and when the journal is full, performance slows because GFS2 has to wait for writes to the storage.

14. What is a Quorum Disk?

Quorum Disk is a disk-based quorum daemon, qdiskd, that provides supplemental heuristics to determine node fitness.
With heuristics you can determine factors that are important to the operation of the node in the event of a network partition
For a 3 node cluster a quorum state is present until 2 of the 3 nodes are active i.e. more than half. But what if due to some reasons the 2nd node also stops communicating with the 3rd node? In that case under a normal architecture the cluster would dissolve and stop working. But for mission critical environments and such scenarios we use quorum disk in which an additional disk is configured which is mounted on all the nodes with qdiskd service running and a vote value is assigned to it.
So suppose in above case I have assigned 1 vote to qdisk so even after 2 nodes stops communicating with 3rd node, the cluster would have 2 votes (1 qdisk + 1 from 3rd node) which is still more than half of vote count for a 3 node cluster. Now both the inactive nodes would be fenced and your 3rd node would be still up and running being a part of the cluster.

15. What is rgmanager in Red Hat Cluster and its use?

This is a service termed as Resource Group Manager
RGManager manages and provides failover capabilities for collections of cluster resources called services, resource groups, or resource trees
it allows administrators to define, configure, and monitor cluster services. In the event of a node failure, rgmanager will relocate the clustered service to another node with minimal service disruption.

16. What is luci and ricci in Red Hat Cluster?

luci is the server component of the Conga administration utility
Conga is an integrated set of software components that provides centralized configuration and management of Red Hat clusters and storage
luci is a server that runs on one computer and communicates with multiple clusters and computers via ricci

ricci is the client component of the Conga administration utility
ricci is an agent that runs on each computer (either a cluster member or a standalone computer) managed by Conga
This service needs to be running on all the client nodes of the cluster.

17. What is cman in Red Hat Cluster?

This is an abbreviation used for Cluster Manager.
CMAN is a distributed cluster manager and runs in each cluster node.
It is responsible for monitoring, heartbeat, quorum, voting and communication between cluster nodes.
CMAN keeps track of cluster quorum by monitoring the count of cluster nodes.

18. What are the different port no. used in Red Hat Cluster?

IP Port no.	Protocol	Component
5404,5405	UDP	corosync/cman
11111	TCP	ricci
21064	TCP	dlm (Distributed Lock Manager)
16851	TCP	Modclustered
8084	TCP	luci
4196,4197	TCP	rgmanager

19. How does NetworkManager service affects Red Hat Cluster?

The use of NetworkManager is not supported on cluster nodes. If you have installed NetworkManager on your cluster nodes, you should either remove it or disable it.
 # service NetworkManager stop
 # chkconfig NetworkManager off
The cman service will not start if NetworkManager is either running or has been configured to run with the chkconfig command

20. What is the command used to relocate a service to another node?

 # clusvcadm -r service_name -m node_name

21. What is split-brain condition in Red Hat Cluster?

We say a cluster has quorum if a majority of nodes are alive, communicating, and agree on the active cluster members. For example, in a thirteen-node cluster, quorum is only reached if seven or more nodes are communicating. If the seventh node dies, the cluster loses quorum and can no longer function.
A cluster must maintain quorum to prevent split-brain issues.

If quorum was not enforced, quorum, a communication error on that same thirteen-node cluster may cause a situation where six nodes are operating on the shared storage, while another six nodes are also operating on it, independently. Because of the communication error, the two partial-clusters would overwrite areas of the disk and corrupt the file system.
With quorum rules enforced, only one of the partial clusters can use the shared storage, thus protecting data integrity.
Quorum doesn't prevent split-brain situations, but it does decide who is dominant and allowed to function in the cluster.
quorum can be determined by a combination of communicating messages via Ethernet and through a quorum disk.

22. What are Tie-breakers in Red Hat Cluster?

Tie-breakers are additional heuristics that allow a cluster partition to decide whether or not it is quorate in the event of an even-split - prior to fencing.
With such a tie-breaker, nodes not only monitor each other, but also an upstream router that is on the same path as cluster communications. If the two nodes lose contact with each other, the one that wins

is the one that can still ping the upstream router.That is why, even when using tie-breakers, it is important to ensure that fencing is configured correctly.
CMAN has no internal tie-breakers for various reasons. However, tie-breakers can be implemented using the API.

23. What is fencing in Red Hat Cluster?

Fencing is the disconnection of a node from the cluster's shared storage.
Fencing cuts off I/O from shared storage, thus ensuring data integrity.
The cluster infrastructure performs fencing through the fence daemon, fenced.
When CMAN determines that a node has failed, it communicates to other cluster-infrastructure components that the node has failed.
fenced, when notified of the failure, fences the failed node.

24. What are the various types of fencing supported by High Availability Add On?

Power fencing *— A fencing method that uses a power controller to power off an inoperable node.*
storage fencing *— A fencing method that disables the Fibre Channel port that connects storage to an inoperable node.*
Other fencing *— Several other fencing methods that disable I/O or power of an inoperable node, including IBM Bladecenters, PAP, DRAC/MC, HP ILO, IPMI, IBM RSA II, and others.*

25. What are the lock states in Red Hat Cluster?

A lock state indicates the current status of a lock request. A lock is always in one of three states:

Granted *— The lock request succeeded and attained the requested mode.*

Converting *— A client attempted to change the lock mode and the new mode is incompatible with an existing lock.*

Blocked *— The request for a new lock could not be granted because conflicting locks exist.*
A lock's state is determined by its requested mode and the modes of the other locks on the \ same resource.

26. What is DLM lock model?

DLM is a short abbreviation for Distributed Lock Manager.
A lock manager is a traffic cop who controls access to resources in the cluster, such as access to a GFS file system.GFS2 uses locks from the lock manager to synchronize access to file system metadata (on shared storage) CLVM uses locks from the lock manager to synchronize updates to LVM volumes and volume groups (also on shared storage)In addition, rgmanager uses DLM to synchronize service states. without a lock manager, there would be no control over access to your shared storage, and the nodes in the cluster would corrupt each other's data.

Chapter#29 – Kickstart Installation

1. What is Kickstart installation?

Installation of RedHat Linux in non-interactive mode is called the Kickstart installation.
Many system administrators would prefer to use an automated installation method to install RedHat Enterprise Linux on their machines. Using kickstart, a system administrator can create a single file containing the answer to all the questions that would normally asked during a typical installation.
Kickstart files can be kept on a single server system and read by individual computers during the installation. This installation method can support the use of a single kickstart file to install RedHat Enterprise Linux on multiple machines, making it ideal for network and system administrators.
The default Kickstart installation file is ***anaconda-ks.cfg****.*

2. What are the minimum requirements for kickstart installation?

(i) RedHat Enterprise Linux - 5, 6 or 7 ISO image file with full path.
(ii) Kickstart installation file like anaconda-ks.cfg or out custom kickstart installation file.
(iii) Copy the O/S ISO image file by configuring the kickstart.
(iv) Availability of installation media to remote systems through NFS, FTP or HTTP

3. How to setup the Kickstart installation server?

(i) Install the system-config-kickstart package by
 # yum install system-config-kickstart -y command.

(ii)Create a kickstart installation file in GUI mode.
 # system-config-kickstart (this command will display the kickstart configuration window)

(iii) Basic Configuration is the first option in the kickstart configuration window and we have to choose the following options in this.

- *(a) Select the default language (for example English).*
- *(b) Select the Keyboard type (for example US English).*
- *(c) Select the Time zone (for example Asia/Kolkata).*
- *(d) Type the Root password and Re-type the same to confirm the root password.*
- *(e) Select the Target Architecture (x86_64 or 32 bit)*

(iv) Installation Method is the second option.

- *(a) Installation Method. (Select any one option)*
  - *(1) Perform New Installation*
  - *(2) Upgrade an existing installation*
- *(b) Installation Source. (Select any one option)*
  - *(1) CD-ROM/DVD*
  - *(2) NFS*
  - *(3) FTP*
  - *(4) HTTP*
  - *(5) Hard Drive*

(v) Boot Loader options is the next option in kickstart configuration.
(a) Select Install New Boot Loader option.

(vi) Partition Information is the next option.
(a) Master Boot Record (Select any one option)
(1) Create Master Boot Record
(2) Do not create Master Boot Record
(b) Partitions (Select any one option)
(1) Remove all existing partitions
(2) Remove existing Linux partitions
(3) Preserve existing partitions
(c) Disk Label (Select any one option)
(1) Initialize the disk label
(2) Do not initialize the disk label
(d) Select Add button and select Mount point, File system type and Sizes to create the partitions.

(vii) Network Configuration is the next option.
(a)Select Add Network Device to add the NIC device, configure the IP address either DHCP or Static and select enable the NIC at boot time or not.

(viii) Authentication is the next option.
Select the authentication mechanism like Shadow passwords, NIS, LDAP or Kerberos... etc.,

(ix) Firewall Configuration is the next option.
Select whether activate the SELinux or not, Security Level and Firewall Information.

