**Q:1 Why is LVM is required ?**  
Ans: LVM stands for Logical Volume Manager , to resize filesystem’s size online we required LVM partition in Linux. Size of LVM partition can be extended and reduced using the lvextend & lvreduce commands respectively.

**Q:2 How To check Memory stats and CPU stats ?**

Ans:  Using ‘free’ & ‘vmstat’ command we can display the physical and virtual memory statistics respectively.With the help of ‘sar’ command we see the CPU utilization & other stats.

**Q:3 What does Sar provides and at which location Sar logs are stored ?**  
Ans: Sar Collect, report, or save system activity information. The default version of the sar command (CPU utilization report) might be one of the first facilities the  user  runs  to  begin system  activity investigation, because it monitors major system resources. If CPU utilization is near 100 percent (user + nice + system), the workload sampled is CPU-bound.

By  default log files of Sar command  is located at  /var/log/sa/sadd file, where the dd parameter indicates the current day.

**Q:4 How to increase the size of LVM partition ?**  
Ans: Below are the Logical Steps :  
- Use the lvextend command (lvextend -L +100M /dev/<Name of the LVM Partition> , in this example we are extending the size by 100MB.  
- resize2fs /dev/<Name of the LVM Partition>  
- check the size of partition using ‘df -h’ command

**Q:5 How to reduce or shrink the size of LVM partition ?**  
Ans: Below are the logical Steps to reduce size of LVM partition :  
-Umount the filesystem using umount command,  
-use resize2fs command , e.g resiz2fs /dev/mapper/myvg-mylv 10G  
-Now use the lvreduce command , e.g lvreduce -L 10G /dev/mapper/myvg-mylv

Above Command will shrink the size & will make the filesystem size 10GB.

**Q:6 How to create partition from the raw disk ?**  
Ans: Using fdisk utility we can create partitions from the raw disk.Below are the steps to create partition from the raw dsik :  
- fdisk  /dev/hd\* (IDE) or /dev/sd\* (SCSI)  
- Type n to create a new partition  
-  After creating partition , type w command to write the changes to the partition table.

**Q:7 Where the kernel modules are located ?**  
Ans: The ‘/lib/modules/kernel-version/’ directory stores all kernel modules or compiled drivers in Linux operating system. Also with ‘lsmod’ command we can see all the installed kernel modules.

**Q:8 What is umask ?**  
Ans: umask stands for ‘User file creation mask’, which determines the settings of a mask that controls which file permissions are set for files and directories when they are created.

**Q:9 How to set the umask permanently for a user?**  
Ans: To set this value permanently for a user, it has to be put in the appropriate profile file which depends on the default shell of the user.

**Q:10 How to change the default run level in linux ?**  
Ans: To change the run level we have to edit the file “/etc/inittab” and change initdefault entry ( id:5:initdefault:). Using ‘init’ command we change the run level temporary like ‘init 3′ , this command will move the system in runlevl 3.

**Q:11 How to share a directory using nfs ?**  
Ans: To share a directory using nfs , first edit the configuration file ‘/etc/exportfs’ , add a entry like  
‘/<directory-name>  <ip or Network>(Options)’ and then restart the nfs service.

**Q:12 How to check and mount nfs share ?**  
Ans: Using ‘showmount’ command we can see what directories are shared via nfs e.g ‘showmount -e <ip address of nfs server>’.Using mount command we can mount the nfs share on linux machine.

**Q:13 What are the default ports used for SMTP,DNS,FTP,DHCP,SSH and squid ?**  
Ans: Service      Port  
SMTP          25  
DNS            53  
FTP             20 (data transfer) , 21 ( Connection established)  
DHCP         67/UDP(dhcp server) , 68/UDP(dhcp client)  
SSH            22  
Squid         3128

**Q:14 What is Network Bonding ?**  
Ans: Network bonding is the aggregation of multiple Lan cards into a single bonded interface to provide fault tolerance and high performance. Network bonding is also known as NIC Teaming.

**Q:15 What  are the different modes of Network bonding in Linux ?**  
Ans: Below are list of modes used in Network Bonding :

* balance-rr or 0 – round-robin mode for fault tolerance and load balancing.
* active-backup or 1 – Sets active-backup mode for fault tolerance.
* balance-xor or 2 – Sets an XOR (exclusive-or) mode for fault tolerance and load balancing.
* broadcast or 3 – Sets a broadcast mode for fault tolerance. All transmissions are sent on all slave interfaces.
* 802.3ad or 4  – Sets an IEEE 802.3ad dynamic link aggregation mode. Creates aggregation groups that share the same speed & duplex settings.
* balance-tlb or 5 -  Sets a Transmit Load Balancing (TLB) mode for fault tolerance & load balancing.
* balance-alb or 6 -  Sets an Active Load Balancing (ALB) mode for fault tolerance & load balancing.

**Q:16 How to check and verify the status the bond interface.**

Ans: Using the command ‘cat /proc/net/bonding/bond0′ , we can check which mode is enabled and what lan cards are used in this bond. In this example we have one only one bond interface but we can have multiple bond interface like bond1,bond2 and so on.

**Q:17 How to check default route and routing table ?**  
Ans: Using the Commands ‘netstat -nr’ and ‘route -n’ we can see the default route and routing tables.

**Q:18 How to check which ports are listening in my Linux Server ?**  
Asn:  Use the Command ‘netstat –listen’ and ‘lsof -i’

**Q:19 List the services that are enabled at a particular run level in linux server ?**  
Ans: With the help of command ‘chkconfig –list | grep 5:on’ we can list all the service that are enabled in run level5. For other run levels just replace 5 with the respective run level.

**Q:20 How to enable a service at a particular run level ?**  
Ans: We can enable a service using the Command ‘chkconfig <Service-Name> on –level 3′

**Q:21 How to upgrade Kernel in Linux ?**  
Ans: We should never upgrade Linux Kernel , always install the new New kernel using rpm command because upgrading a kenel can make your linux box in a unbootable state.

**Q:22 How To scan newly asssigned luns on linux box without rebooting ?**  
Ans: There are two ways to scan newly assigned luns :  
Method:1 if sg3 rpm is installed , then run the command ‘rescan-scsi-bus.sh’  
Method:2 Run the Command ,  echo ” – - – ” > /sys/class/scsi\_host/hostX/scan

**Q:23 How  to find WWN numbers of HBA cards in Linux Server ?**  
Ans: We can find the WWN numbers of HBA cards using the command ‘systool -c fc\_host -v | grep port\_name’

**Q:24 How to add & change the Kernel parameters ?**  
Ans: To Set the kernel parameters in linux , first edit the file ‘/etc/sysctl.conf’ after making the changes save the file and run the command ‘sysctl -p’ , this command will make the changes permanently without rebooting the machine.

