**1. How do u force a user to change password on next login in linux?**

A. chage -d 0 "User"

**2.What command can be used to findout server architechure (x86 or x64) apart from**

**uname?**

A. arch

**3. How do u findout the users who are NOT logged in for more than 30 days? which file u**

**will check?**

A. last , lastlog, /var/log/wtmp

**4. whats is called 1.5 stage in boot process of linux?**

A. Which contains extra code to allow cylinders above 1024, or LBA type drives, to be read. The

1.5 boot loader is stored (if needed) in the MBR or the boot partition.The great thing about

GRUB is that it includes knowledge of Linux file systems. Instead of using raw sectors on the

disk, as LILO does, GRUB can load a Linux kernel from an ext2 or ext3 file system. It does this

by making the two-stage boot loader into a three-stage boot loader. Stage 1 (MBR) boots a

stage 1.5 boot loader that understands the particular file system containing the Linux kernel

image. Examples include reiserfs\_stage1\_5 (to load from a Reiser journaling file system) or

e2fs\_stage1\_5 (to load from an ext2 or ext3 file system). When the stage 1.5 boot loader is

loaded and running, the stage 2 boot loader can be loaded."

So Basically,

Stage 1 Boot loader is MBR

Stage 2 Boot loader is GRUB

Stage 1.5 Boot loader is e2fs\_stage1\_5

(Basically this module will load the knowledge of Filesystem to Grub to read the kernel)

**5. When u try to create a file, u got a error that "No space available". But actually space**

**available on volume? How do u resolve this issue?**

A. Try this df -i list inode information instead of block usage [Perhaps are you out of inodes on

this file system.], To "rectify it", remove unwanted files or move them somewhere else.]

**1. Q. How do you list files in a directory?**

**A. ls - list directory contents**

**ls �l (-l use a long listing format)**

**2. Q. How do you list all files in a directory, including the hidden files?**

**A. ls -a (-a, do not hide entries starting with .)**

**3. Q. How do you find out all processes that are currently running?**

**A. ps -f (-f does full-format listing.)**

**4. Q. How do you find out the processes that are currently running or a particular user?**

**A. ps -au Myname (-u by effective user ID (supports names)) (a - all users)**

**5. Q. How do you kill a process?**

**A. kill -9 8 (process\_id 8) or kill -9 %7 (job number 7)**

**kill -9 -1 (Kill all processes you can kill.)**

**killall - kill processes by name most (useful - killall java)**

**6. Q. What would you use to view contents of the file?**

**A. less filename**

**cat filename**

**pg filename**

**pr filename**

**more filename**

**most useful is command: tail file\_name - you can see the end of the log file.**

**7. Q. What would you use to edit contents of the file?**

**A. vi screen editor or jedit, nedit or ex line editor**

**8. Q. What would you use to view contents of a large error log file?**

**A. tail -10 file\_name ( last 10 rows)**

**9. Q. How do you log in to a remote Unix box?**

**A. Using telnet server\_name or ssh -l ( ssh - OpenSSH SSH client (remote login program))**

**10.Q. How do you get help on a UNIX terminal?**

**A. man command\_name**

**info command\_name (more information)**

**11.Q. How do you list contents of a directory including all of its**

**subdirectories, providing full details and sorted by modification time?**

**A. ls -lac**

**-a all entries**

**-c by time**

**12.Q. How do you create a symbolic link to a file (give some reasons of doing so)?**

**A. ln /../file1 Link\_name**

**Links create pointers to the actual files, without duplicating the contents of**

**the files. That is, a link is a way of providing another name to the same file.**

**There are two types of links to a file:Hard link, Symbolic (or soft) link;**

**13.Q. What is a filesystem?**

**A. Sum of all directories called file system.**

**A file system is the primary means of file storage in UNIX.**

**File systems are made of inodes and superblocks.**

**14.Q. How do you get its usage (a filesystem)?**

**A. By storing and manipulate files.**

**15.Q. How do you check the sizes of all users� home directories (one command)?**

**A. du -s**

**df**

**The du command summarizes disk usage by directory. It recurses through all subdirectories and shows disk usage by each subdirectory with a final total at the end.**