(x) Display Configuration is the next option.
Select the display configuration of the O/S either GUI or CLI mode.

(xi) Package Selection is the next option.
Select the required packages for installation.(we cannot select the packages in RHEL - 7)

(xii) and (xiii) Pre-Installation Scripts and Post-Installation Scripts are the last options.
If we have any Pre-installation or Post-installation scripts, then we have to specify the locations of those.

(xiv) Save this fie by select the Save option in File menu.

(xv) Exit from the Kickstart Configuration window by select the Quit option in File menu.

(xvi) Open the kickstart file and the default kickstart file at time by the following command.

 # vim -O <kickstart file><anaconda file>
Go to package section in anaconda file, copy the select the packages and paste them in the kickstart file.

(xvii) Check the kickstart file for syntax errors by # ksvalidator <kickstart file> command.

(xviii) Install the webserver package by # yum install httpd -y command.*

(xix) Copy the kickstart file in Document Root of the webserver and preserver the permissions.
 # cp -p <kickstart file> /var/www/html/

(xx) Restart the webserver deamons in RHEL - 6 and RHEL - 7.
 # service httpd restart (to restart the webserver deamon in RHEL - 6)
 # chkconfig httpd on (to enable the webserver deamon at next boot in RHEL - 6)
 # systemctl restart httpd (to restart the webserver deamon in RHEL - 7)
 # systemctl enable httpd (to enable the webserver deamon at next boot in RHEL - 7)

(xxi) Add the webserver service to IPtables and Firewall.
In RHEL - 6 :
 # setup
Select Firewall configuration -----> Select HTTP and HTTPS to the firewall
 # service iptables save
 # service iptables restart
 # chkconfig iptables on
In RHEL - 7 :
 # firewall-cmd --permanent --add-service=http
 # firewall-cmd --permanent --add-service=https
 # firewall-cmd --complete-reload

4. How to install on client system using kickstart file?

(i) Boot the client system using RHEL - 6 DVD and press ***Esc*** *key.*
(ii) Then it prompts us ***boot :*** *screen.*
(iii) Type the following information about the kickstart file, its server and also assign some IP address to the client system to communicate with kickstart server.
boot : linux ip=< IP address to the client> netmask=<netmask of that IP>
ks=ftp://< IP address of the kickstart server>/<kickstart file name with full path>
(press Enter key)
* *Then the installation will continue by taking the installation information from the kickstart file.*

5. In how many ways can we install RedHat Linux through network?

(i) FTP
(ii) NFS
(iii) HTTP
(iv) PXE

6. How to install RedHat Linux though FTP?

(i) First configure the FTP server and copy the entire RedHat Linux DVD in that FTP document root directory.
(ii) Installation of Linux through network requires one ***boot.iso*** *image or RHEL DVD.*

To make a DVD/Pendrive bootable using boot.iso image :

(a) Download the boot.iso image from redhat website.

 # cdrecord /root/boot.iso *(/root/boot.iso is the path of boot.iso image)*

(b) Copy the boot.iso image into DVD or pendrive.

 # dd if=/root/boot.iso of=/dev/sdb1 *(/dev/sdb1 is the address of the USB or pendrive)*

(iii) Boot the system with the above created boot.iso image and press ***Esc*** *key to get the*

boot : *prompt.*

(iv) Then execute the below command to install the O/S.

boot : linux askmethod *(Press Enter key)*

(v) Select the preferred language for installation (for example English).

(vi) Select the Keyboard layout as US.

(vii) Select the ***url****option for the installation media (for example FTP/NFS/HTTP).*

(viii) Select IPv4 or IPv6 to define network settings and select dynamic or static options.

(ix) Assign the same range IP address and netmask to the client system to communicate with server.

(x) Then specify the FTP server IP address and path of the installation media to install the O/S.

7. How to install RedHat Linux through NFS?

(i) Make an entry in /etc/exports to export the RHEL media.

 # vim /etc/exports

<installation media directory> <network ID>(rw, sync) (save and exit this file)

Example :

/var/ftp/pub/rhel6 172.25.9.0(rw, sync) (If the installation media is in /var/ftp/pub/rhel6)

(ii) Export the above NFS shared directory by ***# exportfs -rv*** *command.*

(iii) Then restart the NFS service by

 # service restart nfs *command and add the NFS to IPtables or firewall.*

(iv) Installation of Linux through network requires one ***boot.iso*** *image or RHEL DVD.*

To make a DVD/Pendrive bootable using boot.iso image :

(a) Download the boot.iso image from redhat website.

 # cdrecord /root/boot.iso *(/root/boot.iso is the path of boot.iso image)*

(b) Copy the boot.iso image into DVD or pendrive.

 # dd if=/root/boot.iso of=/dev/sdb1 *(/dev/sdb1 is the address of the USB or pendrive)*

(v) Boot the system with the above created boot.iso image and press ***Esc*** *key to get the*

boot : *prompt.*

(vi) Then execute the below command to install the O/S.

boot : linux askmethod *(Press Enter key)*

(vii) Select the preferred language for installation (for example English).

(viii) Select the Keyboard layout as US.

(xi) Then select the ***NFS directory*** *option and specify the NFS server IP address and NFS shared directory and the installation will be done.*

8. How to install the RedHat Linux through HTTP?

(i) First install the http webserver by ***# yum install httpd* -y*** *command.*

(ii) Copy the entire RHEL DVD contents into ***/var/www/html/rhel6*** *by*

 # cp -rvpf /media/RHEL/*.* /var/www/html/rhel6

(iii) If not possible to do the above step2, then create a link between the /var/ftp/pub/rhel6 and /var/www/html by ***# ln -s /var/ftp/pub/rhel6 /var/www/html/rhel6*** *command.*

(iv) Restart the http services and add it to the firewall.

In RHEL - 6 :

 # service httpd restart (to restart the http service in RHEL - 6)
 # chkconfig httpd on (to enable the http service at next boot in RHEL - 6)
 # setup (through the setup command add the http service to the IP tables)
 # service iptables save (to save the iptables configuration)
 # service iptables restart (to restart the iptables service)

In RHEL - 7 :

 # systemctl restart httpd (to restart the http service in RHEL - 7)
 # systemctl enable httpd (to enable the http service at next boot in RHEL - 7)
 # firewall-cmd --permanent -add-service=http (to add the http service to the firewall in RHEL - 7)
 # firewall-cmd -complete-reload (to reload the firewall configuration)

(v) Installation of Linux through network requires one ***boot.iso*** *image or RHEL DVD.*

To make a DVD/Pendrive bootable using boot.iso image :

(a) Download the boot.iso image from redhat website.
 # cdrecord /root/boot.iso *(/root/boot.iso is the path of boot.iso image)*
(b) Copy the boot.iso image into DVD or pendrive.
 # dd if=/root/boot.iso of=/dev/sdb1 *(/dev/sdb1 is the address of the USB or pendrive)*

(vi) Boot the system with the above created boot.iso image and press ***Esc*** *key to get the* ***boot :*** *prompt.*

(vii) Then execute the below command to install the O/S.
boot : linux askmethod *(Press Enter key)*

(viii) Select the preferred language for installation (for example English).
(ix) Select the Keyboard layout as US.
(xii) Select the ***url****option for the installation media and specify the http or https IP address and location.*

Example :

http or https://172.25.9.11/rhel6

(xi) Then installation of RedHat Linux will be done through HTTP.

9. What is PXE installation and what are it's requirements?

Automatic Installation of RHEL from the Network is called PXE installation.
This is also called as un-attended
installation. The means nobody interaction is required in the installation process.
PXE stands for ***Pre Execution****. The PXE does not requires a RHEL DVD or any boot.iso image.*

The requirements for PXE server :

(i) Static network at server side.
(ii) DHCP server should be configured on the server.
(ii) FTP server should be configured on the server.

(iv) Yum server should be configured on the server.
(v) TFTP server should be configured on the server.
(vi) Create the kickstart installation file.
** If all the above 5 servers are configured in one server, that server should be called as PXE server.*

10. How to configure the PXE server and how to install RedHat from PXE server?

(a) Put the RHEL - 6 DVD into the DVD drive and go to Packages directory.

```
# cd /media/RHEL6/Packages
```

(b) Install the vsftpd package to configure the FTP server.

```
# rpm -ivh vsftpd*
```

(b) Copy the entire RHEL - 6 DVD

contents into the /var/ftp/pub/rhel6 directory.

```
# cp -rvpf /media/RHEL6/*.* /var/ftp/pub/rhel6
```

(c) Restart, enable the ftp service at next boot, add the service to IP tables and restart the IP tables.

```
# service vsftpd restart
# chkconfig vsftpd on
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 21 -j ACCEPT
# iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 21 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 20 -j ACCEPT
# iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 20 -j ACCEPT
# service iptables save
# service iptables restart
# chkconfig iptables on
```

(d)Configure the network as static by

```
# setup command and restart the network and NetworkManager.
```

(e)Configure the yum server.

```
# vim /etc/yum.repos.d/linux.repo
  [linux]
  name=Linux yum server
   baseurl=ftp://172.25.9.11/pub/rhel6          (Specify the FTP server IP address)
   gpgcheck=0
   enabled=1                                                    (save and exit the file)
# yum clean all
# yum repolist
```

(f) Configure the DHCP server.

```
# yum install dhcp* -y
# cp -rvpf /usr/share/doc/dhcp-4.1.1/dhcpd.conf.sample /etc/dhcp/dhcpd.conf
# vim /etc/dhcp/dhcpd.conf
  Go to line number 47 and edit the line as below.
  subnet 172.25.9.0 netmask 255.255.255.0 {
      range 172.25.9.50 172.25.9.200;
* comment on next two lines
  option routers 172.25.9.11;
  option broadcast-address 172.25.9.255;
default-lease-time 600;
```

max-lease-time 7200;
allow booting;
allow bootp;
next-server 172.25.9.11;
filename "Pxelinux.0";
authoritative; *(save and exit this file)*

 # service dhcpd restart
 # chkconfig dhcpd on
 # iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 67 -j ACCEPT
 # iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 68 -j ACCEPT
 # iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 67 -j ACCEPT
 # iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 68 -j ACCEPT

(g)Configure the TFTP server.