**Q:25 What is Puppet Server ?**  
Ans: Puppet is an open-source & enterprise software for configuration management toll in UNIX like  operating system.  Puppet is a  IT automation software used to push configuration to its clients (puppet agents) using code. Puppet code can do a variety of tasks from installing new software, to check file permissions, or updating user accounts & lots of other tasks.

**Q:26 What are manifests in Puppet ?**  
Ans: Manifests, in Puppet, are the files in which the client configuration is specified.

**Q:27 Which Command is used to sign requested certificates in Puppet Server ?**  
Ans: ‘puppetca  –sign hostname-of-agent’ in (2.X)  & ‘puppet ca  sign hostname-of-agent’ in  (3.X)

**Q:28  At which location  Puppet Master Stores Certificates ?**  
Ans:  /var/lib/puppet/ssl/ca/signed

**Q:29 How to find all the regular files in a directory  ?**  
Ans: using the command ‘find /<directory -type f’.

**Q:30 What is load average in a linux ?**  
Ans: Load  Average is defined as the average sum of the number of process waiting in the run queue and number of process currently executing over the period of 1,5 and 15  minutes. Using the ‘top’ and ‘uptime’ command we find the load average of a linux sever.

**1. What is the difference between service and process?**

A process is any piece of software that is running on a computer. For example, your anti-virus software runs in the background as a process, which was automatically started when the computer booted. Some processes start when your computer boots, others are started manually when needed.

Some processes are services that publish methods to access them, so other programs can call them as needed. Printing services would be an example of a service type of process, where your email program can just call the print services process to say it wants to print, and the service does the actual work.

**2. How to view crond status? If it’s show service is not found.**

Service crond restart

**3. My clients are getting services from servers but how to know which client is using which service. is there any files to keep information about these? Clients used ftp, nis, samba, apache, squid, nfs and mail services how to know how many users got service from server side with date, time and client system ip?**

Mail server – /var/log/mail/maillog [RedHat,centos]  
ssh – /var/log/secure  
Apache – /var/log/http/access.log  
nfs – /var/lib/nfs/rmtab

**4. How to FTP user access other directory except his own home directory?**

vim /etc/vsftpd/vsftpd.conf  
Chroot\_list\_enable=yes

**5. What are the Linux-based security tools?**

Selinux  
Firewall  
iptables  
Tcp-wrappers

**6. What are the basic elements of firewall?**

A firewall should be able to filter packets (drop/pass them) based on certain rules specified by the user. The rules may be used to identify an incoming packet to the computer or outgoing packet from the computer, it can be based on target port number/ip add , traffic from a particular Network card etc…

The firewall rules can be in a tabular form (saved on the disk) from where the firewall software can read them and implement it. iptables firewall on Linux is a great example

**7. What is a command to display top 10 users who are using huge space?**

du -sh /home/\* | sort -r | head -10

**8. How do find all failed login attempts via ssh?**

tail -f /var/log/secure | grep Failed

**9. How do you configure Linux system as a router?**

vim /etc/sysctl.conf  
net.ipv4.ip\_forward=1  
system-config-network  
eth0 192.168.1.120 eth0:1 172.24.0.1  
255.255.255.0 255.255.0.0  
172.24.0.1 192.168.1.120

**10. What is the UID and GID of root user? Can a normal user can change the ownership of a file? What is the command to change ownership of a file?**

The root UID/GID is 0 (zero). Which is why he can able to intervene in all normal users files even though he don’t had permission. A normal user will don’t have the permission to change ownership of file. The command to change ownership is < chown user.user file >

**11. What is the diff b/w ext2 and ext3?**

Ext3 is a tiny bit slower than ext2 is, but it holds tremendous advantages. There is really only one difference between ext2 and ext3, and that is that ext3 uses a journal to prevent filesystem corruption in the case of an unclean shutdown (ie. before the filesystem is synced to disk). That makes ext3 a bit slower than ext2 since all metadata changes are written to the journal, and then flushed to disk, but on the other hand you don’t risk having the entire filesystem destroyed at power failure or if an unwitted person turns the computer off uncleanly. You don’t have to check the filesystem after an unclean shutdown either. Ext3 has three levels of journalling. Metadata (ie. internal filesystem structures) are always journalled, so that the filesystem itself is never corrupted. How ordinary data is written to the file system is controllable, though. The default option is the “ordered” mode, which causes file contents to be written to the filesystem before metadata is even committed to the journal. The highest reliable mode is called the “journal” mode, which causes file data to be committed to the journal before it is flushed to its final place, like the metadata. The least reliable mode, but rumoured to be the fastest, is called the “writeback” mode, which makes no promises at all regarding the consistency of file data. Only metadata is output reliably in writeback mode. So as for anything else, it’s mainly a matter of priority. If you don’t want ultimate speed, go with ext3. If you need the highest speed that is theoratically aquirable though, then go with ext2. For that to be effective you’ll probably need a really advanced hard drive controller, though.

**12. As the system administrator you need to review Bob’s cronjobs. What command would you use?**

crontab –lu Bob

**13. What command is used to remove the password assigned to a group?**

gpasswd –r groupname

**14. What are the different RAID levels?**

♣ RAID level 0  
♣ RAID level RAID level 1  
♣ RAID level 2  
♣ RAID level 3  
♣ RAID level 4  
♣ RAID level 5  
♣ RAID level 6  
♣ RAID level 10  
♣ RAID level 50

**15. How do you create a swapfile?**

dd if=/dev/zero of=/swapfile bs=1024 count=200M  
mkswap /swapfile  
swapon /swapfile

**16. What does nslookup do?**

Nslookup is a program used to find information about internet Domain Name server.  
The two modes of nslookup are: Interactive and non-interactive.  
Using ‘interactive mode’ user can query the name servers for the information pertaining to hosts and domains.  
Using ‘non-interactive mode’ the user can just print the name and requested information of a host.

**17. What is the difference between UDP and TCP?**

TCP is a Transmission Control Protocol.  
UDP is a User Datagram Protocol.  
There are four major differences between UDP and TCP:

1. TCP can establish a Connection and UDP cannot.

2. TCP provides a stream of unlimited length, UDP sends Small packets.

3.TCP gurantees that as long as you have a connection data sent will arrive at the destination, UDP provides not guarantee delivery.  
4.UDP is faster for sending small amounts of data since no connection setup is required, the data can be sent in less time then it takes for TCP to establish a connection.