**Q. in current directory**

**A. ls -ps (p- directory; s - size)**

**16.Q. How do you check for processes started by user 'pat'?**

**A. ps -fu pat (-f -full\_format u -user\_name )**

**17.Q. How do you start a job on background?**

**A. bg %4 (job 4)**

**18 Q. What utility would you use to replace a string '2001' for '2002' in a text file?**

**A. Grep, Kde( works on Linux and Unix)**

**19. Q. What utility would you use to cut off the first column in a text file?**

**A. awk, kde**

**20. Q. How to copy file into directory?**

**A. cp /tmp/file\_name . (dot mean in the current directory)**

**21. Q. How to remove directory with files?**

**A. rm -rf directory\_name**

**22. Q. What is the difference between internal and external commands?**

**A. Internal commands are stored in the; same level as the operating system while external**

**commands are stored on the hard disk among the other utility programs.**

**23. Q. List the three main parts of an operating system command:**

**A. The three main parts are the command, options and arguments.**

**24 Q. What is the difference between an argument and an option (or switch)?**

**A. An argument is what the command should act on: it could be a filename,**

**directory or name. An option is specified when you want to request additional**

**information over and above the basic information each command supplies.**

**25. Q. What is the purpose of online help?**

**A. Online help provides information on each operating system command, the**

**syntax, the options, the arguments with descriptive information.**

**26. Q. Name two forms of security.**

**A. Two forms of security are Passwords and File Security with permissions specified.**

**27. Q. What command do you type to find help about the command who?**

**A. $ man who**

**28. Q. What is the difference between home directory and working directory?**

**A. Home directory is the directory you begin at when you log into the**

**system. Working directory can be anywhere on the system and it is where you are currently**

**working.**

**29. Q. Which directory is closer to the top of the file system tree, parent directory or current directory?**

**A. The parent directory is above the current directory, so it is closer to**

**the root or top of the**

**file system.**

**30. Q. Given the following pathname:**

**$ /business/acctg/payable/supplier/april**

**a) If you were in the directory called acctg, what would be the relative**

**pathname name for the file called april?**

**b) What would be the absolute pathname for april?**

**A.**

**a) $ payable/supplier/april**

**b) $ /business/acctg/payable/supplier/april**

**31. Q. Suppose your directory had the following files:**

**help. 1 help.2 help.3 help.4 help.O1 help.O2**

**aid.O1 aid.O2 aid.O3 back. 1 back.2 back.3**

**a) What is the command to list all files ending in 2?**

**b) What is the command to list all files starting in aid?**

**c) What is the command to list all "help" files with one character extension?**

**A.**

**a) ls \*2**

**b) ls aid.\***

**c) ls help.?**

**32. Q. What are two subtle differences in using the more and the pg commands?**

**A. With the more command you display another screenful by pressing**

**the spacebar, with pg you press the return key.**

**The more command returns you automatically to the UNIX**

**shell when completed, while pg waits until you press return.**

**33. Q. When is it better to use the more command rather than cat command?**

**A. It is sometimes better to use the more command when you are viewing**

**a file that will display over one screen.**

**34. Q. What are two functions the move mv command can carry out?**

**A. The mv command moves files and can also be used to rename a file or directory.**

**35. Q. Name two methods you could use to rename a file.**

**A. Two methods that could be used:**

**a. use the mv command**

**b. copy the file and give it a new name and then remove the original file if no longer needed.**

**36. The soccer league consists of boy and girl teams. The boy file names begin**

**with B, the girl teams begin with G. All of these files are in one directory**

**called "soccer", which is your current directory:**

**Bteam.abc Bteam.OOl Bteam.OO2 Bteam.OO4**

**Gteam.win Gteam.OOl Gteam.OO2 Gteam.OO3**

**Write the commands to do the following:**

**a) rename the file Bteam.abc to Bteam.OO3.**

**b) erase the file Gteam. win after you have viewed the contents of the file**

**c) make a directory for the boy team files called "boys", and one for the girl team files**

**called" girls"**

**d) move all the boy teams into the "boys" directory**

**e) move all the girl teams into the "girls" directory**

**f) make a new file called Gteam.OO4 that is identical to Gteam.OOl**

**g) make a new file called Gteam.OO5 that is identical to Bteam.OO2**

**A.**

**a) mv Bteam.abc Bteam.OO3.**

**b) cat Gteam.win -or- more Gteam.win**

**rm Gteam. win**

**c) mkdir boys**

**mkdir girls**

**d) mv Bteam\* boys**

**e) mv Gteam\* girls**

**f) cd girls**

**cp Gteam.OO1 Gteam.OO4**

**g) There are several ways to do this. Remember that we are currently in the directory**

**/soccer/girls.**

**cp ../boys/Bteam.OO2 Gteam.OO5**

**or**

**cd ../boys**

**cp Bteam.OO2 ../girls/Gteam.OO5**

**37. Q. Draw a picture of the final directory structure for the "soccer"**

**directory, showing all the files and directories.**

**38. Q. What metacharacter is used to do the following:**

**1.1 Move up one level higher in the directory tree structure**

**1.2 Specify all the files ending in .txt**

**1.3 Specify one character**

**1.4 Redirect input from a file**

**1.5 Redirect the output and append it to a file**

**A.**

**1. 1.1 double-dot or ..**

**1.2 asterisk or \***

**1.3 question or ?**

**1.4 double greater than sign: >>**

**1.5 the less than sign or <**

**39. Q. List all the files beginning with A**

**A. To list all the files beginning with A command: ls A\***

**40. Q. Which of the quoting or escape characters allows the dollar sign ($) to retain its special meaning?**

**A. The double quote (") allows the dollar sign ($) to retain its special meaning.**

**Both the backslash (\) and single quote (') would remove the special meaning of the dollar sign.**

**41. Q. What is a faster way to do the same command?**

**mv fileO.txt newdir**

**mv filel.txt newdir**

**mv file2.txt newdir**

**mv file3.txt newdir**

**A. A shortcut method would be: mv file?.txt newdir**

**42. Q. List two ways to create a new file:**

**A.**

**a. Copy a file to make a new file.**

**b. Use the output operator e.g. ls -l > newfile.txt**

**43. Q. What is the difference between > and >> operators?**

**A. The operator > either overwrites the existing file (WITHOUT WARNING) or creates a new file.**

**The operator >> either adds the new contents to the end of an existing file or creates a new file.**

**44. Write the command to do the following:**

**44.1 Redirect the output from the directory listing to a printer.**

**44.2 Add the file efg.txt to the end of the file abc.txt.**

**44.3 The file testdata feeds information into the file called program**

**44.4 Observe the contents of the file called xyz.txt using MORE.**

**44.5 Observe a directory listing that is four screens long.**

**A.**

**44.1 ls > lpr**

**44.2 cat efg.txt >> abc.txt**

**44.3 program < testdata**

**44.4 more < xyz.txt**

**44.5 ls > dirsave | more**

**45. Q. How do you estimate file space usage**

**A. Use du command (Summarize disk usage of each FILE, recursively for**

**directories.) Good to use arguments du -hs**

**(-h, --human-readable print sizes in human readable format (e.g., 1K 234M 2G)**

**(-s, --summarize display only a total for each argument)**

**46. Q. How can you see all mounted drives?**

**A. mount -l**

**47. Q. How can you find a path to the file in the system?**

**A. locate file\_name (locate - list files in databases that match a pattern)**

**48. Q. What Linux HotKeys do you know?**

**A. Ctrl-Alt-F1 Exit to command prompt**

**Ctrl-Alt-F7 or F8 Takes you back to KDE desktop from command prompt**

**Crtl-Alt-Backspace Restart XWindows**

**Ctrl-Alt-D Show desktop**

**49. Q. What can you tell about the tar Command?**

**A. The tar program is an immensely useful archiving utility. It can combine**

**an entire directory tree into one large file suitable for transferring or**

**compression.**

**50. Q. What types of files you know?**

**A. Files come in eight flavors:**

**Normal files**

**Directories**

**Hard links**

**Symbolic links**

**Sockets**

**Named pipes**

**Character devices**

**Block devices**

**51. Q. How to copy files from on PC to another on the same network**

**A. Use the following command:scp yur\_file you\_login@your\_IP**

**example: copy .conf file from your PC to alex computer-**

**scp /etc/X11/xorg.conf alex@10.0.10.169:**

**52. Q. Please describe information below:**

**-rw-rw-r-- 1 dotpc dotpc 102 Jul 18 2003 file.buf**

**drwxr-xr-x 9 dotpc dotpc 4096 Oct 21 09:34 bin**

**lrwxrwxrwx 1 dotpc dotpc 20 Mar 21 15:00 client -> client-2.9.5**

**drwxrwxr-x 11 dotpc dotpc 4096 Sep 2 2005 client-2.8.9**

**drwxrwxr-x 7 dotpc dotpc 4096 Dec 14 12:13 data**

**drwxr-xr-x 12 dotpc dotpc 4096 Oct 21 09:41 docs**

**drwxr-xr-x 5 dotpc dotpc 4096 Dec 7 14:22 etc**

**drwxr-xr-x 11 dotpc dotpc 4096 Mar 21 15:54 client-2.9.5**

**-rw-r--r-- 1 dotpc dotpc 644836 Mar 22 09:53 client-2.9.5.tar.gz**

**A. This is a result of command $ls -l**

**we have two files, 6 directories and one link to client-2.9.5 directory.**

**There is number of files in every directory, size and data of last change.**

**53. Q. If you would like to run two commands in sequence what operators you can use?**

**A. ; or && the difference is:**

**if you separate commands with ; second command will be run automatically.**

**if you separate commands with && second command will be run only in the case**

**the first was run successfully.**

**54. Q. How you will uncompress the file?**

**A. Use tar command (The GNU version of the tar archiving utility):**

**tar -zxvf file\_name.tar.gz**

**55. Q.How do you execute a program or script, my\_script in your current directoty?**

**A. ./my\_script**

**56. Q.How to find current time configuration in the file my\_new.cfg**

**A. grep time my\_new.cfg**

**Grep searches the named input files (or standard input if**

**no files are named, or the file name - is given) for lines**

**containing a match to the given pattern.**

**Q. What does grep() stand for?**

**A. General Regular Expression Parser.**

**57. Q. What does the top command display?**

**A. Top provides an ongoing look at processor activity in real**

**time. It displays a listing of the most CPU-intensive**

**tasks on the system, and can provide an interactive inter­**

**face for manipulating processes. (q is to quit)**

**58. Q. How can you find configuration on linux?**

**A. by using /sin/ifconfig**

**If no arguments are given, ifconfig displays the status of the cur-**

**rently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argu-**

**ment is given, it displays the status of all interfaces, even those**

**that are down. Otherwise, it configures an interface.**

**59. Q. How to find difference in two configuration files on the same server?**

**A. Use diff command that is compare files line by line**

**diff -u /usr/home/my\_project1/etc/ABC.conf /usr/home/my\_project2/etc/ABC.conf**

**60. Q. What is the best way to see the end of a logfile.log file?**

**A. Use tail command - output the last part of files**

**tail -n file\_name ( the last N lines, instead of the last 10 as default)**

**61. Q. Please write a loop for removing all files in the current directory that contains a word 'log'**

**A. for i in \*log\*; do rm $i; done**

**62. Question: How to switch to a previously used directory?**

**Answer: cd -**

**1. Q.How many VI editor modes do you know?**

**A.Three modes -**

**Command mode: letters or sequence of letters interactively command vi.**

**Insert mode: Text is inserted.**

**Command line mode: enter this mode by typing ":" and entry command line at the foot of the screen.**

**2. Q. How can you terminate VI session?**

**A.**

** Use command: ZZ that is save changes and quit.**

** Use command line: ":wq" that is write changes and quit.**

** Use command line: ":q!" to ignore changes and quit.**

**3. Q. How can you copy lines into the buffer in command mode?**

**A.**

**yy - copy a single line defined by current cursor position**

**3yy - copy 3 lines. Current line and two lines below it.**

**Linux Frequently Asked Interview question From Google IBM HCL Infosys**

|  |
| --- |
|  |

what is Partition Tool in all the Linux Distribution  
**fdisk**, using fdisk command we can make the partition table.  
  
How to view the boot message  
**/var/log/messages** File  
#**dmesg** using these these command we can see the boot messages  
**/var/log/lastlog** file contain Information about the used defined passwd in the last logged.  
**/var/log/httpd/error\_log** httpd log file  
**/var/log/httpd/access\_log** >>Httpd Access Log  
  
How to set the DHCP range 192.168.1.2 to 192.168.1.20  
not include 192.168.1.4, 192.168.1.7, 192.168.1.10  
subnet 192.168.1.0 netmask 255.255.255.0  
{  
range 192.168.1.2 192.168.1.3;  
range 192.168.1.5 192.168.1.6;  
range 192.168.1.8 192.168.1.9;  
}  
How to delete the user Home Directory  
**#userdel -r username**  
It will delte the user and there user home directory  
  
How to create the user with Home Directory  
#**adduser -m username**  
it will create the user with home directory  
  
How to change the username  
#**usermod -l newusername oldusername**  
  
Several user want to schedule the at job at peak time , How can we prevent user schedule the job.  
In server Load is too high, How can we avoid the user to schedule job at these time  
**Remove /etc/at.deny file**  
Then only superuser they can schedule the job.  
  
What are the two utilities can be used to schedule the job  
**at and crontab**  
  
we are haveing the two IDE drive we plan to make the Two partition For each device  
what will be the name of the device  
**hda1,hda2,** First IDE device Two partition  
**hdb1,hdb2** Second IDE device Two partition  
  
**what is xinetd service**  
xinetd it is exted Internet Daemon.  
it will maintain the Internet based connectivity.  
xinetd it is only responsible daemon to listen the port number which are service listed under /etc/xinetd.conf or /etc/services.  
It will maintain the Internet related service.  
ftp,telnet,nagios,  
  
**How to use awk Command**  
[root@unix ~]#ls -l  
total 8440  
-rw-r--r-- 1 root root 19 Oct 12 16:31 1  
-rw-r--r-- 1 root root 19 Oct 12 16:31 default.php  
-rw-r--r-- 1 root root 20 Oct 12 16:16 file  
-rw-r--r-- 1 root root 14 Oct 12 16:26 index.hp  
[root@unix ~]#**ls -l | awk '{ print $3 } '** >> It will display only the thrid parameter   
root  
root  
root  
root  
nagios  
  
**Difference Between du and df Command**

df - display free disk space

#**df bin/**  
Filesystem 1K-blocks Used Available Use% Mounted on  
/dev/sda1 10321208 1732180 8064740 18% /  
#**df tmp/**  
Filesystem 1K-blocks Used Available Use% Mounted on  
/dev/sda1 10321208 1732188 8064732 18% /  
df command It will display the free disk space for the particular directory and it shows where it is mounted  
#**df -h bin/ >> -h** refres to the Human Readable form  
Filesystem Size Used Avail Use% Mounted on  
/dev/sda1 9.9G 1.7G 7.7G 18% /  
  
**How To Check The Maximum File size For current directory - Disk Management**

**du -** display free disk usage

**du -h** >> List out the all the directory of File System  
#**du -sh >> Total size of the current directory**  
1.6G .  
#**du -sh \*** >> list only the current directory & separate files  
5.6M bin  
156K boot  
40K dev  
13M etc  
40K home  
**du -sh /home/\* >> list only from the /home directory**  
**How to Check the Maximum File Size under Current Directory**  
du -h   
du -sh >> Total l size of the current rectory  
du -sh \* >> list only the current directory  
du -sh /home/\* >> list only from the /home directory  
**-h Human Readable Form  
-s Summary**  
#**du -sm \* | sort -nr | head -1**  
29 nagios-3.2.1  
  
What are the shutdown command Different Option  
**shutdown -r** is used to restart the system,  
**shutdown -f** restart the sytem fast skiping fsck, -F Force to fsck on reboot  
**shutdown -h** halt the system after shutdown.  
shutdown -h now "message"  
shutdown -h hh:mm "message"  
To restart the system  
shutdown -r now "message"  
shutdown -r +10 "message"  
**reboot,shutdown -r, init 6** using the command we can restart the system.  
  
Which daemon is responsible for tracking the log files  
**syslogd** daemon is responsible for tracking system information and saving to specified log files  
  
what command has been used to check the no of files and disk space used in the each user quota  
**repquota** using repquota command we can check the no of the files and dispace space  
  
what command is used to find in which shell we are working  
[root@nagm ~]#**echo $SHELL**  
/bin/bash  
  
How To create The RAID level 5  
#madam -**c** /dev/md0 yes **-l 5 -n 3** /dev/{hda1,2} >> create  
#madam -D /dev/md0 >> Display infromation  
create the file system  
mkfs.ext3 /dev/md0  
mkdir /tags  
mount /dev/md0 /tags  
  
**What is Linux**  
Linux it is only kernal.  
Combine with Gui mode it will form OS.  
Linux is developed by the source code of unix kernel  
  
**What is NIS**  
NIS in windows called **Active Directory**.  
we can create the user in NIS server and we can use the user in anywhere in the domain  
nis it is provide the **centralization of user** it refers to the configure the nis server and add the user and these user can login in anywhere  
**kerberos it is digital Signature**,  
it is used for authentication scheme.  
it is used to send the data form the one system to another system in encrypted data.  
  
**what is ldd**  
linux digital driver  
  
what is zombie process?  
**zombie is inactive process:**The Process ids dead but it have not been removed from the process table.Zombie process in the other words it is complete the process execution but still entry in the process table.zombie process it is already dead, but it is waiting for parent process to reap them.zombie it is derives form the definition zombie - undead person.  
to kill these process kill.  
zombie process can be identified by z form the output of ps command.  
it can be killed by kill -9 and kill -15.  
  
**How To Identify Zombie Process**  
#ps -el | grep 'z'  
  
**How to kill zombie Process**  
If the process can not be kill directly by the kill -9 or 15 [what is reason - child process is created by parent process but the parent process will leave it,] So we need to send the signal to the process  
#**kill -s SIGCHLD [process id]**  
-s send the signal to the process.  
  
what is **CUPS**  
Common UNIX Printer System  
it is provide the printer service to the Linux system.  
  
**Copy File using Scp From One Remote Machine to Another**  
Using SCP We Can Transfer File  
Remote system >> Local Systemscp   
#root@67.228.6.3:/script/script.tar /home/centos  
Local System >> Remote System  
#scp /home/centos/script.tar root@67.228.6.3:~   
Remote System >> Local System  
  
**How To Compress File**  
#tar -cvf destion.tar /sourcefile  
  
**How to uncompress file**  
tar -xvf <filename>  
bunzip2 <filename>  
gunzip <filename>  
unzip <filename>

**Linux System Admin Interview Questions & Answers part 1**

1. Every command in Linux is a

answer : executable program  
  
2. How long can a filename in Linux be?  
Correct answer: 255 characters  
  
3. What is the shortcut to the login directory?  
Correct answer: cd + enter key  
  
4. The hierarchy of a series of directories branching in a user system starts from  
Correct answer: /home  
  
5. Saving open files, flush the system cache and other necessary system maintenance are allowed by.  
Correct answer: logging off the system  
  
6. Which directory contains configuration files that stores system and application setting?  
Correct answer: /etc  
  
7. Which command is used to find data files, programs, directories that match the search argument?  
Correct answer: locate  
  
8. Applications written to provide a GUI shell for Unix and Linux are called  
Correct answer: x windows  
  
9. The advantage of using NFS rather than Samba for file sharing in Linux is  
Correct answer: compatibility with Windows file sharing  
  
10. Which framework is provided for the programs to interchange information about Linux OS?  
Correct answer: Resource Definition Framework  
  
11. To implement new application on IBM z/10. Which of the following options need to be considered if it to be implemented in Linux?  
Correct answer: Red Hat Linux does not support all the devices supported by IBM z/OS  
  
12. Which of the following has greater market share of Linux SW/HW environment?  
Correct answer: Linux on z10  
  
13. Which of the following commands can be run to remove all the rules in an iptables table?  
Correct answer: iptables -F  
  
14. Which of the following is the BEST way to set up SSH(Secure Shell) for communicating between Systems without needing passwords?  
Correct answer: Use ssh-keygen for generating public-private keys.  
  
15. How much usable space is available, when a Linux system is configured with a RAID 5 array that consists of six 20 GB hard disk drives?  
Correct answer: 100Gb  
  
Formula: S\*(N-1)  
here S=size  
N=number of HDD. remember it is only for RAID5  
  
16. Which of the following commands can be used to check for file corruption?  
Correct answer: md5sum  
  
17. Which of the following allows to secure remote command line access?  
Correct answer: SSH(Secure Shell)  
  
18. Which of the following supports for creating a Linux VPN (Virtual Private Network)?  
Correct answer: 3DES  
  
19. Which of the following commands delete the files from the /tmp directory, issued by non-root user?  
Correct answer: su -c "rm -rf /tmp/\*"  
  
20. Which configuration does cardmgr read at Linux system startup?  
Correct answer: PCMCIA cards  
  
21. When a computer system is reported problems with inodes and blocks, which of the following is the problem and its solution to rectify it?  
Correct answer: The file system has become corrupt and needs to be repaired.  
  
22. Which Linux command will successfully mounts a USB drive?  
Correct answer: mount /dev/sda1 /mnt/usb  
  
23. \_\_\_\_\_\_\_\_\_\_\_ is a common tool for determining services and ports running on a remote Linux.  
Correct answer: nmap  
  
24. For supporting new diskless client workstations, which of the following services needs to be installed on a server?  
Correct answer: PXE (Preboot eXecution Environment) and tftpd  
  
25. Which of the following will kill the process 1010 by an administrator(logged in as a standard user)? The process 1010 was started by the root user.  
Correct answer: su -c "kill 1010"  
  
26. Which of the following Linux commands could be used to find what processor was detected on boot, when a laptop system is slow/  
Correct answer: POST  
  
27. How to accomplish the LILO boot configuration updation for supporting a newly installed IDE hard drive?  
Correct answer: Edit lilo.conf and run "lilo -v -v"

<http://www.linuxhowto.in/2012/07/dns-server-interview-questions-answers.html>

what is DNS?  
why we required CHROOT package? can you explain it?  
What is the location for DHCP server default leased configs file?  
what is the command and syntax to check DNS server named.conf file errors?  
What is the command and syntax to check DNS server zone files config errors?  
How do you update DNS zone file entries with out restarting named demon?  
What are the services/demons will restart when you restart NFS service?  
how do you update NFS sharing details with out restarting NFS server?  
What are the advantages of NIS?  
Can you explain me about LVM and how you configure LVM?  
What is the difference between LVM1 and LVM2?  
What is Amanda server and where is it used?  
Can you explain me corntab?  
How to resize LVM?  
Can you explain me about RAID5?  
How many RAID devices are there in RHEL5 by default?  
Min how many Raid devices will participate in RAID5?  
How do you do Kernel patching and what is the command?  
Can you explain me about in details how you do kernel recompilation?  
Can you explain what is the use fo access file in sendmail and what is its location?  
Can you explain me what is the advantage of local-hosts file and virtusertable in sendmail?  
How you will specify static IP’s in DHCP server?  
how do you update NIS users with out restarting the NIS server?  
What is the partation no for LVM?  
What is the partation no for RAID?  
What is the port no for DNS?  
Can we change default port no for DNS? if yes, how?  
How many RAID device we can create in RHEL4?  
Can you explain me Disk quota in detail and configuration details?  
How to increase RAID devices after it excied max limit?