 # yum install tftp syslinux* -y*
 # vim /etc/xinetd.d/tft
** Go to disable=yes line and make it as no* *(save and exit this file)*
 # cp -rvpf /media/RHEL6/isolinux/.* /var/lib/tftpboot*
 # mkdir /var/lib/tftpboot/pxelinux.cfg
 # cp /var/lib/tftpboot/isolinux.cfg /var/lib/ftfpboot/pxelinux.cfg/default
 # cp -rvpf /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot
 # service xinetd restart
 # chkconfig xinetd on
 # iptables -A INPUT -m state --state NEW -m tcp -p tcp --deport 69 -j ACCEPT
 # iptables -A OUTPUT -m state --state NEW -m tcp -p tcp --deport 69 -j ACCEPT

(h) Create the kickstart file

 # yum install system-config-kickstart -y
 # system-config-kickstart (create a kickstart file and save it in /var/ftp/pub directory)
 # ksvalidator /var/ftp/pub/ks.cfg

(i) Specify the kickstart file location in pxelinux.cfg file.

 # vim /var/lib/tftpboot/pxelinux.cfg/default
** Go to line 19 and edit the lines as below.*
menu label ^ PXE SERVER
menu default
kernel vmlinuz
append initrd=initrd.img linux ks=ftp://172.25.9.11/pub/ks.cfg *(save and exit this file)*

(j) Restart all the services once again.

 # service network restart
 # chkconfig network on
 # service vsftpd restart
 # chkconfig vsftpd on
 # service dhcpd restart
 # chkconfig dhcpd on
 # service xinetd restart
 # chkconfig xinetd on

Chapter#30 – Server Performance

Examples of top command

top is one of the tool for monitoring system usage and also to make any change for improving system performance.

Introduction:

The top program provides a dynamic real-time view of a running system. It can display system summary information as well as a list of tasks currently being managed by the Linux kernel. The types of system summary information shown and the types, order and size of information displayed for tasks are all user configurable and that configuration can be made persistent across restarts.

1. Without any arguments :

```
# top
top - 17:51:07 up 1 day,  2:56, 27 users,  load average: 5.33, 29.71, 28.33
Tasks: 1470 total,   1 running, 1469 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.1%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:  264114424k total, 253006956k used, 11107468k free,    66964k
buffers
Swap: 33554424k total,     3260k used, 33551164k free, 245826024k cached

PID   USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
1960  deepak  15   0 30452 3220 1540 R  2.3  0.0   0:00.78 top
2457  root      11  -5     0    0    0 S  2.3  0.0  11:36.93 kacpid
2493  pmartprd  16   0 1397m 289m 9.8m S  0.3  0.1  18:36.07 pmrepagent
4639  pmartprd  15   0  787m  54m 4080 S  0.3  0.0   5:19.55 pmserver
14402 root      RT   0  151m 5256 2872 S  0.3  0.0   1:41.40  multipathd
17886 root     10  -5     0    0    0 S  0.3  0.0   0:07.41 kondemand/11
```

Generally we use top without any arguments, but the magic is mostly done from the top command line which must of us skip. Well before taking you to that part let me explain you the various system related features which are shown by top command.

***NOTE:** You can enable or disable the marked blue line by pressing "**I**" once top is running.*

```
top - 17:51:07 up 1 day, 2:56, 27 users,  load average: 5.33, 29.71,
28.33
Tasks: 1470 total,   1 running, 1469 sleeping,   0 stopped,   0
zombie
Cpu(s):  0.0%us,  0.1%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi, 0.0%si,
0.0%st
Mem:  264114424k total, 253006956k used, 11107468k free,    66964k
buffers
Swap: 33554424k total,     3260k used, 33551164k free, 245826024k
cached
```

Explanation: *This line tells you about the uptime of your system along with load average value.*

NOTE: *You can enable/disable the marked blue line by pressing "**t**".*

```
top - 17:51:07 up 1 day,  2:56, 27 users,  load average: 5.33, 29.71, 28.33
Tasks: 1470 total,   1 running, 1469 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.1%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  264114424k total, 253006956k used, 11107468k free,    66964k buffers
Swap: 33554424k total,     3260k used, 33551164k free, 245826024k cached
```

Explanation: *This line gives us a brief detail of all the tasks running/sleeping/stopped currently in the system along with the CPU Usage*

Value	Meaning
us	user cpu time (or) % CPU time spent in user space
sy	system cpu time (or) % CPU time spent in kernel space
ni	user nice cpu time (or) % CPU time spent on low priority processes
id	idle cpu time (or) % CPU time spent idle
wa	io wait cpu time (or) % CPU time spent in wait (on disk)
hi	hardware irq (or) % CPU time spent servicing/handling hardware interrupts
si	software irq (or) % CPU time spent servicing/handling software interrupts
st	steal time - - % CPU time in involuntary wait by virtual cpu while hypervisor is servicing another processor (or) % CPU time stolen from a virtual machine

NOTE: *You can enable/disable the marked blue line by pressing "**m**".*

```
top - 17:51:07 up 1 day,  2:56, 27 users,  load average: 5.33, 29.71, 28.33
Tasks: 1470 total,   1 running, 1469 sleeping,   0 stopped,   0 zombie
Cpu(s): 0.0%us, 0.1%sy, 0.0%ni,99.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
```

```
Mem: 264114424k total, 253006956k used, 11107468k free,    66964k buffers
Swap: 33554424k total,     3260k used, 33551164k free, 245826024k cached
```

Explanation: *The next line shows your memory(RAM and swap) usage and capacity.*

```
PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
13916 stmprd    18   0  903m 129m 9936 S 51.4  0.1   3:07.01 java
13921 stmprd    18   0  901m 128m 9936 S 49.8  0.0   3:02.92 java
13825 stmprd    18   0  951m 190m 9932 S 49.5  0.1   3:07.13 java
13856 stmprd    20   0  978m 197m 9936 S 49.2  0.1   3:05.89 java
13853 stmprd    18   0  921m 150m 9932 S 48.5  0.1   3:09.14 java
13875 stmprd    18   0  907m 132m 9940 S 48.5  0.1   3:09.49 java
13937 stmprd    25   0  926m 165m 9936 S 48.2  0.1   3:10.31 java
13919 stmprd    18   0  917m 153m 9936 S 47.5  0.1   3:05.92 java
```

```
13879  stmprd    25   0  921m 160m 9936 S 47.2     0.1   3:08.43    java
13908  stmprd    25   0  901m 131m 9932 S 47.2     0.1   3:12.23    java
13905  stmprd    25   0  907m 137m 9932 S 46.6     0.1   2:59.85    java
```

The left sections shows you the details of the process running along with the below details.