**18. What command do you run to check file system consistency?**

Need to run fsck [file system consistency check] command to check file system consistency and repair a Linux / UNIX file system.

fsck

**19. What is the command to remove Lvm ,Pv and vg**

1st remove the entry on /etc/fstab file & save – quit.  
2nd remove LVM – lvremove lvname  
3rd remove VG – vgremove vgname  
4th remove PV – pvremove pvname

**20. How to create SAMBA server in fedora 9 Linux?**

yum install samba -y

yum install samba-swat –y

vi /etc/samba/smb.conf

comment = windows sharing  
path = path/your/share/directory  
valid users = surendra  
writable = yes  
browseable = yes

then type testparm for code testing.

smbpasswd -a username  
smbpasswd -e username

service smb restart  
chkconfig smb on

**21. How to schedule cron backup to run on 4th Saturday of month?**

\* \* \* \* 6 weekdaynum 4 && sh /backup/test.sh

**22. What is an inode?**

ext2 and ext3 file systems keep a list of the files they contain in a table called an inode table. The inode is referenced by its number. This is unique within a file system.

The inode contains the metadata about files. Among the data stored in the inode is

File type

File permissions

Link count

User ID number of the file owner and the group ID number of the associated group

Last modification time

Location of the data on the hard disk

Other metadata about the file

ls -li – view inode number only

stat /etc/passwd – view inode details

**23. How to see unallocated hard disk space on linux**

df -h

**24. How do u find remote machine operating system and version?**

nmap -A –v 192.168.1.100

**25. How do you port scanning with netstat command?**

netstat –an

**26. Linux system monitoring Tools?**

top – Process Activity Command  
vmstat – System Activity, Hardware and System Information  
w – Find out Who Is Logged on And What They Are Doing  
Uptime – Tell How Long the System Has Been Running  
ps – Displays the Processes  
free – Memory Usage  
iostat – Average CPU Load, Disk Activity  
sar – Collect and Report System Activity  
mpstat – Multiprocessor Usage  
pmap – Process Memory Usage

**27. Linux Network monitoring Tools?**

netstat and ss – Network Statistics  
iptraf – Real-time Network Statistics  
tcpdump – Detailed Network Traffic Analysis  
strace – System Calls

/Proc file system – Various Kernel Statistics  
# cat /proc/cpuinfo  
# cat /proc/meminfo  
# cat /proc/zoneinfo  
# cat /proc/mounts

Nagios – Server And Network Monitoring  
Cacti – Web-based Monitoring Tool  
Gnome System Monitor – Real-time Systems Reporting and Graphing  
**28. What is mean by system calls?**

A system call is the mechanism used by an application program to request service from the operating system.

On Unix-based and POSIX-based systems, popular system calls are open, read, write, close, wait, exec, fork, exit, and kill. Many of today’s operating systems have hundreds of system calls. For example, Linux has 319 different system calls. FreeBSD has about the same (almost 330). Tools such as strace and truss report the system calls made by a running process.

**29. Important port no:**

NFS – 2049  
FTP – 21  
SAMBA – 445  
SSH – 22  
DNS – 53  
POP3 – 110  
IMAP – 143  
HTTPS – 443  
HTTP – 80

**30. How do u extract files from iso cd images in linux?**

mount –o loop disk1.iso /mnt/iso

) What is Linux and why is it so popular?  
Linux is an operating system based on UNIX, and was first introduced by Linus Torvalds commonly used in servers.It is based on the Linux Kernel, and can run on different hardware platforms manufactured by Intel, MIPS, HP, IBM, SPARC and Motorola. Another popular element in Linux is its mascot, a penguin figure named Tux.

Popularity of Linux is because of the following reasons

It is free and open source. We can download Linux for free and customize it as per our needs.  
It is very robust and adaptable.  
Immense amount of libraries and utilities

2) What is the difference between UNIX and LINUX?  
Unix originally began as a propriety operating system from Bell Laboratories, which later on spawned into different commercial versions. On the other hand, Linux is free, open source and intended as a non-propriety operating system for the masses.

3) What is BASH?  
BASH is short for Bourne Again SHell. It was written by Steve Bourne as a replacement to the original Bourne Shell (represented by /bin/sh). It combines all the features from the original version of Bourne Shell, plus additional functions to make it easier and more convenient to use. It has since been adapted as the default shell for most systems running Linux.

4) What is Linux Kernel?  
The Linux Kernel is a low-level systems software whose main role is to manage hardware resources for the user. It is also used to provide an interface for user-level interaction.

5) What is LILO?  
LILO is a boot loader for Linux. It is used mainly to load the Linux operating system into main memory so that it can begin its operations.

6) What is a swap space?  
A swap space is a certain amount of space used by Linux to temporarily hold some programs that are running concurrently. This happens when RAM does not have enough memory to hold all programs that are executing.

7) What is the advantage of open source?  
Open source allows you to distribute your software, including source codes freely to anyone who is interested. People would then be able to add features and even debug and correct errors that are in the source code. They can even make it run better, and then redistribute these enhanced source code freely again. This eventually benefits everyone in the community.

8 ) What are the basic components of Linux?  
Just like any other typical operating system, Linux has all of these components: kernel, shells and GUIs, system utilities, and application program. What makes Linux advantageous over other operating system is that every aspect comes with additional features and all codes for these are downloadable for free.

9) Does it help for a Linux system to have multiple desktop environments installed?  
In general, one desktop environment, like KDE or Gnome, is good enough to operate without issues. It’s all a matter of preference for the user, although the system allows switching from one environment to another. Some programs will work on one environment and not work on the other, so it could also be considered a factor in selecting which environment to use.

10) What is the basic difference between BASH and DOS?  
The key differences between the BASH and DOS console lies in 3 areas:  
- BASH commands are case sensitive while DOS commands are not;  
- under BASH, / character is a directory separator and \ acts as an escape character. Under DOS, / serves as a command argument delimiter and \ is the directory separator  
- DOS follows a convention in naming files, which is 8 character file name followed by a dot and 3 character for the extension. BASH follows no such convention.

11) What is the importance of the GNU project?  
This so-called Free software movement allows several advantages, such as the freedom to run programs for any purpose and freedom to study and modify a program to your needs. It also allows you to redistribute copies of a software to other people, as well as freedom to improve software and have it released to the public.

12) Describe the root account.  
The root account is like a systems administrator account, and allows you full control of the system. Here you can create and maintain user accounts, assigning different permissions for each account. It is the default account every time you install Linux.