### UNIX - LINUX Interview Questions and Answers :

**1. How are devices represented in UNIX?**

All devices are represented by files called special files that are located in/dev directory. Thus, device files and other files are named and accessed in the same way. A 'regular file' is just an ordinary data file in the disk. A 'block special file' represents a device with characteristics similar to a disk (data transfer in terms of blocks). A 'character special file' represents a device with characteristics similar to a keyboard (data transfer is by stream of bits in sequential order).

**2. What is 'inode'?**

All UNIX files have its description stored in a structure called 'inode'. The inode contains info about the file-size, its location, time of last access, time of last modification, permission and so on. Directories are also represented as files and have an associated inode. In addition to descriptions about the file, the inode contains pointers to the data blocks of the file. If the file is large, inode has indirect pointer to a block of pointers to additional data blocks (this further aggregates for larger files). A block is typically 8k.  
Inode consists of the following fields:

* File owner identifier
* File type
* File access permissions
* File access times
* Number of links
* File size
* Location of the file data

**3. Brief about the directory representation in UNIX**

A Unix directory is a file containing a correspondence between filenames and inodes. A directory is a special file that the kernel maintains. Only kernel modifies directories, but processes can read directories. The contents of a directory are a list of filename and inode number pairs. When new directories are created, kernel makes two entries named '.' (refers to the directory itself) and '..' (refers to parent directory).  
System call for creating directory is mkdir (pathname, mode).

**4. What are the Unix system calls for I/O?**

* open(pathname,flag,mode) - open file
* creat(pathname,mode) - create file
* close(filedes) - close an open file
* read(filedes,buffer,bytes) - read data from an open file
* write(filedes,buffer,bytes) - write data to an open file
* lseek(filedes,offset,from) - position an open file
* dup(filedes) - duplicate an existing file descriptor
* dup2(oldfd,newfd) - duplicate to a desired file descriptor
* fcntl(filedes,cmd,arg) - change properties of an open file
* ioctl(filedes,request,arg) - change the behaviour of an open file

The difference between fcntl anf ioctl is that the former is intended for any open file, while the latter is for device-specific operations.

**5. How do you change File Access Permissions?**

Every file has following attributes:  
owner's user ID ( 16 bit integer )  
owner's group ID ( 16 bit integer )  
File access mode word

'r w x -r w x- r w x'

(user permission-group permission-others permission)  
r-read, w-write, x-execute  
To change the access mode, we use chmod(filename,mode).  
Example 1:  
To change mode of myfile to 'rw-rw-r–' (ie. read, write permission for user - read,write permission for group - only read permission for others) we give the args as:  
chmod(myfile,0664) .  
Each operation is represented by discrete values

'r' is 4  
'w' is 2  
'x' is 1

Therefore, for 'rw' the value is 6(4+2).  
Example 2:  
To change mode of myfile to 'rwxr–r–' we give the args as:

chmod(myfile,0744).

**6. What are links and symbolic links in UNIX file system?**

A link is a second name (not a file) for a file. Links can be used to assign more than one name to a file, but cannot be used to assign a directory more than one name or link filenames on different computers.  
Symbolic link 'is' a file that only contains the name of another file.Operation on the symbolic link is directed to the file pointed by the it.Both the limitations of links are eliminated in symbolic links.  
Commands for linking files are:

Link ln filename1 filename2  
Symbolic link ln -s filename1 filename2

**7. What is a FIFO?**

FIFO are otherwise called as 'named pipes'. FIFO (first-in-first-out) is a special file which is said to be data transient. Once data is read from named pipe, it cannot be read again. Also, data can be read only in the order written. It is used in interprocess communication where a process writes to one end of the pipe (producer) and the other reads from the other end (consumer).

8. How do you create special files like named pipes and device files?

The system call mknod creates special files in the following sequence.  
1. kernel assigns new inode,  
2. sets the file type to indicate that the file is a pipe, directory or special file,  
3. If it is a device file, it makes the other entries like major, minor device numbers.  
For example:  
If the device is a disk, major device number refers to the disk controller and minor device number is the disk.

**9. Discuss the mount and unmount system calls**

The privileged mount system call is used to attach a file system to a directory of another file system; the unmount system call detaches a file system. When you mount another file system on to your directory, you are essentially splicing one directory tree onto a branch in another directory tree. The first argument to mount call is the mount point, that is , a directory in the current file naming system. The second argument is the file system to mount to that point. When you insert a cdrom to your unix system's drive, the file system in the cdrom automatically mounts to /dev/cdrom in your system.

**10. How does the inode map to data block of a file?**

Inode has 13 block addresses. The first 10 are direct block addresses of the first 10 data blocks in the file. The 11th address points to a one-level index block. The 12th address points to a two-level (double in-direction) index block. The 13th address points to a three-level(triple in-direction)index block. This provides a very large maximum file size with efficient access to large files, but also small files are accessed directly in one disk read.

**11. What is a shell?**

A shell is an interactive user interface to an operating system services that allows an user to enter commands as character strings or through a graphical user interface. The shell converts them to system calls to the OS or forks off a process to execute the command. System call results and other information from the OS are presented to the user through an interactive interface. Commonly used shells are sh,csh,ks etc.

**12. Brief about the initial process sequence while the system boots up.**

While booting, special process called the 'swapper' or 'scheduler' is created with Process-ID 0. The swapper manages memory allocation for processes and influences CPU allocation. The swapper inturn creates 3 children:

* the process dispatcher,
* vhand and
* dbflush

with IDs 1,2 and 3 respectively.  
This is done by executing the file /etc/init. Process dispatcher gives birth to the shell. Unix keeps track of all the processes in an internal data structure called the Process Table (listing command is ps -el).

**13. What are various IDs associated with a process?**

Unix identifies each process with a unique integer called ProcessID. The process that executes the request for creation of a process is called the 'parent process' whose PID is 'Parent Process ID'. Every process is associated with a particular user called the 'owner' who has privileges over the process. The identification for the user is 'UserID'. Owner is the user who executes the process. Process also has 'Effective User ID' which determines the access privileges for accessing resources like files.

* getpid() -process id
* getppid() -parent process id
* getuid() -user id
* geteuid() -effective user id

**14. Explain fork() system call.**

The `fork()' used to create a new process from an existing process. The new process is called the child process, and the existing process is called the parent. We can tell which is which by checking the return value from `fork()'. The parent gets the child's pid returned to him, but the child gets 0 returned to him.

**15. Predict the output of the following program code**

main()  
{  
fork();  
printf("Hello World!");  
}

Answer:

Hello World!Hello World!

**Explanation:**  
The fork creates a child that is a duplicate of the parent process. The child begins from the fork().All the statements after the call to fork() will be executed twice.(once by the parent process and other by child). The statement before fork() is executed only by the parent process.

**16. Predict the output of the following program code**

main()  
{  
fork(); fork(); fork();  
printf("Hello World!");  
}

Answer:  
"Hello World" will be printed 8 times.  
**Explanation:**  
2^n times where n is the number of calls to fork()

**17. List the system calls used for process management:**

System calls Description

* fork() To create a new process
* exec() To execute a new program in a process
* wait() To wait until a created process completes its execution
* exit() To exit from a process execution
* getpid() To get a process identifier of the current process
* getppid() To get parent process identifier
* nice() To bias the existing priority of a process
* brk() To increase/decrease the data segment size of a process.

**18. How can you get/set an environment variable from a program?**

Getting the value of an environment variable is done by using `getenv()'. Setting the value of an environment variable is done by using `putenv()'.

**19. How can a parent and child process communicate?**

A parent and child can communicate through any of the normal inter-process communication schemes (pipes, sockets, message queues, shared memory), but also have some special ways to communicate that take advantage of their relationship as a parent and child. One of the most obvious is that the parent can get the exit status of the child.

**20. What is a zombie?**

When a program forks and the child finishes before the parent, the kernel still keeps some of its information about the child in case the parent might need it - for example, the parent may need to check the child's exit status. To be able to get this information, the parent calls `wait()'; In the interval between the child terminating and the parent calling `wait()', the child is said to be a `zombie' (If you do `ps', the child will have a `Z' in its status field to indicate this.)

**21. What are the process states in Unix?**

As a process executes it changes state according to its circumstances. Unix processes have the following states:  
**Running** : The process is either running or it is ready to run .  
**Waiting** : The process is waiting for an event or for a resource.  
**Stopped** : The process has been stopped, usually by receiving a signal.  
**Zombie** : The process is dead but have not been removed from the process

c The useradd command will use the system default for the user's homedirectory. The home directory is not created, however, unless you use the -moption.

You want to enter a series of commands from the command-line. Whatwould be the quickest way to do this?

Choose Onea. Press enter after entering each command and its argumentsb. Put them in a script and execute the scriptc. Separate each command with a semi-colon (;) and press enterafter the last commandd. Separate each command with a / and press enter after the lastcommand

c The semi-colon may be used to tell the shell that you are entering multiplecommands that should be executed serially. If these were commands that youwould frequently want to run, then a script might be more efficient. However,to run these commands only once, enter the commands directly at thecommand line.

You attempt to use shadow passwords but are unsuccessful. Whatcharacteristic of the /etc/passwd file may cause this?

Choose one:a. The login command is missing.b. The username is too long.c. The password field is blank.d. The password field is prefaced by an asterisk.

c The password field must not be blank before converting to shadow passwords.

When you install a new application, documentation on that application isalso usually installed. Where would you look for the documentation afterinstalling an application called MyApp?

Choose one:a. /usr/MyAppb. /lib/doc/MyAppc. /usr/doc/MyAppd. In the same directory where the application is installed.

c The default location for application documentation is in a directory named forthe application in the /usr/doc directory.

What file would you edit in your home directory to change which windowmanager you want to use?

A) XinitB) .xinitrcC) XF86SetupD) xstartE) xf86init

Answer: B - The ~/.xinitrc file allows you to set which window man-ager youwant to use when logging in to X from that account.Answers a, d, and e are all invalid files. Answer c is the main X serverconfiguration file.

What command allows you to set a processor-intensive job to use lessCPU time?

A) psB) niceC) chpsD) lessE) more

Answer: B - The nice command is used to change a job's priority level, so thatit runs slower or faster. Answers a, d, and e are valid commands but are notused to change process information. Answer c is an invalid command.

While logged on as a regular user, your boss calls up and wants you tocreate a new user account immediately. How can you do this without firsthaving to close your work, log off and logon as root?

Choose one:a. Issue the command rootlog.b. Issue the command su and type exit when finished.c. Issue the command su and type logoff when finished.d. Issue the command logon root and type exit when finished.

Answer: b You can use the su command to imitate any user including root. You will beprompted for the password for the root account. Once you have provided ityou are logged in as root and can do any administrative duties.

There are seven fields in the /etc/passwd file. Which of the followinglists all the fields in the correct order?

Choose one:a. username, UID, GID, home directory, command, commentb. username, UID, GID, comment, home directory, commandc. UID, username, GID, home directory, comment, commandd. username, UID, group name, GID, home directory, comment

Answer: b The seven fields required for each line in the /etc/passwd file are username,UID, GID, comment, home directory, command. Each of these fields must beseparated by a colon even if they are empty.

Which of the following commands will show a list of the files in yourhome directory including hidden files and the contents of allsubdirectories?

Choose one:a. ls -c homeb. ls -aR /home/usernamec. ls -aF /home/usernamed. ls -l /home/username

Answer: b The ls command is used to display a listing of files. The -a option will causehidden files to be displayed as well. The -R option causes ls to recurse downthe directory tree. All of this starts at your home directory.

In order to prevent a user from logging in, you can add a(n)

\_\_\_\_\_\_\_\_

atthe beginning of the password field.

Answer: asterickIf you add an asterick at the beginning of the password field in the/etc/passwd file, that user will not be able to log in.

You have a directory called /home/ben/memos and want to move itto /home/bob/memos so you issue the command mv/home/ben/memos /home/bob. What is the results of this action?

Choose one:a. The files contained in /home/ben/memos are moved to thedirectory /home/bob/memos/memos.b. The files contained in /home/ben/memos are moved to thedirectory /home/bob/memos.c. The files contained in /home/ben/memos are moved to thedirectory /home/bob/.d. The command fails since a directory called memos already existsin the target directory.

Answer: aWhen using the mv command to move a directory, if a directory of the samename exists then a subdirectory is created for the files to be moved.

Which of the following tasks is not necessary when creating a new userby editing the /etc/passwd file?

Choose one:a. Create a link from the user's home directory to the shell the userwill use.b. Create the user's home directoryc. Use the passwd command to assign a password to the account.d. Add the user to the specified group.

Answer: a There is no need to link the user's home directory to the shell command.Rather, the specified shell must be present on your system.

You issue the following command useradd -m bobm But the user cannotlogon. What is the problem?

Choose one:a. You need to assign a password to bobm's account using thepasswd command.b. You need to create bobm's home directory and set the appropriatepermissions.c. You need to edit the /etc/passwd file and assign a shell for bobm'saccount.d. The username must be at least five characters long.

Answer: a The useradd command does not assign a password to newly createdaccounts. You will still need to use the passwd command to assign apassword.

You wish to print the file vacations with 60 lines to a page. Which of thefollowing commands will accomplish this? Choose one:

1. pr -l60 vacations | lprb. pr -f vacations | lpr

**Which file defines all users on your system?  
Choose one:  
a. /etc/passwd  
b. /etc/users  
c. /etc/password  
d. /etc/user.conf**

Answer: a  
The /etc/passwd file contains all the information on users who may log into your system. If a user account is not contained in this file, then the user cannot log in.

**Which two commands can you use to delete directories?  
A) rm  
B) rm -rf  
C) rmdir  
D) rd  
E) rd -rf**

Answer(s): B, C – You can use rmdir or rm -rf to delete a directory. Answer a is incorrect, because the rm command without any specific flags will not delete a directory, it will only delete files. Answers d and e point to a non-existent command.