Fields/Column	Description
PID	Process Id
USER	The effective user name of the task's owner
PR	The priority of the task
NI	The nice value of the task. A negative nice value means higher priority, whereas a positive nice value means lower priority. Zero in this field simply means priority will not be adjusted in determining a task's dispatchability
%CPU	The task's share of the elapsed CPU time since the last screen update, expressed as a percentage of total CPU time.
%MEM	A task's currently used share of available physical memory
TIME+	Total CPU time the task has used since it started
S	The status of the task which can be one of: 'D' = uninterruptible sleep 'R' = running 'S' = sleeping 'T' = traced or stopped 'Z' = zombie
RES	The non-swapped physical memory a task has used
SHR	The amount of shared memory used by a task
Command	Display the command line used to start a task or the name of the associated program

2. Arrange Tasks with High to Low CPU Usage :

*Press "**P**" or "**shift+p**" once top is running to arrange all the tasks with **High to Low CPU Usage** as shown below.*

```
top - 18:03:00 up 1 day, 3:08,27 users, load average: 12.54, 32.34, 32.75
Tasks: 1485 total,   3 running, 1482 sleeping,   0 stopped,   0 zombie
Cpu(s): 41.2%us, 0.8%sy, 0.0%ni, 56.6%id, 1.4%wa, 0.0%hi, 0.0%si,  0.0%st
Mem:  264114424k total, 258863028k used, 5251396k free,    76308k buffers
Swap: 33554424k total,     3256k used, 33551168k free, 250950544k cached

PID    USER                PR      NI      VIRT        RES        SHR
S      %CPU       %MEM        TIME+          COMMAND
 9663      stmprd    22   0      902m  301m  9888  S 2578.3        0.1
2:27.04    java
32117      etlprd    18  -1      32416       5908  1716  R     6.2   0.0
0:04.84 cleanup_dirfile
10053      root       18  -1     27100       1936  1460  S     4.9    0.0
0:00.15    ps
5456 pmartprd  16   0      1182m       130m  8560  S  3.9     0.1
```

```
 38:39.72   pmserver
17492      deepak   16   0   30592      3388  1544  R     3.6   0.0
0:17.11    top
 2843      pmartprd  15   0      730m        48m   4052  S     3.3    0.0
4:40.33    pmserver
 2457      root       11  -5           0     0     0     S     2.9   0.0
11:42.39   kacpid
 3731      tdmsprd   15   0      370m        49m   32m   S     2.3   0.0
0:00.64    pmdtm.orig
```

3. Arrange Tasks with High to Low Memory Usage.

*Press "**M**" or "**shift+m**"once top is running to arrange all the tasks with **High to Low Memory Usage** as shown below.*

```
Top -18:04:26 up 1 day, 3:09, 27 users, load average: 37.12, 34.56, 33.44
Tasks: 1676 total,   1 running, 1675 sleeping,   0 stopped,   0 zombie
Cpu(s): 2.3%us,76.7%sy, 0.0%ni,19.7%id, 1.3%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  264114424k total, 262605184k used, 1509240k free,    77924k buffers
Swap: 33554424k total,     3256k used, 33551168k free, 252198368k cached

PID    USER              PR      NI      VIRT         RES         SHR
S      %CPU       %MEM        TIME+          COMMAND
1852   pmartprd  18   0       2005m       319m  4776  S     6.9   4.1
28:34.32    java
2493   pmartprd  16   0       1397m       289m  9.8m  S     0.0   4.0
18:37.79 pmrepagent
20557  etlprd    15   0 911m 201m  3024  S 0.0 3.0  17:09.02 pmdtm.orig
18778  root      RT   0 286m  188m  156m  S 0.0 2.1  13:24.98   aisexec
5456   pmartprd  15   0       1182m       130m  8560  S     6.2
1.1  38:40.58 pmserver
16004  etlprd   14  -1   179m  83m   2636  S     0.0   0.1   9:41.36    db2bp
11272  stmprd   25   0   906m        67m   9736  S     99.7        0.0
0:48.11      java
```

4. Change the nice value (priority) of any task

To understand what is nice value follow the below link

What is nice and how to change the priority of any process in Linux?

*Press "**r**" when top is running on the terminal. You should get a prompt as shown below in blue color.*

```
top - 18:08:38 up 115 days, 8:44, 4 users, load average: 0.03, 0.03, 0.00
Tasks: 325 total,   2 running, 323 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.1%us, 6.4%sy, 0.0%ni, 93.3%id, 0.3%wa, 0.0%hi, 0.0%si,  0.0%st
Mem:  49432728k total,  2063848k used, 47368880k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297572k cached
PID to renice: 1308 [Hit Enter]

PID    USER            PR      NI      VIRT         RES         SHR          S
%CPU       %MEM        TIME+          COMMAND
5359   root       39       19          0  0     0     R     100.1       0.0
94:31:35    kipmi0
```

```
1308   deepak   16   0    29492 2292  1512  S     0.7   0.0    0:00.33    top
6116   root      15    0  369m      30m   11m   S     0.7   0.1   77:24.97
cimserver
```

*Give the **PID** whose nice value has to be changed and hit "Enter". Then give the **nice value** for the PID*

```
top - 18:08:38 up 115 days, 8:44, 4 users, load average: 0.03, 0.03, 0.00
Tasks: 325 total,   2 running, 323 sleeping,   0 stopped,   0 zombie
Cpu(s): 0.1%us, 6.4%sy,  0.0%ni, 93.3%id, 0.3%wa, 0.0%hi, 0.0%si,  0.0%st
Mem:  49432728k total,  2063848k used, 47368880k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297572k cached
```

***Renice PID 1308 to value:** -1 [Hit Enter]*

```
PID     USER              PR      NI      VIRT        RES         SHR
S      %CPU      %MEM       TIME+          COMMAND
  5359  root       39       19         0      0 0     R       100.1    0.0
9431:35     kipmi0
1308   deepak  16   0    29492       2292  1512  S     0.7   0.0
0:00.33     top
6116   root       15    0     369m       30m   11m   S     0.7   0.1
77:24.97 cimserver
```

Verify the changes :

```
top -18:09:06 up 115 days, 8:45,  4 users, load average: 0.13, 0.06, 0.01
Tasks: 325 total,   1 running, 324 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.1%sy, 0.0%ni, 9.8%id, 0.1%wa, 0.0%hi, 0.0%si,  0.0%st
Mem:  49432728k total,  2063276k used, 47369452k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297588k cached
```

```
PID     USER              PR      NI      VIRT        RES         SHR
S      %CPU      %MEM       TIME+          COMMAND
1308   deepak  15  -1    29492       2292  1512  S     0.7   0.0   0:00.42
top
5359   root       34       19      0     0     0     S     0.7   0.0
9431:42     kipmi0
1      root  15   0 10352     692   580   S     0.0   0.0   0:02.16    init
2      root    RT  -5   0     0     0     S 0.0 0.0   0:02.37 migration/0
3           root       34  19          0    0    0      S     0.0   0.0
0:00.00 ksoftirqd/
```

5. Kill any task

*Press "**k**" on the terminal when top is running. You should get a prompt as shown below in blue color*

```
top - 18:09:31 up 115 days, 8:45, 4 users, load average: 0.08, 0.05, 0.01
Tasks: 325 total,   1 running, 324 sleeping,   0 stopped,   0 zombie
Cpu(s):0.1%us, 0.1%sy, 0.0%ni,99.8%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  49432728k total,  2062036k used, 47370692k free,   310072k buffers
Swap:  2097144k total, 0k used, 2097144k free, 1297596k cached
PID to kill:1308
```

```
PID     USER              PR      NI      VIRT        RES         SHR
S      %CPU      %MEM       TIME+          COMMAND
```

```
5359   root       34   19     0        0     0     S     1.3   0.0
9431:42           kipmi0
6460   root  24   0  79m 30m 3976  S     1.0   0.1 79:04.77          java
 1308  deepak     15   -1    29492      2292  1512  S     0.7   0.0
 0:00.49           top
1434   root       15   0     29492      2288  1516  R     0.7   0.0
0:00.13           top
 top - 18:09:31 up 115 days, 8:45, 4 users, load average: 0.08, 0.05,
0.01
 Tasks: 325 total,   1 running, 324 sleeping,   0 stopped,   0 zombie
 Cpu(s): 0.1%us, 0.1%sy, .0%ni, 99.8%id,  0.1%wa, 0.0%hi,  0.0%si,
 0.0%st
 Mem:  49432728k total,  2062036k used, 47370692k free,   310072k buffers
 Swap:  2097144k total,        0k used,  2097144k free,  1297596k cached
Kill PID 1308 with signal [15]: [Hit Enter for default]
PID    USER              PR      NI      VIRT        RES         SHR
S      %CPU      %MEM        TIME+          COMMAND
 5359  root       34   19     0        0     0     S     1.3   0.0
9431:42     kipmi0
 6460  root       24    0    179m       30m   3976  S     1.0   0.1
79:04.77          java
1308   deepak     15   -1    29492      2292  1512  S     0.7   0.0
0:00.49           top
```

6. View all the processes running by a user

*Press "**u**" on the terminal when top is running. You should get a prompt as shown below in blue color*

```
top - 18:12:24 up 115 days,  8:48,  4 users,  load average: 0.06, 0.05,
0.00
Tasks: 328 total,   1 running, 327 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.4%sy,  0.0%ni, 99.6%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:  49432728k total,  2063268k used, 47369460k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297660k cached
Which user (blank for all): deepak [Hit Enter]

PID    USER              PR      NI      VIRT        RES         SHR
S      %CPU      %MEM        TIME+          COMMAND
1729   root       15    0    29488      2196  1432  R     2.0   0.0
0:00.01     top
1      root       15   0     10352      692   580   S     0.0   0.0
0:02.16     init
2      root       RT   -5     0        0     0     S     0.0   0.0
0:02.37     migration/0
3      root       34   19     0        0     0     S     0.0   0.0
0:00.00     ksoftirqd/0
4      root       RT   -5     0        0     0     S     0.0   0.0
0:00.00     watchdog/0

top - 18:12:41 up 115 days,  8:48,  4 users,  load average: 0.04, 0.05,
0.00
Tasks: 328 total,   1 running, 327 sleeping,   0 stopped,   0 zombie
```

```
Cpu(s):  0.0%us,  0.1%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:  49432728k total,  2062356k used, 47370372k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297672k cached

PID    USER              PR      NI      VIRT        RES        SHR
S      %CPU      %MEM        TIME+          COMMAND
1561   deepak     17    0     3984        780   468   S     0.0   0.0
0:0.00      man
1564   deepak     19    0     8704        964   816   S     0.0   0.0
0:0.00            sh
1566   deepak     23    0     8704        464   316   S     0.0   0.0
0:0.00            sh
1571   deepak     16    0     8452        892   712   S     0.0   0.0
0:0.01            less
31328  deepak     15    0     110m  2348  1264  S     0.0   0.0
0:0.20            sshd
31329  deepak     16    0     27676       2564  1816  S     0.0   0.0
0:0.02      bash
31422  deepak     15    0     109m  2360  1260  S     0.0   0.0
0:0.14      sshd
31423  deepak     15    0     27548       2500  1784  S     0.0   0.0
0:0.02      bash
```

7. Change delay between terminal refresh

By default the top terminal is set for auto refresh after every 3 seconds but if you want you can change it as per your requirement.

