Scanned by CamScanner

31. Examples of **top** command

1. 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.

7. **What is file system?**

lsblk Check the CD drive mount option.

Scanned by CamScanner

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 RHEL-7. The vfat file system is used to maintain a common storage between Linux and Windows O/S.

The cdfs file system is used to mount the CD-ROMs and the hdfs file system is used to mount DVDs.

The iso9660 file system is used to read CD/DVD.iso image format files in Linux O/S.

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

Attaching a directory to the file system in order to access the partition and it's file system is known as mounting.

In general the sub directories under /mnt directory are the mount points to mount the file systems.

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)

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

S.No.	Ext2	Ext3	Ext4	Xfs
1.	Stands for Second Extended file system.	Stands for Third Extended file system.	Stands for Fourth Extended file system.	Stands for Extended system.
2.	Does not having Journaling feature.	Supports 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.	Max. file size can be from 16 GB to 8EB.

Scanned by CamScanner

11. 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 device name | 2 mount point | 3 file system type | 4 mount options | 5 take a backup | 6 should run or not fsck or not

12. 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)

13. How to make a file system in Linux?

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

14. 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)

15. How to delete the partition?

fdisk /dev/sdc

Scanned by CamScanner

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.	Max. file system size can be from 2 TB to 16EB.
5.	Cannot convert ext file system to ext2.	We can directly convert ext2 to ext3 file system.	We can convert all file systems to ext4 file system.	Unmount and mou the file system is required.

11. 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 device name | 2 mount point | 3 file system type | 4 mount options | 5 take a backup | 6 should run or not fsck or not

12. 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)

13. How to make a file system in Linux?

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

14. 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)

15. How to delete the partition?

fdisk /dev/sdc

Scanned by CamScanner

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)

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

First check any wrong entries are there in /etc/fstab file. If all are ok then unmount all the partitions by

executing the below command,

umount -a

Then mount again mount all the partitions by executing the below command,

mount -a

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 file or all the file sizes 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?

Scanned by CamScanner

mount LABEL=<label name><mount point>

Example : # 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?

Scanned by CamScanner

(i) Inode number

(ii) File name

(iii)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?

By running the **# 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?

Scanned by CamScanner

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.>%)

Important Commands :

Scanned by CamScanner

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 interactive mode)

mke2fs -n <partition name> (to see the superblock information)

mke2fs -t <file system type><partition name> (to format the partition in the specified file system 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 <mount point or directory name> (to check whether this directory is mount point or 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)

Scanned by CamScanner

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>**and killthose processesforcefully by **# kill -9 <process id>**

journalctl (It tracks all the log files between two different timings and by default saved in **/run/log** location)

* **/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)
sar (sar utility is to watch the system activity report like CPU, memory,...etc.,)
smartctl -H <hard disk name> (to check the health of the specified hard disk)
smartctl -i <hard disk name> (to see the information of the specified hard disk)
smartctl -a <hard disk name> (it gives more information of the specified hard disk)

> **Note:** In the above command results go to **Value**and **Tresh** fields. If **Tresh** is more than the **Value** then immediately hard disk change is required. If **Tresh** is lower than the **Value** then hard disk is ok. So, the **Tresh** is always lower than the **Value**, otherwise hard disk change is required immediately and report this manager.

Scanned by CamScanner

2. 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) :

Scanned by CamScanner

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)

Scanned by CamScanner

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>

Scanned by CamScanner

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>

Scanned by CamScanner

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.

Scanned by CamScanner

- 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)

Q - How to restore LVM.

Scanned by CamScanner

By default, unlimited logical volumes can be created per volume group. But we can control this limit by

vgchange -l <no.><volume group> (to limit max. no. of logical volumes to the specified number)

Example : # vgchange -l 2 <vgname> (to limit max. 2 logical volumes cab be created in this volume group)

vgchange -p <no.><volume group> (to limit max. no. of physical volumes to the specified number)

Example : # vgchange -p 2 <vgname> (to limit max. 2 physical volumes can be added to this volume group)

vgchange -s <block size in no.><volume group> (to change the block size of the volume group)

Example : # vgchange -s 4 <vgname> (to change the volume group block size to 4MB)

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)

Scanned by CamScanner

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)

Scanned by CamScanner

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

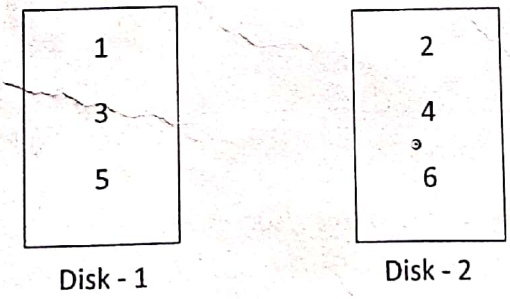
(iv) RAID - (0+1) ---Stripping + Mirroring ---- Minimum 4 disks required

(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)

Scanned by CamScanner

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 ....