**Which partitioning tool is available in all distributions?  
A) Disk Druid  
B) fdisk  
C) Partition Magic  
D) FAT32  
E) System Commander**

Answer(s): B – The fdisk partitioning tool is available in all Linux distributions. Answers a, c, and e all handle partitioning, but do not come with all distributions. Disk Druid is made by Red Hat and used in its distribution along with some derivatives. Partition Magic and System Commander are tools made by third-party companies. Answer d is not a tool, but a file system type. Specifically, FAT32 is the file system type used in Windows 98.

**Which partitions might you create on the mail server’s hard drive(s) other than the root, swap, and boot partitions?  
[Choose all correct answers]  
A) /var/spool  
B) /tmp  
C) /proc  
D) /bin  
E) /home**  
Answer(s): A, B, E – Separating /var/spool onto its own partition helps to ensure that if something goes wrong with the mail server or spool, the output cannot overrun the file system. Putting /tmp on its own partition prevents either software or user items in the /tmp directory from overrunning the file system. Placing /home off on its own is mostly useful for system re-installs or upgrades, allowing you to not have to wipe the /home hierarchy along with other areas. Answers c and d are not possible, as the /proc portion of the file system is virtual-held in RAM-not placed on the hard drives, and the /bin hierarchy is necessary for basic system functionality and, therefore, not one that you can place on a different partition.

**When planning your backup strategy you need to consider how often you will perform a backup, how much time the backup takes and what media you will use. What other factor must you consider when planning your backup strategy? \_\_\_\_\_\_\_\_\_**

what to backup  
Choosing which files to backup is the first step in planning your backup strategy.

**What utility can you use to automate rotation of logs?**  
Answer: logrotate  
The logrotate command can be used to automate the rotation of various logs.

**In order to display the last five commands you have entered using the history command, you would type \_\_\_\_\_\_\_\_\_\_\_ .**

Answer: history 5  
The history command displays the commands you have previously entered. By passing it an argument of 5, only the last five commands will be displayed.

**What command can you use to review boot messages?**  
Answer: dmesg  
The dmesg command displays the system messages contained in the kernel ring buffer. By using this command immediately after booting your computer, you will see the boot messages.

**What is the minimum number of partitions you need to install Linux?**  
Answer: 2  
Linux can be installed on two partitions, one as / which will contain all files and a swap partition.

**What is the name and path of the main system log?**  
Answer: /var/log/messages  
By default, the main system log is /var/log/messages.

**Of the following technologies, which is considered a client-side script?  
A) JavaScript  
B) Java  
C) ASP  
D) C++**

Answer: A – JavaScript is the only client-side script listed. Java and C++ are complete programming languages. Active Server Pages are parsed on the server with the results being sent to the client in HTML

**What file defines the levels of messages written to system log files?**  
kernel.h

To determine the various levels of messages that are defined on your system, examine the kernel.h file.

**What command is used to remove the password assigned to a group?**  
gpasswd -r

The gpasswd command is used to change the password assigned to a group. Use the -r option to remove the password from the group.

**What command would you type to use the cpio to create a backup called backup.cpio of all the users’ home directories?**  
find /home | cpio -o > backup.cpio

The find command is used to create a list of the files and directories contained in home. This list is then piped to the cpio utility as a list of files to include and the output is saved to a file called backup.cpio.

**What can you type at a command line to determine which shell you are using?**  
echo $SHELL

The name and path to the shell you are using is saved to the SHELL environment variable. You can then use the echo command to print out the value of any variable by preceding the variable’s name with $. Therefore, typing echo $SHELL will display the name of your shell.

**What type of local file server can you use to provide the distribution installation materials to the new machine during a network installation?  
A) Inetd  
B) FSSTND  
C) DNS  
D) NNTP  
E) NFS**  
E – You can use an NFS server to provide the distribution installation materials to the machine on which you are performing the installation. Answers a, b, c, and d are all valid items but none of them are file servers. Inetd is the superdaemon which controls all intermittently used network services. The FSSTND is the Linux File System Standard. DNS provides domain name resolution, and NNTP is the transfer protocol for usenet news.

**If you type the command cat dog & > cat what would you see on your display? Choose one:  
a. Any error messages only.  
b. The contents of the file dog.  
c. The contents of the file dog and any error messages.  
d. Nothing as all output is saved to the file cat.**  
d

When you use & > for redirection, it redirects both the standard output and standard error. The output would be saved to the file cat.

**You are covering for another system administrator and one of the users asks you to restore a file for him. You locate the correct tarfile by checking the backup log but do not know how the directory structure was stored. What command can you use to determine this?  
Choose one:  
a. tar fx tarfile dirname  
b. tar tvf tarfile filename  
c. tar ctf tarfile  
d. tar tvf tarfile**

d

The t switch will list the files contained in the tarfile. Using the v modifier will display the stored directory structure.

**You have the /var directory on its own partition. You have run out of space. What should you do? Choose one:  
a. Reconfigure your system to not write to the log files.  
b. Use fips to enlarge the partition.  
c. Delete all the log files.  
d. Delete the partition and recreate it with a larger size.**

d

The only way to enlarge a partition is to delete it and recreate it. You will then have to restore the necessary files from backup.

**You have a new application on a CD-ROM that you wish to install. What should your first step be?  
Choose one:  
a. Read the installation instructions on the CD-ROM.  
b. Use the mount command to mount your CD-ROM as read-write.  
c. Use the umount command to access your CD-ROM.  
d. Use the mount command to mount your CD-ROM as read-only.**

d

Before you can read any of the files contained on the CD-ROM, you must first mount the CD-ROM.

**When you create a new partition, you need to designate its size by defining the starting and ending \_\_\_\_\_\_\_\_\_\_\_\_\_.**  
cylinders

When creating a new partition you must first specify its starting cylinder. You can then either specify its size or the ending cylinder.

**1) What is Linux?**

Linux is an operating system based on UNIX, and was first introduced by Linus Torvalds. 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.

**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?**

[](http://cdn.gointerviews.com/wp-content/uploads/2012/06/linux.jpg)

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 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

**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

**How to check all open ports on linux machine and block unsed ports?**  
netstat -t  
#nmap -v localhost for tcp  
#nmap -sU localhost for udp  
  
#netstat -tulp  
or  
#netstat -tulpn  
  
to verfy the open ports  
-------------------------------  
\* **how u use the iptable firewall to restrict ssh,telnet,ftp**  
For SSH  
iptables -A INPUT -s -p tcp --dport <22> -j  
REJECT/DROP/DENY  
  
For Telnet  
iptables -A INPUT -s -p tcp --dport <23> -j  
REJECT/DROP/DENY  
  
For FTP  
iptables -A INPUT -s -p tcp --dport <21> -j  
REJECT/DROP/DENY  
  
-------------------------------------  
  
\* **what is the difference between unix and linux**  
  
graphics is the main difference  
extra more command are in linux  
userfriendly then unix  
  
the unix is the platform dependent the linux is platform  
independent. we cann't install unix in all machine we  
recquired a special machine to install unix, but linux is  
not like that it support all machines  
  
filesystem are different  
there diff lies in kernel  
linux is under gpl and unix proprietary  
  
Difference Between Linux and Unix  
1)Linux default shell is /bin/bash, where Unix default shell  
is /bin/sh (other shell also supported)  
2) Linux Store all their command history,but if the default  
shell is /bin/sh in Unix, then Unix not store Command history.  
3) Linux support Tab key, but unix not support Tab key  
-------------------------------------  
  
**Who owns the data dictionary?**  
  
The Oracle user SYS owns all base tables and user-  
accessible views of the data dictionary. Therefore, no  
Oracle user should ever alter (update, delete, or insert)  
any rows or schema objects contained in the SYS schema,  
because such activity can compromise data integrity. The  
security administrator should keep strict control of this  
central account.  
  
-------------------------------------  
**which file contains information about os wether it's 32**  
**bit or 64 bit?**  
  
ANS: /proc/cpuinfo  
or  
$uname -m  
or  
/usr/bin/file  
--------------------------------  
**what contains information about file and directory creating time or modification time?**  
  
An inode is a data structure on a Unix / Linux file system.  
An inode stores basic information about a regular file,  
directory, or other file system object. You can use  
following two commands to display an inode:  
  
[a] ls command : list directory contents  
  
-----------------------------------  
**What are RPM?s, what do they offer?**  
  
The full form of RPM is Redhat Package Manager.  
rpm is a powerful Package Manager, which can be used  
to build,install, query, verify, update, and erase  
individual software packages. A package consists of an  
archive of files and meta-data used to install and erase the  
archive files.  
  
[b] stat command : display file or file system status  
  
eg : # stat /etc/passwd  
Output:  
File: `/etc/group'  
Size: 566 Blocks: 16 IO Block: 4096  
regular file  
Device: fd00h/64768d Inode: 2443679 Links: 1  
Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: (  
0/ root)  
Access: 2009-08-12 08:23:31.245032672 +0530  
Modify: 2002-01-01 05:54:15.000000000 +0530  
Change: 2002-01-01 05:54:15.000000000 +0530  
--------------------------------------------------  
\***how to confirm from client end about nfs server sharing?**  
  
with mount and showmount -e server IP  
  
-------------------------------------------------  
**How do i check which nfs version I am using ?**  
  
rpcinfo -p localhost | grep -i nfs  
  
This cmd is used for nfs version  
rpm -qa | grep nfs  
rpm -qi nfs nfs-utils  
yum info nfs nfs-utils  
  
------------------------------------------------  
**Through ssh whole directory structure from / is shared regardless the user we have connected with ....... how do i prevent sharing ??**  
  
vi /etc/ssh/sshd\_config  
"in last line enter the folowing entry"  
AllowUsers "username"  
  
And  
  
vi /etc/hosts.deny  
"in last line enter the folowing entry"  
sshd: ALL EXCEPT "DOMAIN-NAME"  
  
its benefitial to use setfacl command for secure your  
stuff..  
-------------------------------------------------------  
\* **what restrict telnet for root itself but allow for other user**  
  
Root can login through telnet session, but by default it is  
disabled. You can enable by appending /etc/securetty file  
open /etc/securetty using vi  
  
#vi /etc/securetty  
  
pts/0  
pts/1  
  
don't remove anything from this /etc/securetty , just  
append your entry  
  
vi /etc/pam.d/login  
  
auth required pam\_securetty.so== 1st line  
should be placed as required.if we change the option as  
sufficient instead of required telnet can login as "root".  
-----------------------------------------------------------  
**How to send automated email to a set of people at fixed time ?**  
  
1)just create a alias of people and create a command file and  
create a crond entry  
2)configure sendmail & postfix to configure procmail..  
Or configure Q-mail / Squirrel mail & use contab  
----------------------------------------------------  
**how do i check which package has installed some command**  
**suppose ls , mkdir or whatever ???**  
  
rpm -qa | grep "pakage name"  
  
rpm -qa | grep   
yum install it will show already installed  
or not if not then it will install  
Pirut same as yum  
rpm -qa /usr/bin/ls  
gives you from which rpm the "ls" command is installed.  
  
-----------------------------------------------------  
  
**What is the difference between Telnet and SSH?**  
  
ssh is a secured shell, where telnet is not a secured  
one.when you ssh to trasnfer data between a system, the data  
will be send in the encrypted form, where the hacker cannot  
encode or decode it. While you telnet,the data send between  
the system is alphabetical format(ASCII), where every one  
can understand. More over as per network security, telnet  
and ftp are prohibited. Always, trust SSL based data transfer.  
  
Telnet ->  
Its just getting (Telenet) a connection to the server.  
Its not more secure. Anybody can use it.  
It can be easly hacked.It can be easily read by anybody in  
that network  
  
SSH -> secured shocket shell  
Its more secure than Telnet .  
This has an encrption and decrption of the data /usr/pwd  
None can hack this. It is the good way to transfer the data  
  
---------------------------------------------------  
**What is the difference between home directory and working directory?**  
  
home directory is one over which user have complete control  
and it is its default working directory when its logs in.  
while the working directory is the users current directory  
which may or may not be his home directory.  
------------------------------------------  
How can you see all mounted drives?  
  
with df -hT command and  
with the mount command.  
#vi /etc/fstab contains perminant mounts  
---------------------------------------------  
  
**When you install RedHat what is the kernel mode ? What is kernel compilation / upgrade ?**  
  
Kernel mode, also referred to as system mode, is one of the  
two distinct modes of operation of the CPU in Linux. The  
other is user mode, a non-privileged mode for user programs,  
that is, for everything other than the kernel.  
When the CPU is in kernel mode, it is assumed to be  
executing trusted software, and thus it can execute any  
instructions and reference any memory addresses. The kernel  
is trusted software, but all other programs are considered  
untrusted software. Thus, all user mode software must  
request use of the kernel by means of a system call in order  
to perform privileged instructions, such as process creation  
or input/output.  
  
Kernel compilation is installing a new kernel or adding  
custom modules to the same kernel.  
Kernel upgradation is upgrading it to a different version  
altogether.  
------------------------------  
**what is the difference between fork and thread ? and parent and child process in fork system call?**  
fork() system call in UNIX causes creation of a new process  
the new process (child process) which is an exact copy of  
the calling process(parent process).return value from fork  
() is used to distinguish the parent from the child; the  
parent receives the child's process id, but the child  
receives zero.  
  
A thread is a stream of instructions that can be scheduled  
as an independent unit.  
  
A thread is a stream of instructions that can be scheduled  
as an independent unit. It is important to understand the  
difference between a thread and a process. A process  
contains two kinds of information: resources that are  
available to the entire process such as program  
instructions, global data and working directory, and  
schedulable entities, which include program counters and  
stacks. A thread is an entity within a process that  
consists of the schedulable part of the process.  
  
A fork() duplicates all the threads of a process. The  
problem with this is that fork() in a process where threads  
work with external resources may corrupt those resources  
(e.g., writing duplicate records to a file) because neither  
thread may know that the fork() has occurred.  
  