*Press "**d**" when top is running. You should get a prompt as shown below in blue color.*

```
top - 18:14:55 up 115 days,  8:50,  4 users,  load average: 0.01, 0.04,
0.00
Tasks: 328 total,   1 running, 327 sleeping,   0 stopped,   0 zombie
Cpu(s): 0.0%us, 0.1%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:  49432728k total,  2063828k used, 47368900k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297728k cached
Change delay from 3.0 to:2.0 [Hit Enter]

PID    USER          PR      NI      VIRT        RES        SHR          S
%CPU      %MEM        TIME+          COMMAND
 5359  root       34    19          0     0     0     S     0.7   0.0
 9431:58    kipmi0
 1795  root       15    0 29492 2300 1524     R     0.3   0.0
 0:00.20           top
      1     root       15    0 10352  692     580   S     0.0   0.0
 0:02.16           init
```

Verify the changes. You must see the screen buffer getting refresh much earlier or just to verify you can provide a higher value of delay and observer the refresh rate on the terminal

8. No. of task to be displayed

By default this option is set to unlimited that is the reason your terminal is fully covered with list of tasks when you run the top command. Any how you can list the no of tasks to be visible once you run top command.

*Press "**n**"when top is running. You should get a prompt as shown below in blue color*

```
top - 18:18:07 up 115 days,  8:54,  4 users,  load average: 0.01, 0.03,
0.00
Tasks: 328 total,   1 running, 327 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.2%sy,  0.0%ni, 99.7%id,  0.1%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:  49432728k total,  2063348k used, 47369380k free,   310072k buffers
Swap:  2097144k total,        0k used,  2097144k free,  1297804k cached
Maximum tasks = 0, change to (0 is unlimited):2 [Hit Enter]
PID    USER              PR      NI      VIRT      RES         SHR
S      %CPU      %MEM       TIME+          COMMAND
 5359  root       34    19         0     0     0     S     2.3   0.0
 9432:08    kipmi0
 0.00
 Tasks: 318 total,   1 running, 317 sleeping,   0 stopped,   0 zombie
 Cpu(s):  0.0%us,  0.1%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
 Mem:  49432728k total,  2051952k used, 47380776k free,   310176k buffers
 Swap:  2097144k total,        0k used,  2097144k free,  1293800k cached
 PID   USER              PR      NI      VIRT     RES         SHR          S
%CPU      %MEM       TIME+          COMMAND
5359   root       34  19          0     0     0     S     1.0   0.0
9502:15     kipmi0
25009 prasadee    15   0 29492 2280 1516  0.0      0:01.88          top
```

9. View live individual CPU processor performance :

By default top command shows you the average of all the available CPUs in the machine.

*In case you want to see report of all the individual CPUs press "**1**" once you are running top command and you will get to see something like below*

```
top - 00:00:58 up 215 days,13:36, 5 users, load average: 4.07, 4.04, 4.00
 Tasks: 339 total,   5 running, 334 sleeping,   0 stopped,   0 zombie
 Cpu0  :  0.0%us,  0.2%sy,  0.0%ni, 99.8%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
 Cpu1  :  0.0%us,  0.4%sy,  0.0%ni, 99.6%id,  0.0%wa,  0.0%hi,  0.0%si,
 Cpu7  :  0.1%us,  1.4%sy,  0.0%ni, 98.5%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
 Mem:  49432728k total, 11891852k used, 37540876k free,  7996596k buffers
 Swap:  2097144k total,        0k used,  2097144k free,  1850540k cached
 PID   USER              PR      NI      VIRT        RES         SHR
S      %CPU      %MEM       TIME+          COMMAND
23102  root       25    0     23724      2024  1168  R     100.1      0.0
64446:36          pvs
23338  root       25    0 23724 2028 1168 R  100.1  0.0 128828:38 pvs
```

10. Add a new field in top output :

By default you see limited set of output when you use the top command. But apart from those there are a other list of field which can be added to the top output. To view all the list f field which can be added follow the below steps.Run top command and then,

*Press "**f**" which will take you the list of available fields under top command.*

All the field initials stated in BLOCK letters are visible by default when you issue top command. To add a new field press the field initial as shown in the first column.

```
* A: PID      =   Process Id                 0x00000001       PF_ALIGNWARN
* E: USER     =     User Name                              0x00000002
PF_STARTING
* H: PR     =     Priority              0x00000004       PF_EXITING
* I: NI       =   Nice value            0x00000040       PF_FORKNOEXEC
* O: VIRT     =   Virtual Image (kb)    0x00000100       PF_SUPERPRIV
* Q: RES      =   Resident size (kb)          0x00000200       PF_DUMPCORE
* T: SHR      =   Shared Mem size (kb)       0x00000400       PF_SIGNALED
* W: S        =   Process Status               0x00000800     PF_MEMALLOC
* K: %CPU     =     CPU usage    0x00002000     PF_FREE_PAGES (2.5)
* N: %MEM    =     Memory usage (RES)    0x00008000       debug flag (2.5)
* M: TIME+   = CPU Time, hundredths   0x00024000   special threads (2.5)
b: PPID      =   Parent Process Pid 0x001D0000    special states (2.5)
c: RUSER     =     Real user name 0x00100000  PF_USEDFPU (thru 2.4)
d: UID       =     User Id
f: GROUP     =     Group Name
g: TTY       =     Controlling Tty
 j: P        =     Last used cpu (SMP)
* P: SWAP     =     Swapped size (kb)
 l: TIME     =     CPU Time
 r: CODE     =     Code size (kb)
 s: DATA     =     Data+Stack size (kb)
 u: nFLT     =     Page Fault count
 v: nDRT     =     Dirty Pages count
 y: WCHAN      =  Sleeping in Function
 z: Flags     =     Task Flags <sched.h>
* X: COMMAND    =      Command name/line
```

*For example to add "**swap**" field press "**p**" (in small letters). As soon as you press "**p**" it should turn into block letter notifying that it has been added to top output.Once done hit enter and it will take you back to top output*

You should see something like below screen

```
  PID   USER PR   NI  VIRT   RES  SHR  S   %CPU  %MEM TIME+
COMMAND
20472 prasadee    15   0 30748 2412 1620     R     0.8   0.0
0:00.43     27m top
22568  root       17   0  296m 5300 3536     S     0.4   0.1
3:00.30 291m eventlogd
 0:00.00          0 watchdog/1
8      root       RT   -5         0    0     0     S     0.0   0.0
```

Chapter#31 – General Questions

1. Tell me about yourself ?

(i) Tell your personal details
(ii) Technical (Educational details)

2. Tell me about your profile?

(i) Tell your personal details.
(ii) Educational details.
(iii) Work history (previous companies).
(iv) Profile (Present company) :
*(a) **Coming to Linux** : (upto till date)*
(1) O/S installation.
(2) File system creation.
(3) User administration like user creation, user permissions, profiles, setting environment to user, giving special permissions (sudo and ACLs) to them and user troubleshooting issues like user unable to login password requests.
(4) Hardware related issues like adding disks, NIC cards, processor replacement, memory replacement, increase memory and power supply replacement, ...etc.,
(5) Network related issuesproviding networking,setting NIC card parameters,troubleshooting issues.
(6) Some internal backups.
(7) O/S patching and package administration whenever needed using rpm and yum.
(8) I also supports process related issues like memory utilization full (90%), CPU utilization full (90%) and file system full, ...etc.,
(9) I also support for system troubleshooting issues like system not responding, node down, starting and stopping services and deamons.