13) What is CLI?  
CLI is short for Command Line Interface. This interface allows user to type declarative commands to instruct the computer to perform operations. CLI offers an advantage in that there is greater flexibility. However, other users who are already accustom with using GUI find it difficult to remember commands including attributes that come with it.

14) What is GUI?  
GUI, or Graphical User Interface, makes use of images and icons that users click and manipulate as a way of communicating with the computer. Instead of having to remember and type commands, the use of graphical elements makes it easier to interact with the system, as well as adding more attraction through images, icons and colors.

15) How do you open a command prompt when issuing a command?  
To open the default shell (which is where the command prompt can be found), press Ctrl-Alt-F1. This will provide a command line interface (CLI) from which you can run commands as needed.

16) How can you find out how much memory Linux is using?  
From a command shell, use the “concatenate” command: cat /proc/meminfo for memory usage information. You should see a line starting something like: Mem: 64655360, etc. This is the total memory Linux thinks it has available to use.

17) What is typical size for a swap partition under a Linux system?  
The preferred size for a swap partition is twice the amount of physical memory available on the system. If this is not possible, then the minimum size should be the same as the amount of memory installed.

18) What are symbolic links?  
Symbolic links act similarly to shortcuts in Windows. Such links point to programs, files or directories. It also allows you instant access to it without having to go directly to the entire pathname.

19) Does the Ctrl+Alt+Del key combination work on Linux?  
Yes, it does. Just like Windows, you can use this key combination to perform a system restart. One difference is that you won’t be getting any confirmation message and therefore, reboot is immediate.

20) How do you refer to the parallel port where devices such as printers are connected?  
Whereas under Windows you refer to the parallel port as the LPT port, under Linux you refer to it as /dev/lp . LPT1, LPT2 and LPT3 would therefore be referred to as /dev/lp0, /dev/lp1, or /dev/lp2 under Linux.

21) Are drives such as harddrive and floppy drives represented with drive letters?  
No. In Linux, each drive and device has different designations. For example, floppy drives are referred to as /dev/fd0 and /dev/fd1. IDE/EIDE hard drives are referred to as /dev/hda, /dev/hdb, /dev/hdc, and so forth.

22) How do you change permissions under Linux?  
Assuming you are the system administrator or the owner of a file or directory, you can grant permission using the chmod command. Use + symbol to add permission or – symbol to deny permission, along with any of the following letters: u (user), g (group), o (others), a (all), r (read), w (write) and x (execute). For example the command chmod go+rw FILE1.TXT grants read and write access to the file FILE1.TXT, which is assigned to groups and others.

23) In Linux, what names are assigned to the different serial ports?  
Serial ports are identified as /dev/ttyS0 to /dev/ttyS7. These are the equivalent names of COM1 to COM8 in Windows.

24) How do you access partitions under Linux?  
Linux assigns numbers at the end of the drive identifier. For example, if the first IDE hard drive had three primary partitions, they would be named/numbered, /dev/hda1, /dev/hda2 and /dev/hda3.

25) What are hard links?  
Hard links point directly to the physical file on disk, and not on the path name. This means that if you rename or move the original file, the link will not break, since the link is for the file itself, not the path where the file is located.

26) What is the maximum length for a filename under Linux?  
Any filename can have a maximum of 255 characters. This limit does not include the path name, so therefore the entire pathname and filename could well exceed 255 characters.

27) What are the filenames that are preceded by a dot?  
In general, filenames that are preceded by a dot are hidden files. These files can be configuration files that hold important data or setup info. Setting these files as hidden makes it less likely to be accidentally deleted.

28) Explain virtual desktop.  
This serves as an alternative to minimizing and maximizing different windows on the current desktop. Using virtual desktops, each desktop is a clean slate where you can open one or more programs. Rather than minimizing/restoring all those programs as needed, you can simply shuffle between virtual desktops with programs intact in each one.

29) How do you share a program across different virtual desktops under Linux?  
To share a program across different virtual desktops, in the upper left-hand corner of a program window look for an icon that looks like a pushpin. Pressing this button will “pin” that application in place, making it appear in all virtual desktops, in the same position onscreen.

30) What does a nameless (empty) directory represent?  
This empty directory name serves as the nameless base of the Linux file system. This serves as an attachment for all other directories, files, drives and devices.

31) What is the pwd command?  
The pwd command is short for print working directory command. It’s counterpart in DOS is the cd command, and is used to display the current location in the directory tree.

32) What are daemons?  
Daemons are services that provide several functions that may not be available under the base operating system. Its main task is to listen for service request and at the same time to act on these requests. After the service is done, it is then disconnected and waits for further requests.

33) How do you switch from one desktop environment to another, such as switching from KDE to Gnome?  
Assuming you have these two environments installed, just log out from the graphical interface. Then at the Log in screen, type your login ID and password and choose which session type you wish to load. This choice will remain your default until you change it to something else.

34) What are the kinds of permissions under Linux?  
There are 3 kinds of permissions under Linux:  
- Read: users may read the files or list the directory  
- Write: users may write to the file of new files to the directory  
- Execute: users may run the file or lookup a specific file within a directory

35) How does case sensitivity affect the way you use commands?  
When we talk about case sensitivity, commands are considered identical only if every character is encoded as is, including lowercase and uppercase letters. This means that CD, cd and Cd are three different commands. Entering a command using uppercase letters, where it should be in lowercase, will produce different outputs.

36) What are environmental variables?  
Environmental variables are global settings that control the shell’s function as well as that of other Linux programs. Another common term for environmental variables is global shell variables.

37) What are the different modes when using vi editor?  
There are 3 modes under vi:  
- Command mode – this is the mode where you start in  
- Edit mode – this is the mode that allows you to do text editing  
- Ex mode – this is the mode wherein you interact with vi with instructions to process a file

38) Is it possible to use shortcut for a long pathname?  
Yes, there is. A feature known as filename expansion allows you do this using the TAB key. For example, if you have a path named /home/iceman/assignments directory, you would type as follows: /ho[tab]/ice[tab]/assi[tab] . This, however, assumes that the path is unique, and that the shell you’re using supports this feature.

39) What is redirection?  
Redirection is the process of directing data from one output to another. It can also be used to direct an output as an input to another process.

40) What is grep command?  
grep a search command that makes use of pattern-based searching. It makes use of options and parameters that is specified along the command line and applies this pattern into searching the required file output.