When a new perl thread is created, all the data associated  
with the current thread is copied to the new thread, and is  
subsequently private to that new thread! This is similar in  
feel to what happens when a UNIX process forks, except that  
in this case, the data is just copied to a different part  
of memory within the same process rather than a real fork  
taking place.  
  
A fork() induces a parent-child relationship between two  
processes. Thread creation induces a peer relationship  
between all the threads of a process.  
--------------------------------------------------------  
**You want to create a compressed backup of the users' home directories. What utility should you use?**  
  
Tar -czf kk.tar.gz /home/username  
If we want to extract  
the the command is tar -xzf kk.tar.gz  
--------------------------------------------------------  
**What is the difference between an argument and an option/switch?**  
  
A linux/unix syntax format is as follows  
  
command option arguement  
  
example: ls -a /boot  
here ls command, -a is option,/boot is arguement  
  
option specifies the command how to run  
arguement specifies the command on what to run  
---------------------------------------------------------  
**How does the boot process[init levels] work on Linux? How is it different from Solaris?**  
  
When an x86 computer is booted, the processor looks at the  
end of the system memory for the BIOS (Basic Input/Output  
System) and runs it. The BIOS program is written into  
permanent read-only memory and is always available for use.  
The BIOS provides the lowest level interface to peripheral  
devices and controls the first step of the boot process.  
  
The BIOS tests the system, looks for and checks peripherals,  
and then looks for a drive to use to boot the system.  
Usually it checks the floppy drive (or CD-ROM drive on many  
newer systems) for bootable media, if present, and then it  
looks to the hard drive. The order of the drives used for  
booting is usually controlled by a particular BIOS setting  
on the system. Once Linux is installed on the hard drive of  
a system, the BIOS looks for a Master Boot Record (MBR)  
starting at the first sector on the first hard drive, loads  
its contents into memory, then passes control to it.  
  
This MBR contains instructions on how to load the GRUB (or  
LILO) boot-loader, using a pre-selected operating system.  
The MBR then loads the boot-loader, which takes over the  
process (if the boot-loader is installed in the MBR). In the  
default Red Hat Linux configuration, GRUB uses the settings  
in the MBR to display boot options in a menu. Once GRUB has  
received the correct instructions for the operating system  
to start, either from its command line or configuration  
file, it finds the necessary boot file and hands off control  
of the machine to that operating system.  
  
1. The system BIOS checks the system and launches the first  
stage boot loader on the MBR of the primary hard disk.  
  
2. The Frist stage boot loader loads itself into memory and  
launches the second stage boot loader from the /boot/  
partition.  
  
3. The second stage boot loader loads the kernel into  
memory, which in turn loads any necessary modules and  
mounts the root  
partition read-only.  
  
4. The kernel transfers control of the boot process to the /  
sbin/init program.  
  
5. The /sbin/init program loads all services and user-space  
tools, and mounts all partitions  
listed in /etc/fstab.  
  
6. The user is presented with a login screen for the  
freshly booted Linux system.  
-------------------------------------------------------------  
**What are the main differences between RHEL4 & RHEL5?**   
  
XEN, YUM and improved SELinux  
all the features updated with better options  
Better GUI support then RHEL4  
YUM over RPM package management  
IPTables and SELinux for more secure environment  
ext2 & ext3 file system  
In RHEL 4 SELinux Block only 13 services, But on RHEL 5  
SElinux Block 80 services  
-------------------------------------------------------  
**What text filter can you use to display a binary file in octal numbers?**  
  
hexdump file1 > file2  
--------------------------------------------------------  
**tell me some of the Linux HotKeys do you know?**  
  
alt+f1 for application menu  
ctl+l to clear screen  
alt+f2 to open run application window  
alt+f3 for find  
alt+f4 to close application  
alt+f9 to minimise window  
Ctrl-Alt-D Show desktop  
Crtl-Alt-Backspace Restart XWindows  
-------------------------------------------------  
  
**What file should you examine to determine the defined runlevels for your system?**  
  
/etc/inittab  
  
id:X:initdefault  
  
where X=runlevel (ex.0 to 6)  
0 =system poweroff  
1 = single user mode  
2 = multiuser mode without network and X window  
3 = multiuser mode with network without X window  
4 = unused  
5 = X11 (multiuser mode with network and X window  
6 = reboot  
--------------------------------------  
**What is the name and path of the main system log?**  
  
/var/log/messages system log messages can be seen here  
/var/log/dmesg Kernel boot log messages can view  
  
There are Three centralized loggin demons  
1)syslogd  
2)klogd  
3)auditd  
  
klogd:- collect log file created by the Kernel  
syslogd:- Collect log file created by the system  
auditd:- Collect log file created by the SELinux  
  
After collecting the log system store logs on different location  
/var/log/dmesg:- Created at boot time, by kernel  
/var/log/messages:- standard system error message,  
/var/log/secure:- authentication related log  
/var/log/maillog:- Mail related log  
/var/log/audit/audit.log:-Selinux related log  
  
We can redirect the log by configuring  
/etc/sysconfig/syslog  
/etc/syslog.conf  
  
-------------------------------------------------  
**what is the difference between semaphore, mutex & spinlock?**  
  
Kernel Locking Techniques  
Semaphores in Linux are sleeping locks. Because they cause a  
task to sleep on contention, instead of spin, they are used  
in situations where the lock-held time may be long.  
Conversely, since they have the overhead of putting a task  
to sleep and subsequently waking it up, they should not be  
used where the lock-held time is short. Since they sleep,  
however, they can be used to synchronize user contexts  
whereas spinlocks cannot. In other words, it is safe to  
block while holding a semaphore.  
  
A "mutex" (or "mutual exclusion lock") is a signal that two  
or more asynchronous processes can use to reserve a shared  
resource for exclusive use. The first process that obtains  
ownership of the "mutex" also obtains ownership of the  
shared resource. Other processes must wait for for the first  
process to release it's ownership of the "mutex" before they  
may attempt to obtain it.  
  
The most common locking primitive in the kernel is the  
spinlock. The spinlock is a very simple single-holder lock.  
If a process attempts to acquire a spinlock and it is  
unavailable, the process will keep trying (spinning) until  
it can acquire the lock. This simplicity creates a small and  
fast lock.  
---------------------------------------------------  
**What are seven fields in the /etc/passwd file.**   
  
1. Username: It is used when user logs in. It should be between 1 and 32 characters in length.  
2. Password: An x character indicates that encrypted password is stored in /etc/shadow file.  
3. User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.  
4. Group ID (GID): The primary group ID (stored in /etc/group file)  
5. User ID Info: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.  
6. Home directory: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /  
7. Command/shell: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell.  
  
------------------------------------------------------  
  
1. **Q. How do you list files in a directory?**  
A. ls - list directory contents  
ls -l (-l use a long listing format)  
  
2. **Q. How do you list all files in a directory, including the hidden files?**  
A. ls -a (-a, do not hide entries starting with .)  
  
3. **Q. How do you find out all processes that are currently running?**  
A. ps -f (-f does full-format listing.)  
  
4. **Q. How do you find out the processes that are currently running or a particular user?**  
A. ps -au Myname (-u by effective user ID (supports names)) (a - all users)  
  
5. **Q. How do you kill a process?**  
A. kill -9 8 (process\_id 8) or kill -9 %7 (job number 7)  
kill -9 -1 (Kill all processes you can kill.)  
killall - kill processes by name most (useful - killall java)  
  
  
6. Q. **What would you use to view contents of the file?**  
A. less filename  
cat filename  
pg filename  
pr filename  
more filename  
most useful is command: tail file\_name - you can see the end of the log file.  
  
7. Q. **What would you use to edit contents of the file?**  
A. vi screen editor or jedit, nedit or ex line editor  
  
8. Q. **What would you use to view contents of a large error log file?**  
A. tail -10 file\_name ( last 10 rows)  
  
9. Q. H**ow do you log in to a remote Unix box?**  
A. Using telnet server\_name or ssh -l ( ssh - OpenSSH SSH client (remote login program))  
  
10.Q. **How do you get help on a UNIX terminal?**  
A. man command\_name  
info command\_name (more information)  
  
11.Q. **How do you list contents of a directory including all of its**  
**subdirectories, providing full details and sorted by modification time?**  
A. ls -lac  
-a all entries  
-c by time  
  
12.Q. **How do you create a symbolic link to a file (give some reasons of doing so)?**  
A. ln /../file1 Link\_name  
Links create pointers to the actual files, without duplicating the contents of  
the files. That is, a link is a way of providing another name to the same file.  
There are two types of links to a file:Hard link, Symbolic (or soft) link;  
  
13.Q. **What is a filesystem?**  
A. Sum of all directories called file system.  
A file system is the primary means of file storage in UNIX.  
File systems are made of inodes and superblocks.  
  
14.Q. **How do you get its usage (a filesystem)?**  
A. By storing and manipulate files.  
  
15**.Q. How do you check the sizes of all users home directories (one command)?**  
A. du -s  
df  
  
The du command summarizes disk usage by directory. It recurses through all subdirectories and shows disk usage by each subdirectory with a final total at the end.

**What "neat" command will do?**  
  
neat command provides Graphical interface to change network settings for network devices.  
  
  
  
**Q: - Which protocol is required to allow local printing and print sharing?**  
  
Internet Printing Protocol (IPP) is required to allow local printing and print sharing.  
  
  
**Q: - What is CUPS?**  
  
CUPS stands for "Common UNIX Printing System". CUPS is a open source printing system developed by Apple Inc. CUPS uses the Internet Printing Protocol (IPP) to allow local printing and print sharing.  
  
  
**Q: -What is the location of log files for CUPS?**  
  
The log files for the CUPS printing system are located in the /var/log/cups/ directory.  
  
  
**Q: - What is YUM?**  
  
YUM stands for Yellow dog Updater, Modified because it is based on YUP, the Yellow dog Updater. Where does the name Yellow dog come from? Yellow Dog is a version of Linux for the Power Architecture hardware and is RPM-based, just like Red Hat Enterprise Linux and Fedora. YUP, and later YUM, were written by the Linux community as a way to maintain an RPM-based system.  
  
  
**Q: - What are the advantages of YUM?**  
  
- Automatic resolution of software dependencies.  
- Multiple software locations at one time.  
- Ability to specify particular software versions or architectures.  
  
  
**Q: - How you will install software by YUM?**  
  
yum install <pkgname>

**Q: - Which option is required to assume the answer "yes" to any questions asked during installation of package dependencies for YUM?**  
  
The "-y" option is used to assume the answer "yes".

For Example

yum -y install squid

**Q: - How to remove a software by YUM?**  
  
yum remove <pkgname>

**Q: - How Many Run Levels present in Linux?**  
  
There are 7 run levels, with each having its own properties.

- 0: Halt the system  
- 1: Single-user mode  
- 2: Not used  
- 3: Multi-user mode with text login  
- 4: Not used  
- 5: Multi-user mode with graphical login  
- 6: Reboot

**Q: - Which configuration file is required to change the Run Level of Server or system?**  
  
/etc/inittab

To change the default run level, modify this line.

id:5:initdefault:

**Q: - Explain architectures required for RPMs?**  
  
noarch Architecture-independent, can run on any architecture

i386 Generic build for a 32-bit x86 system

i586 Sometimes used when building kernels for older x86 processors  
Intel® Pentium ® II, Intel Pentium III, Intel Pentium 4, AMD Athlon, and

i686 AMD Duron systems (Most RPMs for these architectures are built using the i386 architecture, with the kernel for these architectures being built with the  
i686 for optimal performance.)

x86\_64 64-bit processors such as AMD Athlon64, AMD Opteron, and Intel EM64T

ia64 Intel® Itanium

ppc 32-bit IBM® POWER, IBM eServer„ pSeries®, and IBM eServer iSeries

s390x 64-bit IBM eServer System z

**Q: - How to install Linux software’s by RPM?**  
  
rpm -ivh test-1.0-1.i386.rpm

test ######################### [100%]

**Q: - If a file associated with test-1.0-1.i386.rpm deleted, than How we will recover that file?**  
  
We can reinstall this rpm again.

**Q: - If you are getting error "package is already installed" but you have to install package any how. what option you will use?**  
  
rpm -ivh test-1.0-1.i386.rpm

Preparing... ########################################### [100%] package test-1.0-1 is already installed

In this case you can use "--replacepkgs" option.

rpm -ivh –replacepkgs test-1.0-1.i386.rpm

**1. How do u force a user to change password on next login in linux?**

A. chage -d 0 "User"

**2.What command can be used to findout server architechure (x86 or x64) apart from**

**uname?**

A. arch

**3. How do u findout the users who are NOT logged in for more than 30 days? which file u**

**will check?**

A. last , lastlog, /var/log/wtmp

**4. whats is called 1.5 stage in boot process of linux?**

A. Which contains extra code to allow cylinders above 1024, or LBA type drives, to be read. The

1.5 boot loader is stored (if needed) in the MBR or the boot partition.The great thing about

GRUB is that it includes knowledge of Linux file systems. Instead of using raw sectors on the

disk, as LILO does, GRUB can load a Linux kernel from an ext2 or ext3 file system. It does this

by making the two-stage boot loader into a three-stage boot loader. Stage 1 (MBR) boots a

stage 1.5 boot loader that understands the particular file system containing the Linux kernel

image. Examples include reiserfs\_stage1\_5 (to load from a Reiser journaling file system) or

e2fs\_stage1\_5 (to load from an ext2 or ext3 file system). When the stage 1.5 boot loader is

loaded and running, the stage 2 boot loader can be loaded."

So Basically,

Stage 1 Boot loader is MBR

Stage 2 Boot loader is GRUB

Stage 1.5 Boot loader is e2fs\_stage1\_5

(Basically this module will load the knowledge of Filesystem to Grub to read the kernel)

**5. When u try to create a file, u got a error that "No space available". But actually space**

**available on volume? How do u resolve this issue?**

A. Try this df -i list inode information instead of block usage [Perhaps are you out of inodes on

this file system.], To "rectify it", remove unwanted files or move them somewhere else.]