*(b) **Coming to Veritas Volume Manager** : (from the last 1 year)*
(1) We get requests from production, database, Q A people like creating volumes, file system creation,increase and (or) decrease the volume sizes, provide permissions, redundancy, put the volume into cluster to provide high availability,
(2) sometimes destroy or remove the volumes, backup and restore whenever necessary,
(3) We also get some troubleshooting issues like volume not started, volume not accessible, file system crashed, mount point deleted, disks failed, volume manager deamons are not working, configuration files missed, crashed, disk groups not deporting and not importing, volume started but users are unable to access file systems on those volumes..etc.,

*(c) **Coming to Veritas Cluster** : (from 6 months)*
(1) We get requests like node adding, resource adding, service group adding, adding service groups and resources to existing service groups, mount points adding, adding NIC cars, IP ddresses, adding volumes, disk groups, freezing and unfreezing services groups and also

get some troubleshooting issues like cluster not running, if resources faulted then restart the service groups, communication failed between two systems, Gab is not running, llt not running, and configuration files main.cf crashed or missed and resources are not started, ... etc.
(d) I also write small scripts to perform internal routine jobs, document preparation, handover mails checking, how many tickets issued, how many tickets solved and how many jobs pending, ...etc.,
(e) I also supports in application deployment, database deployment and others.

3. What are the tools you are using?

(i) netstat, vmstat, iostat, nmap and top for performance monitoring tools.
(ii) cron and at for job scheduling.
(iii) Remedy tool for ticketing system.
(iv) Veritas Netbackup, Tivoli, ... etc., for backing purpose
(v) Outlook for internal mailing.

4. What are the storage boxes using?

(i) NetApps, VMC, Clarian and EMC2.
(ii) Emulex, Qlogic (HBA cards).

5. What are the Applications are you using?

(i) Databases (Oracle 10g, 11g and Mysql).
(ii) Oracle Applications like ERP packages (Oracle 11i and 12).
(iii) SAP applications.
(iv) Datawarehousing, ...etc.,

6. What is your company hierarchy?

Me -----> Team Lead or Tech Lead -----> Manager -----> Delivery Manager -----> Asia head

7. What level are you supporting?

Linux Administrator as Level 2.

8. What are your shift timings?

General shift -----> 09:00 - 18:00 hrs.
Shifts : One shift from USA and two shifts from India operations upto last 2 months and now all the operations are from India only and data centre operations from USA only.
1 st shift from 07:00 - 15:00 hrs, 2 nd shift from 15:00 - 23:00 hrs, 3 rd shift from 21:00 - 07:00 hrs.

9. What is your team size?

Total 18 members. For each shift 5 members each and 3 members on weekly off.

10. What about tickets issues and tickets frequency?

(i) 7 - 8 tickets daily and Max. 10 per day.
In those 85 - 90% are CPU utilization full, memory full, file system full, login problems and sometimes node down issues.

(ii) General tickets severity - 3, severity - 2, severity - 1.
We are not resolved severity level - 1 tickets.
(iii) Incidents :
Severity level - 1 should be solved within 1 hour (Immediate).
Severity level - 2 should be solved within 6 hours.
Severity level - 1 should be solved within 24 hours.
Severity level - 1 should be solved within 2 days.
Request priority ----> High, medium and low

11. What is your notice period?

25 - 30 days.

12. Any Mail ids?

Internal mail id (mails won't come from outside and go to outside).

13. Are you contract or permanent? And why are you changing?

Permanent in XXXXXXXXXX Pvt limited. I am looking the company which provides high availability on cloud, virtualization and storage environments to enhance my knowledge and better career growth.

14. What are the projects are you dealing?

(i) Databases.
(ii) Banking.
(iii) Finance.
(iv) Logistics.
(v) Hotel and Tourism, ...etc.,

15. How many servers are you handling?

Total 600 systems.
200 physical systems and remaining 400 systems are in virtualization environment.

550 for Linux	*10 for Windows*	*10 for Application Development*	*20 for Quality & Internal Testing*	*10 under transition*

16. What is your environment?

(i) Development upto 10 servers
(ii) Quality Assurance or Quality testing upto 20 servers.
(iii) User Authentication (U A) upto 10 servers.
(iv) Production upto 550 servers.
(v) Under building 10.

17. How to handover the shift?

* *Mail to reliever.*
* *Direct to reliever.*

18. Can you contact the data centre?

(i) It depends on the severity.

(ii) If the situation is emergency, then we will call the data centre by phone.
(iii) If the situation is non - emergency then we will mail to the data centre people.

19. What is server hardening?

(i) To checking our system is reaching to standards required by the organization.
(ii) That is minimum password length, minimum size of root partition.
(iii) Minimum free space and password expiry and all other security standards.

20. What are decommission and recommission?

(i) Normally servers should be changed every 5 - 6 years because of performance degradation as per standards of the company.
(ii) Decommission means the process of removing the old system from the production environment and Recommission means the process of putting the new system into the production environment.
(iii) We are not dedicated for decommission. We do decommission along with our routine work.
(iv) Login as root though console.
(v) First inform or raise the ticket to monitoring team to ignore the alerts.
(vi) Stop the application and databases.
(vii) Stop the cluster and Volume Manager.
(viii) Unmount the file system.
(ix) After that we should put the system for one week.
(x) We will inform or raise the ticket to the network team to release the ports belonging to that system.
(xi) Finally we inform to the data centre people to remove the cables from that system.

21. Explain backup and what is your backup policy?

(i) Backup means taking a copy of the existing system and restore when the system is formatted or crashed.

(ii) In backup environment normally we have 3 servers.
(a) Master Server (1 or 2 systems).
(b) Media Server (1 or 2 systems).
(c) Client Server (1 or 2 systems).

(iii) In our organization we used to take the backup in Media Server.

(iv) Backup fails means production server may down or media server may be in down, file system may not be available or backup tool port number may be blocked.

(v) Backup can be taken in 3 types.
(a) Application Backup (Application people will take).
(b) File system (O/S) backup (System Administrators will take).
(c) Database backup (Database Administrators will take).

(vi) Backup is automated though crontab or separate backup tools like Veritas Net backup and Tivoli, ...etc.,

(x) The crontab will not inform the failed backup. But Veritas Net backup and Tivoli tools will send messages about backup fails and why the backup is failed because these tools will generate the failed backup log files.

(viii) If any files are open in the production server, the backup may be failed. So, check any files opened or not by # lsof or # fuser -cv <file system> commands.

(ix) Sometimes the script in Veritas Net backup or Tivoli tools may be corrupted or not running, then restore those scripts from backup or we need manually deport & import and take backup.

(x) Sometimes backup failed due to backup port no. 13782 may be not working or in blocked state. It can be checked by # netstat -ntulp | grep 13782 command.

(xi) If the media server and production server are not in the same domain, then backup may be failed. (ie., production server domain name may be changed but no intimation to backup team about that change, so media server is in another domain).

Backup Procedure :

(i) Deport the disk group on production server.
(ii) Import the disk group on backup (media) server.
(iii) Join the disk group with media server.
(iv) Sync the data with production server.
(v) Take the backup.
(vi) split the disk group from media server.
(vii) Join the disk group with production server.
(viii) Deport the disk group from media server.
(ix) Import the disk group on production server.

Backup policy :

(i) Complete (full) backup (every month ie., once in a month).
(ii) Incremental backup (Daily).
(iii) Differential or cumulative backup (every week end).

22. How to troubleshoot if the file system is full?

(i) First check whether the file system is O/S or other than O/S.

(ii) If it is other than O/S, then inform to that respective teams to house keep the file system (ie., remove the unnecessary files in those file system).

(iii) If not possible to house keep then inform to different teams (raise the CRQ (Change Request)) for increasing the file system.

(a) First take business approval and raise the CRQ to monitoring team to ignore the alerts from the system, stop the application team to stop the application and database team to stop the database.
(b) Normally team lead or tech lead or manager will do this by initiate the mail thread.
(c) We will do this on weekend to reduce the business impact.

(iv) First take a backup of the file system then unmount the file system.

(v) Remove that partition and again create that file system with increased size, then mount again that file system and restore the backup.

(vi) If the file system belongs to system log files or other log files and not to delete then they requested us to provide one Repository server (only for log files). Normally one script will do automatically redirect the log files to that repository server.

(vii) Sometimes we will delete file contents not the files to reduce the file sizes. For that we execute the command ***# cat /dev/null ><file name with path>*** *ie., nullifying the files.*

(ix) If it is root file system or O/S file system,
(a) may be ***/opt*** *full or may be* ***/var*** *full or may be* ***/tmp*** *full*
(b) In ***/var/log/secure*** *or* ***/var/log/system*** *or* ***/var/tmp*** *files may be full. If those files are important then redirect them to other central repository server or backup those files and nullifying those files.*
(c) If ***/home*** *directory is present in root (/) file system then this file system full will occur. Generally* ***/home*** *will be separated from root file system and created as separate* ***/home*** *file system. If* ***/home*** *is in root (/) as a directory then create a separate file system for* ***/home*** *and copy those files and directories belongs to* ***/home*** *and remove that* ***/home*** *directory.*
(d) If root (/) is full then cannot login to the system. So, boot with net or CDROM in single user mode and do the above said.
(x) Normally if file system is other than O/S then we will inform to that respective manager or owner and take the permissions to remove unnecessary files through verbal permission or CRQ .