41) What could possibly be the problem when a command that was issued gave a different result from the last time it was used?  
One highly possible reason for getting different results from what seems to be the same command has something to do with case sensitivity issues. Since Linux is case sensitive, a command that was previously used might have been entered in a different format from the present one. For example, to lists all files in the directory, you should type the command ls, and not LS. Typing LS would either result in an error message if there is no program by that exact name exist, or may produce a different output if there is a program named LS that performs another function.

42) What are the contents in /usr/local?  
It contains locally installed files. This directory actually matters in environments where files are stored on the network. Specifically, locally-installed files go to /usr/local/bin, /usr/local/lib, etc.). Another application of this directory is that it is used for software packages installed from source, or software not officially shipped with the distribution.

43) How do you terminate an ongoing process?  
Every process in the system is identified by a unique process id or pid. Use the kill command followed by the pid in order to terminate that process. To terminate all process at once, use kill 0.

44) How do you insert comments in the command line prompt?  
Comments are created by typing the # symbol before the actual comment text. This tells the shell to completely ignore what follows. For example: “# This is just a comment that the shell will ignore.”

45) What is command grouping and how does it work?  
You can use parentheses to group commands. For example, if you want to send the current date and time along with the contents of a file named OUTPUT to a second file named MYDATES, you can apply command grouping as follows: (date cat OUTPUT) > MYDATES

46) How do you execute more than one command or program from a single command line entry?  
You can combine several commands by separating each command or program using a semicolon symbol. For example, you can issue such a series of commands in a single entry:  
ls –l cd .. ls –a MYWORK  
which is equivalent to 3 commands:  
ls -l  
cd..  
ls -a MYWORK  
\*\*Note that this will be executed one after the other, in the order specified.

47) Write a command that will look for files with an extension “c”, and has the occurrence of the string “apple” in it.  
Answer: Find ./ -name “\*.c” | xargs grep –i “apple”

48) Write a command that will display all .txt files, including its individual permission.  
Answer: ls -a -l \*.txt

49) Write a command that will do the following:  
-look for all files in the current and subsequent directories with an extension c,v  
-strip the,v from the result (you can use sed command)  
-use the result and use a grep command to search for all occurrences of the word ORANGE in the files.  
Find ./ -name “\*.c,v” | sed ‘s/,v//g’ | xargs grep “ORANGE”

50) What, if anything, is wrong with each of the following commands?  
a) ls -l-s  
b) cat file1, file2  
c) ls – s Factdir  
Answers:  
a) there should be space between the 2 options: ls -l -s  
b) do not use commas to separate arguments: cat file1 file2  
c) there should be no space between hyphen and option label: ls –s Factdir

**Basic Questions**

**1. What is initrd image and what is its function in the linux booting process ?**

The initial RAM disk (initrd) is an initial root file system that is mounted prior to when the real root file system is available.The initrd is bound to the kernel and loaded as part of the kernel boot procedure. The kernel then mounts this initrd as part of the two-stage boot process to load the modules to make the real file systems available and get at the real root file system. Thus initrd image plays a vital role in [linux booting process](http://linoxide.com/booting/boot-process-of-linux-in-detail/).

**2. Explain the terms suid, sgid and sticky bit ?**

In addition to the basic file permissions in Linux, there are few special permissions that are available for executable files and directories.

**SUID :** If setuid bit is set, when the file is executed by a user, the process will have the same rights as the owner of the file being executed.

**SGID :** Same as above, but inherits group previleges of the file on execution, not user previleges. Similar way when you create a file within directory,it will inherit the group ownership of the directories.

**Sticky bit** : Sticky bit was used on executables in linux so that they would remain in the memory more time after the initial execution, hoping they would be needed in the near future. But mainly it is on folders, to imply that a file or folder created inside a stickybit enabled folder could only be deleted by the owner. A very good implementation of sticky bit is /tmp ,where every user has write permission but only users who own a file can delete them.

**3. List out few of the differences between Softlink and Hardlink ?**

**a)** Hardlink cannot be created for directories. Hard link can only be created for a file.

**b)** Symbolic links or symlinks can link to a directory.

**c)** Removing the original file that your hard link points to does not remove the hardlink itself; the hardlink still provides the content of the underlying file.

**d)** If you remove the hard link or the symlink itself, the original file will stay intact.

**e)** Removing the original file does not remove the attached symbolic link or symlink, but without the original file, the symlink is useless

**4. How do you sent a mail attachment via bash console ?**

“mutt” is an opensource tool for sending emails with attachments from the linux bash command line. We can install “mutt” from the binary rpm or via packagemanager.

For Ubuntu / Debian based destros.

# apt-get install mutt

For Redhat / Fedor based destros,

# yum install mutt

Usage :

# mutt -s “Subject of Mail” -a “path of attachment file” “email address of recipient” < “message text containing body of the message”

Eg : mutt -s “Backup Data” -a /home/backup.tar.gz admin@mywebsite.com < /tmp/message.txt

**5. What is the difference between umask and ulimit ?**

umask stands for ‘User file creation mask’, which determines the settings of a mask that controls which file permissions are set for files and directories when they are created. While ulimit is a linux built in command which provides control over the resources available to the shell and/or to processes started by it.

You can limit user to specific range by editing /etc/security/limits.conf at the same time system wide settings can be updated in /etc/sysctl.conf

**6. What are the run levels in linux and how to change them ?**

A run level is a state of init and the whole system that defines what system services are operating and they are identified by numbers.There are 7 different run levels present (run level 0-6) in Linux system for different purpose. The descriptions are given below.

0: Halt System (To shutdown the system)  
1: Single user mode  
2: Basic multi user mode without NFS  
3: Full multi user mode (text based)  
4: unused  
5: Multi user mode with Graphical User Interface  
6: Reboot System

To change the run level, edit the file “/etc/inittab” and change initdefault entry ( id:5:initdefault:). If we want to change the run level on the fly, it can be done using ‘init’ command.

For example, when we type ‘init 3′ in the commandline , this will move the system from current runlevel to runlevl 3. Current level can be listed by typing the command ‘who -r’

**7. What is the functionality of a Puppet Server ?**

Puppet is an open-source and enterprise application for configuration management toll in UNIX like operating system. Puppet is an IT automation software used to push configuration to its clients (puppet agents) using code. Puppet code can do a variety of tasks from installing new software, to check file permissions, or updating user accounts and lots of other tasks.

**8. What is SeLinux?**

SELinux is an acronym for Security-enhanced Linux. It is an access control implementation and security feature for the Linux kernel. It is designed to protect the server against misconfigurations and/or compromised daemons. It put limits and instructs server daemons or programs what files they can access and what actions they can take by defining a security policy.