1	1
2	2
3	3
4	4
5	5
6	6

Disk - 1 Disk - 2

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

mdadm -Cv /dev/md0 -n 2 /dev/sdb /dev/sdc -l 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)

Scanned by CamScanner

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)

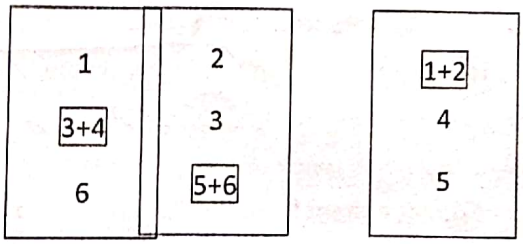
mdadm /dev/md0 --add /dev/sde (to add third disk to the RAID - 1 volume)

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)

Scanned by CamScanner

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? Troubleshoot

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?

Scanned by CamScanner

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. ie., 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

• (dot) means current directory

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

Scanned by CamScanner

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)

Scanned by CamScanner

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)

Scanned by CamScanner

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)

cms [otor now

Scanned by CamScanner

3. User and Group Administration

1. What is a user?

In Linux user is one who uses the system. There can be at least one or more than one user in Linux at a time.

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 and are maintained system deamons).

(In RHEL - 7 the System users are (i) 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	Defaul Shell
Super User	Root	0	0	/root	/bin/bas
Normal User	ram, raju, gopal, ...etc.,	500 - 60000	500 - 60000	/home/<user name>	/bin/bas
System User	ftp, ssh, apache, nobody, ...etc.,	1 - 499	1 - 499	/vat/ftp, ...etc	/sbin/nolg
Network User	Remote user like LDAP user	Same as normal users	Same as normal users	/home/guests/ldapuser	/bin/bas
Sudo User	Normal users with admin privileges	Same as normal users	Same as normal users	/home/<user name>	/bin/bas

3. What is user management?

User management means managing user. ie., Creating the users, deleting the users and modifying the users.

Scanned by CamScanner

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>

Scanned by CamScanner

(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 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) # cat /etc/passwd |grep <user name> (It shows the user's details if that user is already created)

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

Scanned by CamScanner

-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 **gidin /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 as same as other user's id)

-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 also rename

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

.bash_profile : This 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 primary group.

Scanned by CamScanner

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?

Scanned by CamScanner

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, ie., **# 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

Scanned by CamScanner

<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

for 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?

Scanned by CamScanner

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.

ITL Infotech

useradd <user name> (to create the user)

passwd -S <user name> (to see the status of the password of that user. if root user is not assigned the password then the password status is **locked**)

passwd -d <user name> (then delete the password for that user)

chage -d 0 <user name> (it will change the password age policy)

su - <user name> (Try to switch to that user then it will display the following message)

Newpassword : (type new password for that user)

Retype password : (retype the password again)

The other useful commands :

w (this command gives the login user information like how many users currently login and their processes)

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)

Scanned by CamScanner

* **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)

1 /bin/sh -----> default shell for Unix

2 /bin/bash -----> default shell for Linux

3 /sbin/nologin -----> users cannot login shell

4 /bin/tcsh -----> c shell to write 'C++' language programs

5 /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 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.,)

Scanned by CamScanner

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)

34. 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)

35. 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 direc

Scanned by CamScanner

x	Not required for file. It is required only for scripting files	Go to inside the directory Ex. # cd /dir

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

chmod <options><file name or directory name> (to change the owner or permissions of the file or directory)

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)	"	"

37. 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)

38. 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

How to change the ownership & Group at a time,

chown user1:demo1 /testfile

ls -lt /filename

Scanned by CamScanner

-L -----> do not traverse-p -----> do not traverse

39. 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

40. 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.

41. 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)

42. 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)

Scanned by CamScanner

-rwsrwxrwx <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.

43. 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)

44. 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>

rwxrwxrwt <directory name> (where 't' is called the sticky bit)

45. 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.

46. What is the use of group?

Scanned by CamScanner

(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.

47. Can we login to the user without password?

Yes, we can login.

48. 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.

Scanned by CamScanner

49. 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).

50. How to put never expiry to a user?

passwd -x -1 <user login name>

51. Which one is the default sticky bit directory?

/tmp is the default sticky bit directory.

52. 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.

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

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

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

fuser -cu (to see who are login)

#fuser -ck <user login name> (to kill the specified user)

55. 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.

56. 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.

Scanned by CamScanner

Create the mount point using **# mkdir /<mount point>** command.

Mount that file system on the mount point using **# mount -o acl <partition name><mount point>** command.

Mount the partition permanently using **# vim /etc/fstab** (open this file and make an entry as below)

<partition name><mount point><file system type> defaults, acl 0 0

Save and exit this file.