23. CPU utilization full, how to troubleshoot it?

(a) Normally we get these scenarios on weekends because backup team will take heavy backups.
(b) First check which processes are using more CPU utilization by # top and take a snap shot of that user processes and send the snap shot and inform to that user to kill the unnecessary process.
(b) If those processes are backups then inform to the backup team to reduce the backups by stopping some backups to reduce the CPU utilization.
(c) Sometimes in peak stages (peak hours means having business hours) CPU utilization will full and get back to the normal position automatically after some time (within seconds). But ticket raised by monitoring team. So, we have to take a snap shot of that peak stage and attach that snap shot to the raised ticket and close that ticket.
(d) Sometimes if heavy applications are running and not to kill (ie., business applications), then if any spare processor is available or other low load CPUs available then move those heavy application processes to those CPUs.
(e) If CPUs are also not available then if the system supports another CPU then inform to the data centre people or CPU vendor to purchase new CPU though Business approval and move some processes to the newly purchased CPUs.

24. How to troubleshoot when the system is slow?

(a) System slow means the end users response is slow.

(b) Check the Application file system, CPU utilization, memory utilization and O/S file system utilization.
(c) If all are ok, then check network statistics and interfaces whether the interfaces are running in full duplex mode or half duplex mode and check whether the packets are missing. If all are ok from our side then,
(d) Inform to network team and other respective teams to solve this issue.

25. How to troubleshoot if the node is down?

(a) Check pinging the system. If pinging, then check whether the system is in single user mode or not.
(b) If the system is in single user mode then put the system in multi user mode ie., default run level by confirming with our team whether system is under maintenance or not.
(c) Check in which run level the system is running. If it is in init 1 it will not be able to ping. If it is in init s then it will ping.
(d) In this situation also if it is not pinging then try to login through console port. If not possible then inform to data centres people to hard boot the system.
(d) If connected through console port then we may get the console prompt.

26. How to troubleshoot if the memory utilization full?

(a) Check how much memory is installed in the system by # dmidecode -t memory command.
(b) Check the memory utilization by # vmstat -v command.
(c) Normally application or heavy backups utilize more memory. So, inform to application team or backup team or other teams which team is utilizing the more memory to reduce the processes by killing them or pause them.
(d) Try to kill or disable or stop the unnecessary services.
(e) If all the ways are not possible then inform to team lead or tech lead or manager to increase the memory (swap space). If it is also not possible then taking higher authority's permissions to increase the physical memory. For those we contact the server vendor and co-ordinate with them through data centre people to increase the RAM size.

27. How to replace the failed hard disk?

(a) Check whether the disk is failed or not by # iostat -En | grep -i hard/soft command.
(b) If hard errors are above 20 then we will go for replacement of the disk.
(c) If the disk is from SAN people then we will inform to them about the replacement of the disk. If it is internal disk then we raise the CRQ to replace the disk.
(d) For this we will considered two things.
(i) whether the system is within the warranty.
(ii) without warranty.
(f) We will directly call to the toll free no. of the system vendor and raise the ticket. They will issue the case no. This is the no. we have to mention in all correspondences to vendor regarding this issue.
(g) If it is having warranty they asks rack no. system no. and other details and replace the hard disk with co-ordinate of the data centre people.
(h) If it is not having warranty, we have to solve the problem by our own or re-agreement to extend the warranty and solve that problem.

28. How to replace the processor?

(a) Check the processor's status using # lscpu or # dmidecode -t processor commands.

(b) If it shows any errors then we have to replace the processor.
(c) Then raise the case to vendor by toll free no. with higher authorities permission.
(d) The vendor will give case no. for future references.
(e) They also asks rack no. system no. of the data centre for processor replacement.
(f) We will inform to the Data centre people to co-ordinate with vendor.

29. How replace the failed memory modules?

Causes :

(a) The system is continuously rebooting .
(b) When in peak business hours, if the heavy applications are running the system get panic and rebooted. This is repeating regularly.

Solution :

(a) First we check how much RAM present in the system with # dmidecode -t memory command.
(b) Then we raise the case to vendor with the help of higher authorities.
(c) Then the vendors will provide the case no. for future reference.
(d) They will also asks rack no. system no. to replace the memory.
(e) we will inform the data centre people to co-ordinate with the vendor.

30. What is your role in DB patching?

In Database patching the following teams will be involved.

(i) Database Administrator (DBA) team.
(ii) Linux Administrators team.
(iii) Monitoring team.
(iv) Application team.

(i) ***DBA team :***

This is the team to apply the patches to the databases.

(ii) Linux team :

This team is also involved if any problems occur. If the database volume is having a mirror we should first break the mirror and then the DBA people will apply the patches. After 1 or 2 days there is no problem again we need sync the data between mirrored volume to patch applied volume. If there is no space for patch we have to provide space to DBA team.

(iii) Monitoring team :

This team should receive requests or suggestions to ignore any problems occurs. After applied the patch if the system is automatically rebooted then monitoring team will raise the ticket "Node down" to system administrators team. So, to avoid those type of tickets we have to sent requests to ignore those type alerts.

(iv) Application team :

For applying any patches, the databases should not be available to application. So, if suddenly database is not available then application may be crashed. So, first the application should be stopped. This will be done by application team.

31. What is SLA?

A service-level agreement (SLA) is simply a document describing the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured and the remedies or penalties, if any, should the agreed-upon levels not be achieved. Usually, SLAs are between companies and external suppliers, but they may also be between two departments within a company.

32. What is Problem Management?

The objective of Problem Management is to minimize the impact of problems on the organisation. Problem Management plays an important role in the detection and providing solutions to problems (work around& known errors) and prevents their reoccurrence.
A 'Problem' is the unknown cause of one or more incidents, often identified as a result of multiple similar incidents.A 'Known error' is an identified root cause of a Problem.

33. What is Incident Management?

An 'Incident' is any event which is not part of the standard operation of the service and which causes or may cause, an interruption or a reduction of the quality of the service.
The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.
Inputs for Incident Management mostly come from users, but can have other sources as well like management Information or Detection Systems. The outputs of the process are RFC's (Requests for Changes), resolved and closed Incidents, management information and communication to the customer.

34. What is Change Management?

Change management is a systematic approach to dealing with change, both from the perspective of an organization and on the individual level. change management has at least three different aspects, including adapting to change, controlling change, and effecting change. A proactive approach to dealing with change is at the core of all three aspects.In an information technology (IT) system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operatingsystem release is running on each computer and which fixes have been applied).

35. What is Request Management?

service request management (SRM) is the underlying workflow and processes that enable an IT procurement or service request to be reliably submitted, routed, approved, monitored and delivered. SRM is the process of managing a service request through its lifecycle from submission through delivery and follow-up. SRM may be manual or automated. In a manual system, a user calls a help desk to request a service, and help desk personnel create a service ticket to route the service request. In an automated system, the user submits a request through an online service catalog, and the application software automatically routes the request through the appropriate processes for approval and service delivery. These systems also typically enable users to track the status of their service requests, and management to monitor service delivery levels for quality control purposes.

36. What is grep?

(i) grep means Globally search for Regular Expression.

(ii) Using grep we can filter the results to get a particular information.
(iii) We can get only information about what string we have specified in grep command.

37. What are pipes and filters in Linux?

Pipes :

(a) Pipes are nothing but adding two commands and make as one command.
(b) Normally we cannot combine two commands, but using pipes we get one command by combining two commands.
(c) So, we can get the results as what we required.

Filters :

(a) Filters are nothing but filtering the results what we required.
(b) Using filters we can get exact results depends upon what we specified in the expression.
(c) So, there is no wastage of time because it filters results what we specified in the command expression.

38. What is the full form of COMPUTER ?

C *----->Commonly*
O *-----> Operated*
M *-----> Machine*
P *-----> Particularly*
U *----->Used*
T *----->Technical and*
E *----->Educational*
R *-----> Research*

39. What is the command in sar to monitor NIC devices received/transmitted packets?

 # sar -n DEV 1 5
This will show 5 consecutive output each with a time interval of 1 sec for all the ethernet devices

40. What is Linux Kernel?

It acts as an interpreter between Linux OS and its hardware. It is the fundamental component of Linux OS and contains hardware drivers for the devices installed on the system. The kernel is a part of the system which loads first and it stays on the memory.

41. What are the main parameters effect on server performance?

The one of the most important task of any Linux Admin includes performance monitoring which includes parameter "Load Average" or "CPU Load".

42. What is load average?

Load Average is the value which represents the load on your system for a specific period of time.
Also it can be considered the ratio of the number of active tasks to the number of available CPUs.

43. How to check?

We can use either top or uptime command to view the output of the load average as shown below.
 # uptime
00:07:00 up 4 days, 6:14, 1 user, load average: 0.11, 0.14, 0.09

 # top
top - 00:07:12 up 4 days, 6:15, 1 user, load average: 0.09, 0.13, 0.09

44. What are the three values?

As you can see three values representing the load average column. These show the load on your system over a significant period of time (one or current, five and fifteen minutes averages).