**9. What is crontab and explain the fields in a crontab ?**

The cron is a deamon that executes commands at specific dates and times in linux. You can use this to schedule activities, either as one-time events or as recurring tasks. Crontab is the program used to install, deinstall or list the tables used to drive the cron daemon in a server. Each user can have their own crontab, and though these are files in /var/spool/cron/crontabs, they are not intended to be edited directly. Here are few of the command line options for crontab.

crontab -e Edit your crontab file.  
crontab -l Show your crontab file.  
crontab -r Remove your crontab file.

Traditional cron format consists of six fields separated by white spaces:

<Minute> <Hour> <Day\_of\_the\_Month> <Month\_of\_the\_Year> <Day\_of\_the\_Week> <command/program to execute>

The format is explained in detail below.

\* \* \* \* \* \*  
| | | | | |  
| | | | | +-- Year (range: 1900-3000)  
| | | | +---- Day of the Week (range: 1-7, 1 standing for Monday)  
| | | +------ Month of the Year (range: 1-12)  
| | +-------- Day of the Month (range: 1-31)  
| +---------- Hour (range: 0-23)  
+------------ Minute (range: 0-59)

**10. What are inodes in Linux ? How to find the inode associated with a file ?**

An inode is a data structure on a filesystem on Linux and other Unix-like operating systems that stores all the information about a file except its name and its actual data. When a file is created, it is assigned both a name and an inode number, which is an integer that is unique within the filesystem. Both the file names and their corresponding inode numbers are stored as entries in the directory that appears to the user to contain the files. The concept of inodes is particularly important to the recovery of damaged filesystems. When parts of the inode are lost, they appear in the lost+found directory within the partition in which they once existed.

The following will show the name of each object in the current directory together with its inode number:

# ls -i

The avialble number inodes in a filesystem can be found using the below command :

# df -i

The other way we can get the inode details of a file by using the stat commmand.

Usage : # stat <file name>

Example :

-sh-4.1$ stat note.txt  
File: `note.txt’  
Size: 4 Blocks: 8 IO Block: 4096 regular file  
Device: fd05h/64773d Inode: 8655235 Links: 1  
Access: (0644/-rw-r--r--) Uid: (69548/nixuser) Gid: (25000/ UNKNOWN)  
Access: 2014-06-29 15:27:56.299214865 +0000  
Modify: 2014-06-29 15:28:28.027093254 +0000  
Change: 2014-06-29 15:28:28.027093254 +0000

Apart from the above basic questions, be prepared for answers for the below questions

**1.** How to set linux file/directory permissions ?

**2.** How to set ownership for files/directories ?

**3.** How to create user/group and how to modify it ?

**4.** How to find kernel / OS version and its supported bit (32/64) version ?

**5.** How to set / find interface ip address ?

**6.** How to find linux mount points and disk usage ?

**7.** What command to find memory and swap usage ?

**8.** Have a look on ps, top, grep, find, awk and dmesg commands ?

**Linux Scenario Questions**

**11. What is the difference between name based virtual hosting and IP based virtual hosting ? Explain the scenario where name based virtual hosting seems useful ?**

Virtual hosts are used to host multiple domains on a single apache instance. You can have one virtual host for each IP your server has, or the same IP but different ports, or the same IP, the same port but different host names. The latter are called “name based vhosts”.

n IP-based virtual hosting, we can run more than one web site on the same server machine, but each web site has its own IP address while In Name-based virtual hosting, we host multiple websites on the same IP address. But for this to succeed, you have to put more than one DNS record for your IP address in the DNS database.

In the production shared webhosting environment, getting a dedicated IP address for every domains hosted in the server is not feasible in terms of cost. Most of the customers wont be able to afford the cost of having a dedicated IP address. Here is the place where the concepts of Name based virtual hosting find its place.

**12. What is network bonding in Linux and where the important configuration files involved? What is the advantage of Network Bonding ?**

Network Bonding is a Linux kernel feature that allows to aggregate multiple network interfaces into a single virtual link. This is a great way to achieve redundant links, fault tolerance or load balancing networks in production system. If one of the physical NIC is down or unplugged, it will automatically move traffic to the other NIC card. Similar way the bonding will increase the interface throughput to handle the traffic it it is configured in active-active mode.

There are 7 modes starting from 0 to 6 which decides how the bonding configuration behaves.

**mode=0** (balance-rr) - Round-robin policy

It the default mode. It transmits packets in sequential order from the first available slave through the last.  
This mode provides load balancing and fault tolerance.

**mode=1** (active-backup)

Active-backup policy: In this mode, only one slave in the bond is active. The other one will become active, only when the active slave fails. The bond’s MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.

**mode=2** (balance-xor)

Transmit the traffic based on [(source MAC address XOR'd with destination MAC address) modulo slave count]. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance.

**mode=3** (broadcast)

Broadcast policy: transmits everything on all slave interfaces. This mode provides fault tolerance.

**mode=4** (802.3ad)

Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.

**mode=5** (balance-tlb) - Adaptive transmit load balancing

channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

**mode=6** (balance-alb) - Adaptive load balancing

It includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation.

Important Configuration Files involved :

/etc/sysconfig/network-scripts/ifcfg-bond0  
/etc/modprobe.d/bonding.conf  
/etc/sysconfig/network-scripts/ifcfg-eth[0-4]  
/proc/net/bonding/bond0

**13. Explain briefly the procedure for re-installing Grub in Linux ?**

**1)**Download Ubuntu Installation / Live cd

**2)**Boot from Ubuntu Installation / Live cd - usb, burned cd etc.  
**3)**During boot select “Try Ubuntu” , Don’t select install !  
**4)** Mount your Linux root partition  
sudo mount /dev/sda6 /mnt ( Assuming /dev/sda6 is the Linux root partition)  
**5)** Install / reinstall grub  
$ sudo grub-install --root-directory=/mnt/ /dev/sda ( where /dev/sda is your primary disk)  
Installation finished. No error reported.

**6)** Reboot your system, remove bootable CD and we should have the boot menu ready when the system starts.

Note : There would be slight difference when using with other distros.

**14. Explain the fields in /etc/passwd and /etc/shadow ?**

The /etc/shadow file stores actual password in encrypted format with some additional properties related to user password.It mainly holds athe account aging parameters. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file Generally, shadow file entry looks as below.

steve:$1$XOdE07rn$WA6qFm4W5UIqNfaqE5Uub.:13775:0:99999:7:::

Here is the explanation of each field.