If the partition is already mounted then just add **acl** after defaults in **/etc/fstab** file and execute the below command **# mount -o remount <partition name>**

57. How to check the ACL permissions?

getfacl <options><file or directory name>

The options are, -d -----> Display the default ACLs.

-R -----> Recurses into subdirectories.

58. 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

59. 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 the group)

setfacl -x o : <user name><file or directory name> (to remove the ACL permissions from the other)

setfacl -b <file or directory> (to remove all the ACL permissions on that file directory)

Scanned by CamScanner

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? Redhat Interview

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 package is not Installed then install the quota package by **# yum install quota* -y** command.

quotaon (to enable the quota)

quotaoff (to disable the quota)

Scanned by CamScanner

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	grace period
/dev/sdb1	0	5000	10000	0	0	0	6 days

(save and exit the quota editor)

Scanned by CamScanner

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.

hard=10000 ---> If it reached to 10MB, then it will not allow to create the files. The grace period by default is 7 days. So, we can change the grace period by **#edquota -t** command, here we can change the default 7 days grace period to our required days of grace period.

grace period means, if the user not created any files within the grace period days the soft limit becomes as hard limit. ie., soft and hard limits are equal.

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

66. How to enable the group quota?

(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?

Scanned by CamScanner

chpasswd (to change multiple user's passwords)

<user name 1> : <password>

<user name 2> : <password>

<user name 3> : <password>

<user name 4> : <password>

<user name 5> : <password> (Ctrl + d -----> to save and exit)

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

4. Network 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 computer network. 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?**

Scanned by CamScanner

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 Rout
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.

Scanned by CamScanner

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?

Scanned by CamScanner

(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)

#nmtui

Scanned by CamScanner

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 nam** is the file which contains the NIC configuration de
/etc/resolve.conf is the file which contains DNS server IP and domain name location.	**/etc/resolve.conf** is the file which contains DN server IP and domain name location.
/etc/sysconfig/network is the hostname configuration file.	**/etc/hostname** is the hostname configuration fi
/etc/hosts is the file which contains the local DNS server IP address.	**/etc/hosts** is the file which contains the local DN 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 ca disable the NIC card and If it is **no** except root nobody can disable the NIC card.

22. How to set the hostname temporarily and permanently?

RHEL - 6 :

Scanned by CamScanner

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 and 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 and 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)

Scanned by CamScanner

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

Scanned by CamScanner

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

(iii)vim /etc/sysconfig/network-scripts/ifcfg-eth2 (Save and exit this file)
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

Scanned by CamScanner

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 : RHEL-7

(i) Add the team0 connection by

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

(ii) 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

Scanned by CamScanner

(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

Scanned by CamScanner

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)

Scanned by CamScanner

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)

Scanned by CamScanner

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><default gateway>'
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)

Scanned by CamScanner

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)

Scanned by CamScanner

(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)

Scanned by CamScanner

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)

Scanned by CamScanner

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 (1)

(b) Permissive (0)

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.

Scanned by CamScanner

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)

Scanned by CamScanner

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)

6. Booting Procedure and Kernel parameters

1. **Explain the booting procedure?**

In Linux systems the booting is done in 6 stages.

- BIOS
- MBR
- GRUB

Scanned by CamScanner

- 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 :

Scanned by CamScanner

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?**

Scanned by CamScanner

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.

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

(iii) 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?

Scanned by CamScanner

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 Controller i-DRAC ---> Integrated DELL Remote Access Controller
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. (ii) At console prompt and boot with CDROM in single user mode and mount the root (/ ---> O/S) file system on temporary mount point.

(iii)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).

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

(vi) 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.

(viii) 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.

Scanned by CamScanner

(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.

Scanned by CamScanner

(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)

Scanned by CamScanner

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.

(ii) 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.

(ii) 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.

Scanned by CamScanner

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 :

(i) at jobs are executes only once.

(ii) 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.

Scanned by CamScanner

- **/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)

(iii)# crontab -e (to edit the crontab)

11. How to troubleshoot if the cron job failed?

Scanned by CamScanner

(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.

(iii) 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.

(iv) 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 :

(i) See the job id which job we want to delete by **# atq** command and note that job id.

(ii) 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.

Scanned by CamScanner

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)

Scanned by CamScanner

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)

Scanned by CamScanner

* 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

(v) @reboot <mail command> (every reboot, one mail will be send to the root)

(vi)@monthly <command> (every month the command will be executed)

(vii) @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.

Scanned by CamScanner

8. Administrating Remote Systems (SSH)

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.,

(v) If it is through remote desktop, we can manage the servers using the GUI tools.

(vi) 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?

Scanned by CamScanner

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 dat 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).

Scanned by CamScanner

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.

(v) 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.

(vi) 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)

Scanned by CamScanner

(vii) 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)

Scanned by CamScanner