### Beginners UNIX Interview Questions Answers

**1. Write command to list all the links from a directory?**

In this UNIX command interview questions interviewer is generally checking whether user knows basic use of "ls" "grep" and regular expression etc

You can write command like:

ls -lrt | grep "^l"

**2. Create a read-only file in your home directory?**

This is a simple UNIX command interview questions where you need to create a file and change its parameter to read-only by using chmod command you can also change your umask to create read only file.

touch file

chmod 400 file

read more about [**file and directory permission in unix and linux**](http://javarevisited.blogspot.com/2011/11/file-permissions-in-unix-linux-example.html) here.

**3. How will you find which operating system your system is running on in UNIX?**

By using command **"uname -a"** in UNIX

**4. How will you run a process in background? How will you bring that into foreground and how will you kill that process?**

For running a process in background use "&" in command line. For bringing it back in foreground use command "**fg jobid"** and for getting job id you use command "jobs", for killing that process find PID and use kill -9 PID command. This is indeed a good Unix Command interview questions because many of programmer not familiar with background process in UNIX.

**5. How do you know if a remote host is alive or not?**

You can check these by using either **ping** or **telnet** command in UNIX. This question is most asked in various Unix command Interview because its most basic networking test anybody wants to do it.

**6. How do you see command line history in UNIX?**

Very useful indeed, use history command along with[**grep command in unix**](http://javarevisited.blogspot.com/2011/06/10-examples-of-grep-command-in-unix-and.html)to find any relevant command you have already executed. Purpose of this Unix Command Interview Questions is probably to check how familiar candidate is from available tools in UNIX operation system.

**7. How do you copy file from one host to other?**

Many options but you can say by using "**scp**" command. You can also use **rsync** command to answer this UNIX interview question or even **sftp** would be ok.

**8. How do you find which process is taking how much CPU?**

By using "top" command in UNIX, there could be multiple follow-up UNIX command interview questions based upon response of this because “TOP” command has various interactive options to [sort](http://javarevisited.blogspot.com/2011/08/unix-sort-command-example-tutorial.html) result based upon various parameter.

**9. How do you check how much space left in current drive ?**

By using **"df"** command in UNIX. For example **"df -h ."** will list how full your current drive is. This is part of anyone day to day activity so I think this Unix Interview question will be to check anyone who claims to working in UNIX but not really working on it.

**10. What is the difference between Swapping and Paging?**

Swapping:

Whole process is moved from the swap device to the main memory for execution. Process size must be less than or equal to the available main memory. It is easier to implementation and overhead to the system. Swapping systems does not handle the memory more flexibly as compared to the paging systems.

Paging:

Only the required memory pages are moved to main memory from the swap device for execution. Process size does not matter. Gives the concept of the virtual memory. It provides greater flexibility in mapping the virtual address space into the physical memory of the machine. Allows more number of processes to fit in the main memory simultaneously. Allows the greater process size than the available physical memory. Demand paging systems handle the memory more flexibly.

### Intermediate UNIX Interview Questions Answers

**1. What is difference between ps -ef and ps -auxwww?**

[](http://javarevisited.blogspot.com/2011/03/10-find-command-in-unix-examples-basic.html)This is indeed a good Unix Interview Command Question and I have faced this issue while ago where one culprit process was not visible by execute **ps –ef** command and we are wondering which process is holding the file.

ps -ef will omit process with very long command line while ps -auxwww will list those process as well.

**2. How do you find how many cpu are in your system and there details?**

By looking into file /etc/cpuinfo for example you can use below command:

**cat /proc/cpuinfo**

**3. What is difference between HardLink and SoftLink in UNIX?**

I have discussed this Unix Command Interview questions in my blog post [difference between Soft link and Hard link in Unix](http://javarevisited.blogspot.com/2011/04/symbolic-link-or-symlink-in-unix-linux.html)

**4. What is Zombie process in UNIX? How do you find Zombie process in UNIX?**

When a program forks and the child finishes before the parent, the kernel still keeps some of its information about the child in case the parent might need it - for example, the parent may need to check the child's exit status. To be able to get this information, the parent calls 'wait()'; In the interval between the child terminating and the parent calling 'wait()', the child is said to be a 'zombie' (If you do 'ps', the child will have a 'Z' in its status field to indicate this.)

**Zombie : The process is dead but have not been removed from the process table.**

**5. What is "chmod" command? What do you understand by this line “r-- -w- --x?**

**6. There is a file some where in your system which contains word "UnixCommandInterviewQuestions” How will find that file in Unix?**

By using find command in UNIX for details see here [10 example of using find command in Unix](http://javarevisited.blogspot.com/2011/03/10-find-command-in-unix-examples-basic.html)

**7. In a file word UNIX is appearing many times? How will you count number?**

grep -c "Unix" filename

**8. How do you set environment variable which will be accessible form sub shell?**

By using **export** for example export count=1 will be available on all sub shell.

**9. How do you check if a particular process is listening on a particular port on remote host?**

By using telnet command for example “telnet hostname port”, if it able to successfully connect then some process is listening on that port. To read more about telnet read [networking command in UNIX](http://javarevisited.blogspot.com/2010/10/basic-networking-commands-in-linuxunix.html)

**10. How do you find whether your system is 32 bit or 64 bit ?**

Either by using **"uname -a"** command or by using "**arch**" command.

### Advanced UNIX Interview Questions and Answers

**1. How do you find which processes are using a particular file?**

By using **lsof** **command** in UNIX. It wills list down PID of all the process which is using a particular file.

**2. How do you find which remote hosts are connecting to your host on a particular port say 10123?**

By using **netstat command** execute netstat -a | grep "port" and it will list the entire host which is connected to this host on port 10123.

**3. What is nohup in UNIX?**

**4. What is ephemeral port in UNIX?**

Ephemeral ports are port used by Operating system for client sockets. There is a specific range on which OS can open any port specified by ephemeral port range.

**5. If one process is inserting data into your MySQL database? How will you check how many rows inserted into every second?**

Purpose of this Unix Command Interview is asking about **"watch" command** in UNIX which is repeatedly execute command provided with specified delay.

**6. There is a file Unix\_Test.txt which contains words Unix, how will you replace all Unix to UNIX?**

You can answer this Unix Command Interview question by using SED command in UNIX for example you can execute **sed s/Unix/UNIX/g fileName.**

**7. You have a tab separated file which contains Name, Address and Phone Number, list down all Phone Number without there name and Addresses?**

To answer this Unix Command Interview question you can either you AWK or CUT command here. CUT use tab as default separator so you can use

**cut -f3 filename.**

**8. Your application home directory is full? How will you find which directory is taking how much space?**

By using disk usage (DU) command in Unix for example du **–sh . | grep G** will list down all the directory which has GIGS in Size.

**9. How do you find for how many days your Server is up?**

By using **uptime** command in UNIX

**10. You have an IP address in your network how will you find hostname and vice versa?**

This is a standard UNIX command interview question asked by everybody and I guess everybody knows its answer as well. By using **nslookup** command in UNIX, you can read more about [**Convert IP Address to hostname in Unix**](http://javarevisited.blogspot.com/2011/09/find-hostname-from-ip-address-to.html) here.

Q) What is NFS? Q) What is its purpose?

Answer - NFS is Network File system. It is a file system used for sharing of files over a network.......

How do I send email with linux?

Answer - Email can be sent in Linux using the mail command. ......

Q) Explain RPM (Red Hat Package Manager) features.

Answer - RPM is a package managing system (collection of tools to manage software packages).......

Q) What is Kernel? Q) Explain the task it performs.

Answer - Kernel is used in UNIX like systems and is considered to be the heart of the operating system.......

Q) What is Linux Shell? Q) What is Shell Script?

Answer - Linux shell is a user interface used for executing the commands. Shell is a program the user......

Q) What are Pipes? Q) Explain use of pipes.

Answer - A pipe is a chain of processes so that output of one process (stdout) is fed an input (stdin) to another.......

Q) Explain trap command; shift Command, getopts command of linux.

Answer - Trap command: controls the action to be taken by the shell when a signal is received. ......

Q) What Stateless Linux server? Q) What feature it offers?

Answer - A stateless Linux server is a centralized server in which no state exists on the single workstations. ......

Q) What does nslookup do? Q) Explain its two modes.

Answer - Nslookup is used to find details related to a Domain name server. Details like IP addresses of a machine, MX records,......

Q) What is Bash Shell?

Answer - Bash is a free shell for UNIX. It is the default shell for most UNIX systems. It has a combination of the C and Korn shell features. ......

Q) Explain some Network-Monitoring Tools in Linux: ping, traceroute, tcpdump, ntop

Answer - Network monitoring tools are used to monitor the network, systems present on the network, traffic etc.......

How does the linux file system work?

Answer - Linux file structure is a tree like structure. It starts from the root directory, represented by '/', and then expands into sub-directories.......

Q) What are the process states in Linux?

Answer - Process states in Linux.......

Q) What is a zombie?

Answer - Zombie is a process state when the child dies before the parent process. In this case the structural information of the process is still in the process table.......

Q) Explain each system calls used for process management in linux.

Answer - System calls used for Process management......

Q) Which command is used to check the number of files and disk space used and the each user’s defined quota?

repquota command is used to check the status of the user’s quota along with the disk space and number of files used. This command gives a summary of the user’s quota that how much space and files are left for the user. Every user has a defined quota in Linux. This is done mainly for the security, as some users have only limited access to files. This provides a security to the files from unwanted access. The quota can be given to a single user or to a group of users.

Q) What is the name and path of the main system log?

By default the main system log is /var/log/messages. This file contains all the messages and the script written by the user. By default all scripts are saved in this file. This is the standard system log file, which contains messages from all system software, non-kernel boot issues, and messages that go to 'dmesg'. dmesg is a system file that is written upon system boot.

Q) How secured is Linux? Q) Explain.

Security is the most important aspect of an operating system. Due to its unique authentication module, Linux is considered as more secured than other operating systems. Linux consists of PAM. PAM is Pluggable Authentication Modules. It provides a layer between applications and actual authentication mechanism. It is a library of loadable modules which are called by the application for authentication. It also allows the administrator to control when a user can log in. All PAM applications are configured in the directory "/etc/pam.d" or in a file "/etc/pam.conf". PAM is controlled using the configuration file or the configuration directory.

Q) Can Linux computer be made a router so that several machines may share a single Internet connection? How?

Yes a Linux machine can be made a router. This is called "IP Masquerade." IP Masquerade is a networking function in Linux similar to the one-to-many (1: Many) NAT (Network Address Translation) servers found in many commercial firewalls and network routers. The IP Masquerade feature allows other "internal" computers connected to this Linux box (via PPP, Ethernet, etc.) to also reach the Internet as well. Linux IP Masquerading allows this functionality even if the internal computers do not have IP addresses.

The IP masquerading can be done by the following steps:

1. The Linux PC must have an internet connection and a connection to LAN. Typically, the Linux PC has two network interfaces-an Ethernet card for the LAN and a dial-up PPP connection to the Internet (through an ISP).

2. All other systems on your LAN use the Linux PC as the default gateway for TCP/IP networking. Use the same ISP-provided DNS addresses on all systems.

3. Enable IP forwarding in the kernel. By default the IP forwarding is not enabled. To ensure that IP forwarding is enabled when you reboot your system, place this command in the /etc/rc.d/rc.local file.

4. Run /sbin/iptables-the IP packet filter administration program-to set up the rules that enable the Linux PC to masquerade for your LAN.

Q) What is the minimum number of partitions you need to install Linux?

Minimum 2 partitions are needed for installing Linux. The one is / or root which contains all the files and the other is swap. Linux file system is function specific which means that files and folders are organized according to their functionality. For example, all executables are in one folder, all devices in another, all libraries in another and so on. / or ‘root’ is the base of this file system. All the other folders are under this one. / can be consider as C: .Swap is a partition that will be used as virtual memory. If there is no more available RAM a Linux computer will use an area of the hard disk, called swap, to temporarily store data. In other words it is a way of expanding your computers RAM.

Which command is used to review boot messages?

dmesg command is used to review boot messages. This command will display system messages contained in the kernel ring buffer. We can use this command immediately after booting to see boot messages. A ring buffer is a buffer of fixed size for which any new data added to it overwrites the oldest data in it. Its basic syntax is

dmesg [options]

Invoking dmesg without any of its options causes it to write all the kernel messages to standard output. This usually produces far too many lines to fit into the display screen all at once, and thus only the final messages are visible. However, the output can be redirected to the less command through the use of a pipe, thereby allowing the startup messages to be viewed on one screen at a time

dmesg | less

Which utility is used to make automate rotation of a log?

logrotate command is used to make automate rotation of log.

Syntax of the command is:

logrotate [-dv] [-f|] [-s|] config\_file+

It allows automatic rotation, compression, removal, and mailing of log files. This command is mainly used for rotating and compressing log files. This job is done every day when a log file becomes too large. This command can also be run by giving on command line. We can done force rotation by giving –f option with this command in command line. This command is also used for mailing. We can give –m option for mailing with this command. This option takes two arguments one is subject and other is recipient name.

Q) What are the partitions created on the mail server hard drive?

The main partitions are done firstly which are root, swap and boot partition. But for the mail server three different partitions are also done which are as follows:

1. /var/spool- This is done so that if something goes wrong with the mail server or spool than the output cannot overrun the file system.

2. /tmp- putting this on its own partition prevents any user item or software from overrunning the system files.

3. /home- putting this on its own is useful for system upgrades or reinstalls. It allow not to wipe off the /home hierarchy along with other areas.

Q) What are the fields in the/etc/passwd file?