***User name*** : Your login name

***Password***: Your encrypted password.

***Last password change*** : Days since Jan 1, 1970 that password was last changed

***Minimum***: The minimum number of days required between password changes.

***Maximum***: The maximum number of days the password is valid.

***Warn*** : The number of days before password is to expire that user is warned that his/her password must be changed

***Inactive*** : The number of days after password expires that account is disabled

***Expire*** : days since Jan 1, 1970 that account is disabled. It indicates an absolute date specifying when the login may no longer be used

The /etc/passwd file stores essential information, which is required during login /etc/passwd is a text file, that contains a list of user account related parameters like user ID, group ID, home directory, shell, etc.

Here is the sample entry from /etc/passwd file

steve:x:6902:6902::/home/steve:/bin/bash

***Username***: User’s login name.

***Password***: An x character indicates that encrypted password is stored in /etc/shadow file.

***User ID (UID)***: Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root.

***Group ID (GID)***: The primary group ID

***User Info***: The comment field. It allow you to add extra information about the user.

***Home directory***: The absolute path to the directory the user will be in when they log in.

***Command/shell***: The absolute path of a command or shell (/bin/bash).

**15. How do you boot your system into the following modes, when you are in some trouble ?**

**a)** Rescue mode  
**b)** Single user mode  
**c)** Emergency mode

Rescue mode provides the ability to boot a small Linux environment from an external bootable device like a CD-ROM, or USB drive instead of the system’s hard drive.Rescue mode is provided to help you with your system from repairing the file system or fixing certain issues which prevent your normal operations.

In order to get into the rescue mode, change the BIOS settings of the machine to boot from the external media. Once the system started booting using bootable disk, add the keyword rescue as a kernel parameter or else you can give the parameter “linux rescue” in the graphical boot interface.

In single-user mode, the system boots to runlevel 1, but it will have many more additional functionalities compared to switching to runlevel 1 from other levels.

The local file systems can be mounted in this mode, but the network is not activated.

Use the following steps to boot into single-user mode:

**1)**At the GRUB splash screen during the booting process, press any key to enter the GRUB interactive menu.  
**2)**Select the proper version of kernel that you wish to boot and type “a” to append the line.  
**3)**Go to the end of the line and type “single” as a separate word.  
**4)**Press Enter to exit edit mode and type “b” to boot into single usermode now.

In emergency mode, you are booting into the most minimal environment possible. The root file system is mounted read-only and almost nothing is set up. The main advantage of emergency mode over single-user mode is that the init files are not loaded. If the init is corrupted , you can still mount file systems to recover data that could be lost during a re-installation. To boot into emergency mode, use the same method as described for single-user mode, with one exception, replace the keyword single with the keyword “emergency”.

**16. In the ps results few of the processes are having process state as “D” . What does it mean ? Briefly explain different process states ?**

To have a dynamic view of a process in Linux, always use the top command. This command provides a real-time view of the Linux system in terms of processes. The eighth column in the output of this command represents the current state of processes. A process state gives a broader indication of whether the process is currently running, stopped, sleeping etc.

A process in Linux can have any of the following four states…

**Running** – A process is said to be in a running state when either it is actually running/ executing or waiting in the scheduler’s queue to get executed (which means that it is ready to run). That is the reason that this state is sometimes also known as ‘runnable’ and represented by (R).

**Waiting or Sleeping** – A process is said to be in this state if it is waiting for an event to occur or waiting for some resource-specific operation to complete. So, depending upon these scenarios, a waiting state can be subcategorised into an interruptible (S) or uninterruptible (D) state respectively.

**Stopped** – A process is said to be in the stopped state when it receives a signal to stop. This usually happens when the process is being debugged. This state is represented by (T).

**Zombie** – A process is said to be in the zombie state when it has finished execution but is waiting for its parent to retrieve its exit status. This state is represented by (Z).

Apart from these four states, the process is said to be dead after it crosses over the zombie state; ie when the parent retrieves its exit status. ‘Dead’ is not exactly a state, since a dead process ceases to exist.

**17. What is drop cache in Linux and how do you clear it ?**

Cache in Linux memory is where the Kernel stores the information it may need later, as memory is incredible faster than disk.

It is great that the Linux Kernel takes care about that.Linux Operating system is very efficient in managing your computer memory, and will automatically free the RAM and drop the cache if some application needs memory.

Kernels 2.6.16 and newer provide a mechanism to have the kernel drop the page cache and/or inode and dentry caches on command, which can help free up a lot of memory. Now we can throw away that script that allocated a ton of memory just to get rid of the cache.

To free pagecache:

# echo 1 > /proc/sys/vm/drop\_caches

To free dentries and inodes:

# echo 2 > /proc/sys/vm/drop\_caches

To free pagecache, dentries and inodes:

echo 3 > /proc/sys/vm/drop\_caches

This is a non-destructive operation in normal scenarios and will only free things that are completely unused. Dirty objects will continue to be in use until written out to disk and are not freeable. However it is always preferred to run “sync” first to flush useful things out to disk.

**18. Password based authentication is disabled in your infrastructure. So how do you login to the servers ?**

To improve the system security even further, most of the organizations turned to use keybased authentications instead of Password based authentication. We can enforce the key-based authentication by disabling the standard password authentication, which involves a public key private key pair. The public key is added in the server configuration file while private key is kept kept confidential on the client side.

Below listed is the procedure, to set up keybased authentication.

**1)** Generating Key Pairs

a) Generate an RSA key pair by typing the following at a shell prompt:

$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/steve/.ssh/id\_rsa):

b) Press Enter to confirm the default location (that is, ~/.ssh/id\_rsa) for the newly created key.

c) Enter a passphrase, and confirm it by entering it again when prompted to do so.

d) Copy the content of ~/.ssh/id\_rsa.pub into the ~/.ssh/authorized\_keys on the machine to which you want to connect,  
appending it to its end if the file already exists.

e) Change the permissions of the ~/.ssh/authorized\_keys file using the following command:

$ chmod 600 ~/.ssh/authorized\_keys

**2)** Now on your client side, open the remote connection agent like putty and browse your public key and try SSH to the server, you should be able to login without a password now.

# ssh server1.myserver.com  
The authenticity of host ‘server1.myserver.com (192.168.44.2)’ can’t be established.  
RSA key fingerprint is e3:c3:89:37:4b:94:37:d7:0c:d5:6f:9a:38:62:ce:1b.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added ‘server1.myserver.com’ (RSA) to the list of known hosts.  
Last login: Tue July 13 12:40:34 2014 from server2.myserver.com

**3)** Public key authentication can prevent brute force SSH attacks, but only if all password-based authentication methods are disabled. Once public key authentication has been confirmed to be working, disable regular password authentication by editing /etc/ssh/sshd\_config and set the following option to “no”.