45. How do you know your system has a high load?

The most important question as in most cases I have seen how do you determine your system has high load.Does a high value represents high load average and that your system requires attention?
What is the threshold value for load average?
How can we conclude if the load average value is good or bad?
A Central Processing Unit in earlier days used to be having only one processor and the core concept was not their in those days. But with the advancement in technology and the urge of higher speed to meet up demands of IT industry multiple processor were integrated in the same CPU making it multi-processor. However increasing the no. of processor did increased the working speed of many tasks and performance but it also leads to increase in size, complexity and heat issues. So, in order to continue improvement of performance the core concept was introduced.
Instead of having two CPUs and a motherboard capable of hosting them, two CPUS are taken together and combined to form a dual core processor which will utilize an individual socket using less power and size capable of performing the same amount of task as dual processor CPU.
***Bottom Line** is that Load value depends on the no. of cores in your machine. For example a dual core is relevant to 2 processor or 2 cores and quad core is relevant to 4 processor or four cores as the maximum value for load.*

46. How do I check the no. of cores on my Linux system?

The information which you see under /proc/cpuinfo can be confusing at times. If you run the below command

```
# less /proc/cpuinfo | grep processor
processor       : 0
processor       : 1
processor       : 2
processor       : 3
processor       : 4
processor       : 5
```

So as per the above command my system has 16 processors in it. However it really has 8 processors with hyper threading enabled. The hyper threading presents 2 logical CPUs to the operating system for each actual core so it effectively doubles the no. of logical CPU in your system.

47. How to find if hyper threading is enabled

Look out for "ht" in the flags section inside cpuinfo with the below command

```
# less /proc/cpuinfo | grep flags | uniq | grep -i  "ht"
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse    sse2 ss ht tm syscall
nx rdtscp lm constant_tsc nonstop_tsc pni monitor ds_cpl vmx est tm2
ssse3 cx16 xtpr  sse4_1 sse4_2 popcnt lahf_lm.
```

*The fields we need to compare to find the no. of core are "**physical id**" and "**core id**".*

Run the below command

```
# less /proc/cpuinfo | grep "physical id" | sort|uniq | wc -l
 2
# less /proc/cpuinfo | grep "core id" | sort|uniq | wc -l
 4
```

*So the no. of cores would be **2x4 = 8 cores.***

48. What do you understand the Load Average?

If the number of active tasks utilizing CPU is less as compared to available CPU cores then the load average can be considered normal but if the no. of active tasks starts increasing with respect to available CPU cores then the load average will start rising. ***For example,***

```
# uptime
 00:43:58 up 212 days, 14:19,  4 users,  load average: 6.07, 7.08, 8.07
```

49. How to check all the current running services in Linux?

To find the status of any single service *:*

```
# service vsftpd status
   vsftpd (pid 5909) is running...
```

To get the status of all the running services :

```
# service --status-all | grep running
 acpid (pid 5310) is running...
 atd (pid  6528) is running...
 auditd (pid  5012) is running...
 Avahi daemon is not running
 Avahi DNS daemon is not running
 The Pegasus CIM Listener is running.
 The Pegasus CIM Object Manager is running.
 crond (pid  6242) is running...
 dcerpcd (pid  5177) is running...
 eventlogd (pid  5223) is running...
```

In case you don't use grep you will be able to see all the services on your machine :

```
# service --status-all
 NetworkManager is stopped
 acpid (pid 5310) is running...
 anacron is stopped
 atd (pid  6528) is running...
 auditd (pid  5012) is running...
 automount is stopped
 Avahi daemon is not running
 Avahi DNS daemon is not running
 hcid is stopped
 sdpd is stopped
```

You can also check the active ports along with their services using :

```
# netstat -ntlp
Active Internet connections (only servers)
 Protocol   Recv-Q Send-Q Local Address Foreign Address       State
PID/Program name
 tcp                0      0 0.0.0.0:52961           0.0.0.0:*
```

```
            LISTEN      5223/eventlogd
tcp                 0      0 0.0.0.0:5988            0.0.0.0:*
LISTEN      6116/cimserver
tcp                 0      0 0.0.0.0:5989            0.0.0.0:*
LISTEN      6116/cimserver
tcp                 0      0 0.0.0.0:678             0.0.0.0:*
LISTEN      5160/rpc.statd
tcp                 0      0 0.0.0.0:14247           0.0.0.0:*
LISTEN      6460/java
tcp                 0      0 127.0.0.1:199           0.0.0.0:*
LISTEN      5857/snmpd
tcp                 0      0 0.0.0.0:135             0.0.0.0:*
LISTEN      5177/dcerpcd
```

50. How do you check Linux machine is Physical or Virtual remotely?

There is no hard and fast rule to check whether the machine is physical or virtual but still we do have some commands which can be used for the same purpose.

The command used to view all the required hardware related information for any Linux machine is

```
# dmidecode
```

But the output would be very long and hard to find out the specific details looking for. So, let's narrow it down.

Physical Servers:

```
# dmidecode -s system-product-name
 System x3550 M2 -[7284AC1]-
```

Now to get more details about the system

```
# dmidecode | less (And search for "System Information")
 System Information
            Manufacturer: IBM
            Product Name: System x3550 M2 -[7284AC1]-
            Version: 00
            Wake-up Type: Other
            SKU Number: XxXxXxX
            Family: System x
```

Virtual Servers :

```
# dmidecode -s system-product-name
 VMware Virtual Platform
# dmidecode | less
 System Information
            Manufacturer: VMware, Inc.
             Product Name: VMware Virtual Platform
            Version: None
            Wake-up Type: Power Switch
            SKU Number: Not Specified
 Family: Not Specified
```

On a virtual server running VMware you can run the below command to verify :

```
# lspci | grep -i vmware
 00:0f.0 VGA compatible controller: VMware SVGA II Adapter
```

51. How to find the bit size of your linux machine?

 # uname -m
i686
 # uname -m
x86_64
If we get i386, i586 and i686 that signifies your machine is 32-bit but if we getx86_64 or ia64 then your machine will be 64-bit.
 # getconf LONG_BIT
32
 # getconf LONG_BIT
64 (Here we get an output of bit size either 32 or 64)

52. How can you add a banner or login message in Linux?

By editing these two files
/etc/issue
/etc/motd

53. What is the difference between normal kernel and kernel-PAE?

kernel in 32 bit machine supports max of 4 GB RAM, whereas
kernel PAE in 32 bit linux machine supports till 64 GB RAM

54. Tell me the command to find all the commands in your linux machine having only 2 words like ls, cp, cd etc.

 # find /bin /sbin/usr/bin /usr/sbin -name ?? -type f

55. Which file is generally used to configure kickstart?

anaconda.cfg

56. Which log file will you check for all authentication related messages?

/var/log/secure

57. What is the command used to find the process responsible for a particular running file?

 # fuser filename
 # lsof filename

58. What is the command to take remote of any Linux machine?

 # rdesktop

59. What are the three values shown in load average section of top command?

It shows the current, 5 min back and 15 min back load average value.

60. How to check all the process running by a particular user?

 # ps -u<username>

61. What is an orphan process?

An orphan process is a process that is still executing, but whose parent has died.

62. What is a defunct process?

These are also termed as zombie process. These are those process who have completed their execution but still has an entry in the process table. When a process ends, all of the memory and resources associated with it are de-allocated so they can be used by other processes.After the zombie is removed, its process identifier (PID) and entry in the process table can then be reused. Zombies can be identified in the output from the Unix ps command by the presence of a "Z" in the "STAT" column

63. How do you limit maximum connections in your apache server?

Change the below parameter value inside httpd.conf
MaxClients 256

64. Which command do you use to download a file from ftp or http website using CLI?

 # wget path_to_the_file

65. What is the default port for ssh? How will you change it to some other random port no.?

SSH port no. by default is 22. To change the default port no. we need make required changes inside sshd_config file in the below mentioned line
#Port 22 *(Uncomment the above line and define the new port no)*
Restart the services for changes to take effect.

66. What is the difference between A record and CNAME record in DNS?

A record :
It is the Address records also known as host records
Points to the IP address reflecting the domain
Used for forward lookup of any domain name

For example:
Our website is configured on 50.63.202.15 IP so the A record of my domain name will point towards that IP.
Every time a query for golinuxhub.com is made the internet will lookup for contents stored on the machine with 50.63.202.15 this IP.

CNAME Record :
It is short abbreviation for Canonical Name
Provides an alias name for same hostname
Helps create subdomains

NOTE: *You cannot create a CNAME record for the domain name itself (it should be done with A record)*

For example:
golinuxhub.com is a domain name whereas www.golinuxhub.com is a sub domain name.

About us

SUVEN IT *established in 01-Jan--2010 by Mr. Kv. Reddy having 20 years teaching and 17 years of real time work experience across USA & India, We are recognized as a leader in all IT training Courses to supply quality IT Professionals to Industry. SUVEN IT committed to provide high quality service with elevated level of student's satisfaction and provides the high end industry training and real time knowledge to students.*

We trained and placed 5000+ Students in top MNC's within 6 Years (Most of them are selected in first interview)

SUVEN IT

By Kv. Reddy