It contains all the information of the users who log into the system. It contains a list of the system's accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc. It should have general read permission as many utilities, like ls use it to map user IDs to user names, but write access only for the superuser (root). The main fields of /etc/passwd file are:

1. Username: It is used when user logs in. It should be between 1 and 32 characters in length.

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

3. User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.

4. Group ID (GID): The primary group ID (stored in /etc/group file)

5. User ID Info: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.

6. Home directory: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /

7. Command/shell: The absolute path of a command or shell (/bin/bash). Typically, this is a shell.

Which commands are used to set a processor-intensive job to use less CPU time?

nice command is used for changing priority of the jobs.

Syntax: nice [OPTION] [COMMAND [ARG]...]

Range of priority goes from -20 (highest priority) to 19 (lowest).Priority is given to a job so that the most important job is executed first by the kernel and then the other least important jobs. This takes less CPU times as the jobs are scheduled and are given priorities so the CPU executes fast. The priority is given by numbers like -20 describe the highest priority and 19 describe the least priority.

How to change window manager by editing your home directory?

/.xinitrc file allows changing the window manager we want to use when logging into X from that account. The dot in the file name shows you that the file is a hidden file and doesn't show when you do a normal directory listing. For setting a window manager we have to save a command in this file. The syntax of command is: exec windowmanager.After this, save the file. Next time when you run a startx a new window manager will open and become default. The commands for starting some popular window managers and desktop environments are:

-KDE = startkde

-Gnome = gnome-session

-Blackbox = blackbox

-FVWM = fvwm

-Window Maker = wmaker

-IceWM = icewm

Q) How documentation of an application is stored?

When a new application is installed its documentation is also installed. This documentation is stored under the directory named for application. For example if my application name is App1 then the path of the documentation will be /user/doc/App1. It contains all the information about the application. It contains date of creating application, name of application and other important module of the application. We can get the basic information of application from the documentation.

Q) How shadow passwords are given?

pwconv command is used for giving shadow passwords. Shadow passwords are given for better system security. The pwconv command creates the file /etc/shadow and changes all passwords to ‘x’ in the /etc/passwd file. First, entries in the shadowed file which don't exist in the main file are removed. Then, shadowed entries which don't have `x' as the password in the main file are updated. Any missing shadowed entries are added. Finally, passwords in the main file are replaced with `x'. These programs can be used for initial conversion as well to update the shadowed file if the main file is edited by hand.

Q) How do you create a new user account?

useradd command is used for creating a new user account. When invoked without the

-D option, the useradd command creates a new user account using the values specified on the command line and the default values from the system. The new user account will be entered into the system files as needed, and initial files copied, depending on the command line options. This command uses the system default as home directory. If –m option is given then the home directory is made.

Q) Which password package is installed for the security of central password?

Shadow password packages are used for security of central passwords. Security is the most important aspect of every operating system. When this package is not installed the user information including passwords is stored in the /etc/passwd file. The password is stored in an encoded format. These encoded forms can be easily identified by the System crackers by randomly encoding the passwords from dictionaries. The Shadow Package solves the problem by relocating the passwords to another file (usually /etc/shadow). The /etc/shadow file is set so that it cannot be read by just anyone. Only root will be able to read and write to the /etc/shadow file.

Q) Which shell do you assign to a POP3 mail-only account?

POP3 mail only account is assigned to the /bin/false shell. However, assigning bash shell to a POP3 mail only gives user login access, which is avoided. /bin/nologin can also be used. This shell is provided to the user when we don’t want to give shell access to the user. The user cannot access the shell and it reject shell login on the server like on telnet. It is mainly for the security of the shells. POP3 is basically used for downloading mail to mail program. So for illegal downloading of emails on the shell this account is assigned to the /bin/false shell or /bin/nologin. These both shells are same they both do the same work of rejecting the user login to the shell. The main difference between these two shells is that false shell shows the incorrect code and any unusual coding when user login with it. But the nologin shell simply tells that no such account is available. So nologin shell is used mostly in Linux.

Q) Which daemon is responsible for tracking events on Linux system?

syslogd is responsible for tracking system information and save it to the desired log files. It provides two system utilities which provide system logging and kernel message trapping. Internet and UNIX domain sockets support enable this utility package to support both local and remote logging. Every logged message contains at least a time and a hostname field, normally a program name field, too. So to track these information this daemon is used. syslogd mainly reacts to the set of signals given by the user. These are the signals given to syslogd: SIGHUP: This lets syslogd perform a re-initialization. All open files are closed, the configuration file (default is /etc/syslog.conf) will be reread and the syslog facility is started again. SIGTERM: The syslogd will die. SIGINT, SIGQUIT: If debugging is enabled these are ignored, otherwise syslogd will die. SIGUSR1: Switch debugging on/off. This option can only be used if syslogd is started with the - d debug option. SIGCHLD: Wait for Childs if some were born, because of waiting messages.

Q) Which daemon is used for scheduling of the commands?

The crontab command is used for scheduling of the commands to run at a later time. SYNTAX

crontab [ -u user ] file

crontab [ -u user ] { -l | -r | -e }

Options

-l List - display the current crontab entries.

-r Remove the current crontab.

-e Edit the current crontab using the editor specified by the VISUAL or EDITOR environment variables.

When user exits from the editor, the modified crontab will be installed automatically. Each user can have their own crontab, and though these are files in /var, they are not intended to be edited directly. If the –u option is given than the crontab gives the name of the user whose crontab is to be tweaked. If it is given without this then it will display the crontab of the user who is executing the command.

Q) How environment variable is set so that the file permission can be automatically set to the newly created files?

umask command is used to set file permission on newly created files automatically.

Syntax

umask [-p] [-S] [mode]

It is represented in octal numbers. We can simply use this command without arguments to see the current file permissions. To change the permissions, mode is given in the arguments. The default umask used for normal user is 0002. The default umask for the root user is 0022. For calculating the original values, the values shown by the umask must be subtracted by the default values. It is mainly used for masking of the file and directory permission. The /etc/profile script is where the umask command is usually set for all users. The –S option can be used to see the current default permissions displayed in the alpha symbolic format.

For example, umask 022 ensures that new files will have at most 755 permissions (777 NAND 022).

The permissions can be calculated by taking the NAND of original value with the default values of files and directories.

**Update V1.1.**

**1.When do you need a virtual hosting ?**

The term Virtual Host refers to the practice of maintaining more than one server on one machine, as differentiated by their apparent hostname. For example, it is often desirable for companies sharing a web server to have their own domains, with web servers accessible as www.company1.com and www.company2.com, without requiring the user to know any extra path information.

**2.In which port telnet is listening?**

23

**3.How to get the listening ports which is greater than 6000 using netstat ?**

**4.How to block and openrelay ?**

Open relays are e-mail servers that are configured to accept and transfer e-mail on behalf of any user anywhere, including unrelated third parties.

The qmail-smtpd daemon will consult the rcpthosts control file to determine valid destination addresses, and reject anything else.

**5.Q) What is sandwitch configuration in qmail ?**

Qmail + Clam + Spamassassin- This is normally called Sandwitch configuration in qmail.

**6.Advantages of Qmail ?**

More secure, better designed, modular, faster, more reliable, easier to configure, don't have to upgrade it every few months or worry about being vulnerable to something due to some obscure feature being enabled

qmail supports host and user masquerading, full host hiding, virtual domains, null clients, list-owner rewriting, relay control, double-bounce recording, arbitrary RFC 822 address lists, cross-host mailing list loop detection, per-recipient checkpointing, downed host backoffs, independent message retry schedules, etc. qmail also includes a drop-in ``sendmail'' wrapper so that it will be used transparently by your current UAs.

**7.Q) What is the difference between POP3 and IMAP ?**

The Difference

POP3 works by reviewing the inbox on the mail server, and downloading the new messages to your computer. IMAP downloads the headers of the new messages on the server, then retrieves the message you want to read when you click on it.

When using POP3, your mail is stored on your PC. When using IMAP, the mail is stored on the mail server. Unless you copy a message to a "Local Folder" the messages are never copied to your PC.

Scenarios of Use

POP3

· You only check e-mail from one computer.

· You want to remove your e-mail from the mail server.

IMAP

· You check e-mail from multiple locations.

· You use Webmail.

**8.How to drop packets using iptables ?**

Iptables -A INPUT -s xx.xx.xx.xx -d xx.xx.xx.xx -j DROP

**9.Daily routines of Linux Administrators ?**

\*.Check the health of servers

\*.Check for updates

\*.Check the Backup

\*.Check with the trouble ticketing system for any unread ticket.

\*.Troubleshoot if there any problem

\*.Installation of new servers, if needed.

\*.Report to the Boss

**10.How to take the Dump of a MySQL Database ?**

Mysqldump databasename > dumpname

**11.How to know the CPU usage of each process ?**

Top, uptime

**12.How to bind another IP in a NIC ?**

Copy the contents eth0 to eth1, and change the ipaddress. Restart the network. .

**13.Transparently proxy all web-surfing through Squid box**

iptables -t nat -A PREROUTING -i eth1 -tcp --dport 80 -j DNAT --to

iptables -t nat -A PREROUTING -i eth1 -tcp --dport 80 -j DNAT --to

**14.Transparently redirect web connections from outside to the DMZ web server.**

iptables -t nat -A PREROUTING -i eth0 -d 192.168.1.1 -dport 80 -j DNAT –to

**15 Howto Activate the forwarding**

echo 1 >/proc/sys/net/ipv4/ip\_forward

**16.Kill spoofed packets**

for f in /proc/sys/net/ipv4/conf/\*/rp\_filter; do

echo 1 > $f

done.

$iptables -A LDROP --proto tcp -j LOG --log-level info \ --log-prefix “TCP Drop”

**1. What is ldd?**

List dynamic dependencies – print shared library dependencies

**Eg: – # vim new.c**

**# gcc new.c –o new**

**# ldd new**

**2. What is the command to uninstall processes in Linux?**

rpm –e sendmail  
-e – remove

**3. What is the command for finding the highest memory occupied file in Linux?**

du –ah / | sort –n –r | head –n 1

du – estimate file space usage  
-a – write counts for all files, not just directories  
-h – print sizes in human readable format (eg. 1K 234M 2G)

sort – sort lines of text files  
-n – compare according to string numerical value  
-r – reverse the result of comparisons

head – output the first part of files  
-n – number of lines

**4. What are the Linux boot files?**

1./boot/grub/grub.conf: contains boot disk parameters  
2./etc/fstab: contains File systems which need to mount at boot time  
3./etc/initab: Contains default run level  
4./etc/init.d/rc.d/rcN.d: This is a dir it contains

**5. Difference between swap partition and swap file?**

Swap partition is maintained as a separate partition. Same swap partition can be used for two OS within single machine.

Suppose if the system crashes, there is a chance to recover or it may not corrupt the partition.

Less fragmented.

Where as swap file takes very less space. We can increase the space very easily, compared to swap partition. Swap file system fragmented.

If the system crashes then there is a huge chance to lost the swap file system.

**6. A file which is not deleted by normal user and also root (using rm), for that type of file how we delete it?**

Using chattr command, we need to change the attributes and then we remove using rm command.

Eg: – chattr -iIu example  
rm -rf example

**7. Difference between nfs soft and hard mounting points?**

Hard mount option: – If the client fails to access the server, then the connection hangs and once the system is up then it will again access the server.

Soft: – If the client failed to connect the server, it immediately gives the error report and closes the connection.

**8. If we transfer 100 files by ftp to remote server, how to know the files are successfully transfer or some file are not transferred?**

ftp>mput 1 2 3 …. 100  
ftp> ls –l

**9. I know ssh, telnet, dns,apache all are worked on TCP/UDP but i want to know any one service which are working on UDP only?**

snmptrap 162/udp  
snmptrap – simple network management protocol trap  
snmptrapd is an SNMP application that receives and logs

**10. I want to built a fire wall using iptables. My condition is ” inbound to 192.168.0.2 with a port of 80 from 172.168.0.1 should accept”**

iptables –A INPUT –p tcp –dport 80 –s 172.168.0.1 –d 192.168.0.2 –j ACCEPT

**11. I want to see how many interfaces (Ethernet cards) are working using single command?**

ifconfig

**12. What is the status code 403,404 represented in apache server?**

403 represent forbidden error, means if a file misses some selinux security context.

404 represent that there is a cgi script missing or web pages missing.

**13. How to monitor ports in a linux machine, with single command?**

nmap localhost

**14. In my linux machine, i lost /etc/passwd file and /etc/shadow file, then how can i recover it?**

Normally in linux we must have backup by default for /etc/passwd and /etc/shadow files

/etc/passwd —> /etc/passwd-  
/etc/shadow —> /etc/shadow-

from there we can copy or restore. If both are not available. Then follow below steps:

1. reboot  
2. Single user mode [ single init=/bin/bash ]  
3. pwconv  
4. check /etc/passwd and /etc/shadow files are there  
5. sync  
6. init 3 or reboot with init 3

**15. what r the different command to check ram,process and hdd of linux machine**

To check ram in your system:  
#free

To check process  
#ps  
#top

To check hdd  
#fdisk  
#sfdisk -l

**16.If i run ls command it will show me the junk output what is problem and how to resolve it**

Set your terminal setting by stty and before that, export ls command to PATH variable

**17. WHAT IS THE MEANING OF AIX**

AIX (Advanced Interactive eXecutive) is an open operating system from IBM which is based on a version of UNIX. AIX/ESA was designed for IBM’s System/390 or large server hardware platform. AIX/6000 is an operating system that runs on IBM’s workstation platform, the RISC System/6000.

**18. Why ls -F dev/log file output indicate as = sign at end of the file name?**

Standard output

**19. What is nis server?**

NIS is a service that provides any user on a network with the same working environment irrespective of the system on that network, which has been used for login purpose.

For example if NIS server is set up in a single system and configured to hold user accounts and their passwords and access information. Then any user on that network can login to his/her account from any system (with nis client running) on that configured network. This gives a look and feel that the user is logged into his/her own system. But actually it’s the account on the NIS server that is mounted on the local sytem user login.