PasswordAuthentication no

**19. Explain the different Scenarios involved in TCP 3 way handshake ?**

The TCP three way handshake is the process for establishing a TCP connection.We can explain 3 way handshake with a simple scenario where we assume a client computer is contacting a server to send it some information.

**a)** The client sends a packet with the SYN bit set and a sequence number of N.  
**b)** The server sends a packet with an ACK number of N+1, the SYN bit set and a sequence number of X.  
**c)** The client sends a packet with an ACK number of X+1 and the connection is established.  
**d)** The client sends the data.

The first three steps in the above process is called the three way handshake.

**20. As the disk space utilization was so high in the server, the Administrator has removed few files from the server but still the disk utilization is showing as high. What would be the reason ?**

In Linux even if we remove a file from the mounted file system, that will still be in use by some application and for this application it remains available. Its because file descriptor in /proc/ filesystem is held open..So if there are such open descriptors to files already removed, space occupied by them considered as used. You find this difference by checking them using the “df” and “du” commands. While df is to show the file system usage, du is to report the file space usage. du works from files while df works at filesystem level, reporting what the kernel says it has available.

You can find all unlinked but held open files with:

# lsof | grep ‘(deleted)’

This will list the filename which is open witht he pid in which it is running. We can kill those Pids and which will stop these process and will recover the disk space responsible for this file.

**21. What is rDNS and explain its benefits in the Linux Domain Name Systems ?**

A typical DNS lookup is used to determine which IP address is associated with a hostname, and this is called Forward DNS lookup. A reverse DNS lookup is used for the opposite, to determine which hostname is associated with an IP address. Sometimes reverse DNS lookups are required for diagnostic purposes. Today, reverse DNS lookups are used mainly for security purposes to trace a hacker or spammer. Many modern mailing systems use reverse mapping to provide simple authentication using dual lookup: hostname-to-address and address-to-hostname. The rDNS ( reverse DNS ) is implemented using a specialized zone record for reverse lookups called PTR record. PTR records always resolve to names, never IP addresses.

**22. What is sosreport, how do you generate it while working with your Redhat Support Team in production ?**

Sosreport is a command-line utility in Redhat based linux destros (RHEL / CentOS) which collects system configuration and diagnostic information of your linux box like running kernel version, loaded modules, and system and service configuration files. This command also runs external programs to collect further information, and stores this output in the resulting archive. Sosreport is required when you have open a case with redhat for technical support. Redhat support Engineers will require sosreport of your server for troubleshooting purpose. To run sosreport, sos package should be installed. Sos package is part of default installation in most of linux. If for any reason this package is no installed , then use below yum command to install it manually :

# yum install sos

Generate the report

Open the terminal type sosreport command :

# sosreport

This command will normally complete within a few minutes. Depending on local configuration and the options specified in some cases the command may take longer to finish. Once completed, sosreport will generate a compressed a file under /tmp folder. The file should be provided to Redhat support representative as an attachment to open a support case.

**23. What is swappiness in Linux Memory Management and how do we configure that ?**

The swappiness parameter controls the tendency of the kernel to move processes out of physical memory and onto the swap disk. Because disks are much slower than RAM, this can lead to slower response times for system and applications if processes are too aggressively moved out of memory.

swappiness can have a value of between 0 and 100

swappiness=0 tells the kernel to avoid swapping processes out of physical memory for as long as possible

swappiness=100 tells the kernel to aggressively swap processes out of physical memory and move them to swap cache

The default setting in Redhat/Ubuntu based Linux distros is swappiness=60. Reducing the default value of swappiness will probably improve overall performance for a typical Ubuntu desktop installation.

~$ cat /proc/sys/vm/swappiness  
60

If we have enough RAM, we can turn that down to 10 or 15. The swap file will then only be used when the RAM usage is around 80 or 90 percent.

To change the system swappiness value, open /etc/sysctl.conf as root. Then, change or add this line to the file:

vm.swappiness = 10

Reboot for the change to take effect

You can also change the value while your system is still running

sysctl vm.swappiness=10

We can also clear swap by running swapoff -a and then swapon -a as root instead of rebooting to achieve the same effect.

**24. What is git ?**

Git is a very popular and efficient open source Version Control System. It tracks content such as files and directories. It stores the file content in BLOBs - binary large objects. The folders are represented as trees. Each tree contains other trees (subfolders) and BLOBs along with a simple text file which consists of the mode, type, name and Secure Hash Algorithm of each blob and subtree entry. During repository transfers, even if there are several files with the same content and different names, the GIT software will transfer the BLOB once and then expand it to the different files.

**25. What is inode ? Briefly explain the structure ?**

Inode is a data structure that keeps track of all the information about a file. When we keep our information in a file and the OS stores the information about a file in an inode. Information about files is sometimes called metadata. We can say that an inode is metadata of the data. In a file system, inodes consist roughly of 1% of the total disk space, whether it is a whole storage unit or a partition on a storage unit. The inode space is used to ?track? the files stored on the hard disk. The inode entries store metadata about each file, directory or object, but only points to these structures rather than storing the data. Each entry is 128 bytes in size. The metadata contained about each structure can include the following:

Inode number  
Access Control List (ACL)  
Extended attribute  
Direct/indirect disk blocks  
Number of blocks  
File access, change and modification time  
File deletion time  
File generation number  
File size  
File type  
Group  
Number of links  
Owner  
Permissions  
Status flags

Inode structure of a directory consists of a name to inode mapping of files and directories in that directory.In a directory, You can find the inode number corresponding to the files using the command “ls -i”

786727 -rw------- 1 root root 4226530 May 29 13:17 sudo.log  
786437 -rw-------. 1 root root 32640 Jun 23 20:11 tallylog  
786440 -rw-rw-r--. 1 root utmp 276096 Jul 20 06:45 wtmp  
786741 -rw------- 1 root root 9653 Jul 17 09:38 yum.log

Similar way, the number of inodes allocated, used and free in a Filesystem can be listed using “df -i” command

# df -i /root  
Filesystem Inodes IUsed IFree IUse% Mounted on  
/dev/mapper/RootVol-lvmroot  
524288 80200 444088 16% /

- See more at: http://linoxide.com/linux-how-to/linux-interview-questions-answers/#sthash.wXCrjcnM.dpuf