**20. What command can you use to review boot messages?**

Dmesg

**21. Who invented unix?**

Unix was created in 1969 by Ken Thompson and Dennis Ritchie at Bell Laboratories.

**22. Write a cron entry for the following scenario:- At 10:30 AM for every Sunday of every 1st month of a quarter.**

30 10 \* 1-12/3 7

**23. What is the difference between RHEL4 & RHEL5?**

RHEL4: No yum server, Selinux, secure, no cd key  
RHEL5: yum server, advanced selinux, more secure, virtualization

**24. What is the command to make a process to run in the foreground from background?**

When the process is running, press “control+Z”. Now at the command prompt, type “bg”

**25. What are the init levels in Linux?**

7 level

This is the continuation to the Linux Interview Questions And Answers Part-3

**22. You wish to restore the file memo.ben which was backed up in the tarfile MyBackup.tar. What command should you type?**   
**Ans:** tar –xvf –I memo.ben MyBackup.tar

**23. You need to view the contents of the tarfile called MyBackup.tar. What command would you use?**  
**Ans:** tar –tvf MyBackup.tar

**24. You have a file called phonenos that is almost 4,000 lines long. What text filter can you use to split it into four pieces each 1,000 lines long?**   
**Ans:** split –l 1000

**25. What command should you use to check the number of files and disk space used and each user’s defined quotas?**

**26. The top utility can be used to change the priority of a running process? Another utility that can also be used to change priority is \_\_\_\_\_\_\_\_\_\_\_?**  
**Ans:**  
top – interactive  
nice  
renice

**27. What command should you type to see all the files with an extension of ‘mem’ listed in reverse alphabetical order in the /home/ben/memos directory.**   
**Ans:** ls -lr | awk ‘{print $9}’  
-l – to list files sorted by name  
-r – reverse the order of sorting  
awk $9 – gives 9th column of the ls output which contains only file names.

**28. What command is used to remove the password assigned to a group?**  
**Ans:** lpasswd -g -P

29. What can you type at a command line to determine which shell you are using?  
**Ans:** echo $SHELL

**30. If you type the command cat dog & > cat what would you see on your display?**

**31. You have the /var directory on its own partition. You have run out of space. What should you do? Choose one:**  
a. Reconfigure your system to not write to the log files.  
b. Use fips to enlarge the partition.  
c. Delete all the log files.  
d. Delete the partition and recreate it with a larger size.

**Ans:** None of these  
The preferred solutions one of or combination of the following:  
Move the old large files(logs) in external device  
Remove the old large files(logs)  
Save the old files/log in compressed for

**LINUX SYSTEM ADMINISTRATION**  
  
  
**Q: - How are devices represented in UNIX?**  
All devices are represented by files called special files that are located in /dev directory.  
  
**Q: - What is 'inode'?**  
All UNIX files have its description stored in a structure called 'inode'. The inode contains info about the file-size, its location, time of last access, time of last modification, permission and so on. Directories are also represented as files and have an associated inode.   
  
**Q: - What are the process states in Unix?**  
As a process executes it changes state according to its circumstances. Unix processes have the following states:  
Running : The process is either running or it is ready to run .  
Waiting : The process is waiting for an event or for a resource.  
Stopped : The process has been stopped, usually by receiving a signal.  
Zombie : The process is dead but have not been removed from the process table.  
  
**Q: - What command should you use to check the number of files and disk space used and each user's defined quotas?**  
repquota   
  
**Q: - What command is used to remove the password assigned to a group?**  
gpasswd -r  
  
**Q: - What can you type at a command line to determine which shell you are using?**  
echo $SHELL   
  
**Q: - Write a command to find all of the files which have been accessed within the last 30 days.**  
find / -type f -atime -30 > filename.txt  
  
**Q: - What is a zombie?**  
Zombie is a process state when the child dies before the parent process. In this case the structural information of the process is still in the process table.  
  
**Q: - What daemon is responsible for tracking events on your system?**  
syslogd   
  
**Q: - What do you mean a File System?**  
File System is a method to store and organize files and directories on disk. A file system can have different formats called file system types. These formats determine how the information is stored as files and directories.  
  
**Q: - Tell me the name of directory structure hierarchy for Linux**  
/root  
/boot  
/bin  
/sbin  
/proc  
/mnt  
/usr  
/var  
/lib  
/etc  
/dev  
/opt  
/srv  
/tmp  
/media   
  
**Q: - What does /boot directory contains?**  
The /boot/ directory contains static files required to boot the system, such as the Linux kernel, boot loader configuration files. These files are essential for the system to boot properly.   
  
**Q: - If some one deletes /boot directory from your server, than what will happen?**  
In that case your server will be in unbootable state. Your Server can’t boot without /boot directory because this directory contains all bootable files   
  
**Q: - What does /dev directory contain?**  
The /dev directory contains all device files that are attached to system or virtual device files that are provided by the kernel.  
  
**Q: - What is the role of udev daemon?**  
The udev demon used to create and remove all these device nodes or files in /dev/ directory.   
  
**Q: - What kind of files or nodes /dev/ directory contains and how do I access or see device files?**  
**Block Device Files:-**  
Block device files talks to devices block by block [1 block at a time (1 block = 512 bytes to 32KB)].  
Examples: - USB disk, CDROM, Hard Disk  
  
# ls /dev/sd\*   
brw-rw----   
1 root   
root   
8,   
0 Mar 15 2009 sda   
brw-rw----   
1 root   
root   
8,   
1 Mar 15 2009 sda1   
brw-rw----   
1 root   
root   
8,   
2 Mar 15 2009 sda2   
brw-rw----   
1 root   
root   
8,   
3 Mar 15 2009 sda3   
brw-rw----   
1 root   
root   
8,   
4 Mar 15 2009 sda4   
brw-rw----   
1 root   
root   
8,   
16 Mar 15 2009 sdb   
  
**Character Device Files:-**   
  
Character device files talk to devices character by character.  
Examples: - Virtual terminals, terminals, serial modems, random numbers  
  
**#ls /dev/tty\***  
crw-rw----   
1 root   
root   
4,   
64 Mar 15 2009 ttyS0   
crw-rw----   
1 root   
root   
4,   
65 Mar 15 2009 ttyS1   
crw-rw----   
1 root   
root   
4,   
66 Mar 15 2009 ttyS2   
crw-rw----   
1 root   
root   
4,   
67 Mar 15 2009 ttyS3   
  
  
**Q: - Tell me the name of device file for PS/2 mouse connection.**  
/dev/psaux  
  
**Q: - Tell me the name of device file for parallel port (Printers).**  
/dev/lp0   
  
**Q: - What does /etc/X11/ directory contains?**  
The /etc/X11/ directory is for X Window System configuration files, such as xorg.conf.  
  
**Q: - What does /etc/skell directory contains?**  
The /etc/skel directory contains files and directories that are automatically copied over to a new user's home directorywhen such user is created by the useradd or adduser command.  
  
**Q: - Tell me name of Linux File systems?**  
Ext2  
Ext3  
  
**Q: - What is the difference between ext2 and ext3 file systems?**  
The ext3 file system is an enhanced version of the ext2 file system.  
The most important difference between Ext2 and Ext3 is that Ext3 supports journaling.  
After an unexpected power failure or system crash (also called an unclean system shutdown), each mounted ext2 file system on the machine must be checked for consistency by the e2fsck program. This is a time-consuming process and during this time, any data on the volumes is unreachable.  
The journaling provided by the ext3 file system means that this sort of file system check is no longer necessary after an unclean system shutdown. The only time a consistency check occurs using ext3 is in certain rare hardware failure cases, such as hard drive failures. The time to recover an ext3 file system after an unclean system shutdown does not depend on the size of the file system or the number of files; rather, it depends on the size of the journal used to maintain consistency. The default journal size takes about a second to recover, depending on the speed of the hardware.  
  
**Q: - Any idea about ext4 file system?**  
The ext4 or fourth extended filesystem is a journaling file system developed as the successor to ext3. Ext4 filesystem released as a functionally complete and stable filesystem in Linux with kernel version 2.6.28.  
Features of ext4 file system:-  
1. Currently, Ext3 supports 16 TB of maximum file system size and 2 TB of maximum file size. Ext4 have 1 EB of maximum file system size and 16 **TB** of maximum file size.  
[An **EB** or exabyte is 1018 bytes or 1,048,576 TB]  
2. Fast fsck check than ext3  
3 In Ext4 the journaling feature can be disabled, which provides a small performance improvement.  
4. Online defragmentation.  
5. Delayed allocation  
Ext4 uses a filesystem performance technique called allocate-on-flush, also known as delayed allocation. It consists of delaying block allocation until the data is going to be written to the disk, unlike some other file systems, which may allocate the necessary blocks before that step.  
  
**Q: - How we create ext3 file system on /dev/sda7 disk?**  
# mkfs –j /dev/sda7  
  
**Q: - Can we convert ext2 filesystem to ext3 file system?**  
Yes, we can convert ext2 to ext3 file system by tune2fs command.  
tune2fs –j /dev/<Block-Device-Name>  
  
**Q: - <p class="ans">**  
No  
  
**Q: - How we will create ext4 file system?**  
# mke2fs -t ext4 /dev/DEV   
  
**Q: - Explain /proc filesystem?**  
/proc is a virtual filesystem that provides detailed information about Linux kernel, hardware’s and running processes. Files under /proc directory named as Virtual files. Because /proc contains virtual files that’s why it is called virtual file system. These virtual files have unique qualities. Most of them are listed as zero bytes in size. Virtual files such as /proc/interrupts, /proc/meminfo, /proc/mounts, and /proc/partitions provide an up-to-the-moment glimpse of the system's hardware. Others, like the /proc/filesystems file and the /proc/sys/ directory provide system configuration information and interfaces.  
  
**Q: - Can we change files parameters placed under /proc directory?**  
Yes  
To change the value of a virtual file, use the echo command and a greater than symbol (>) to redirect the new value to the file. For example, to change the hostname on the fly, type:   
echo www.nextstep4it.com > /proc/sys/kernel/hostname   
  
**Q: - What is the use of sysctl command?**  
The /sbin/sysctl command is used to view, set, and automate kernel settings in the /proc/sys/ directory.   
  
**Q: - /proc/ directory contains a number of directories with numerical names. What is that?**  
These directories are called process directories, as they are named after a program's process ID and contain information specific to that process.  
  
**Q: - What is RAID?**  
RAID, stands for Redundant Array of Inexpensive Disks. RAID is a method by which same data or information is spread across several disks, using techniques such as disk striping (RAID Level 0), disk mirroring (RAID Level 1), and disk striping with parity (RAID Level 5) to achieve redundancy, lower latency, increased bandwidth, and maximized ability to recover from hard disk crashes.  
  
**Q: - Why should we use RAID?**  
System Administrators and others who manage large amounts of data would benefit from using RAID technology.  
Following are the reasons to use RAID  
- Enhances speed  
- Increases storage capacity using a single virtual disk   
- Minimizes disk failure  
  
**Q: - What is the difference between hardware RAID and Software RAID?**  
The hardware-based RAID is independent from the host. A Hardware RAID device connects to the SCSI controller and presents the RAID arrays as a single SCSI drive. An external RAID system moves all RAID handling "intelligence" into a controller located in the external disk subsystem. The whole subsystem is connected to the host via a normal SCSI controller and appears to the host as a single disk.  
Software RAID is implemented under OS Kernel level. The Linux kernel contains an MD driver that allows the RAID solution to be completely hardware independent. The performance of a software-based array depends on the server CPU performance and load.  
  
**Q: - What are the commonly used RAID types?**  
RAID 0  
RAID 1  
RAID 5  
  
**Q: - Explain RAID 0?**  
RAID level 0 works on “striping” technique. In RAID 0 the array is broken down into strips and data is written into strips. RAID 0 allows high I/O performance but provides no redundancy. RAID 0 Array Size is equal to sum of disks in array. If one drive fails then all data in the array is lost.  
  
**Q: - Explain RAID 1?**  
RAID Level 1 is based on Mirroring technique. Level 1 provides redundancy by writing identical data to each member disk of the array. The storage capacity of the level 1 array is equal to the capacity of one of the mirrored hard disks in a Hardware RAID or one of the mirrored partitions in a Software RAID. RAID 1 provides redundancy means good protection against disk failure. In RAID 1 write speed is slow but read speed is good.  
  
**Q: - Explain RAID 5?**  
RAID Level 5 is based on rotating parity with striping technique. RAID-5 stores parity information but not redundant data (but parity information can be used to reconstruct data). The storage capacity of Software RAID level 5 is equal to the capacity of the member partitions, minus the size of one of the partitions if they are of equal size. The performance of RAID 5 is based on parity calculation process but with modern CPUs that usually is not a very big problem. In RAID 5 read and write speeds are good.  
  
**Q: - Which kernel module is required for Software RAID?**  
“md” module  
  
**Q: - which utility or command is used for creating software RAID’s for RHEL5?**  
mdadm  
  
**Q: - Can we create software RAID during Linux installation?**  
Yes, we can create Software RAID during Linux Installation by “**Disk Druid”**  
  
**Q: - What is the role of chunk size for software RAID?**  
Chunk size is very important parameter on which RAID performance based.  
We know stripes go across disk drives. But how big are the pieces of the stripe on each disk? The pieces a stripe is broken into are called chunks.To get good performance you must have a reasonable chunk size.  
For big I/Os we required small chunks and for small I/Os we required big chunks.  
  
**Q: - What is SWAP Space?**  
Swap space in Linux is used when the amount of physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space. While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM. Swap space is located on hard drives, which have a slower access time than physical memory.  
  
**Q: - What are the steps to create SWAP files or Partition?**  
- Create swap partition or file  
- Write special signature using “**mkswap**”  
- Activate swap space by “**swapon –a**” command  
- Add swap entry into /etc/fstab file  
  
**Q: - How you will create swap file of size 4 GB and explain swap file entry in /etc/fstab file?**  
Use “dd” command to create swap file.  
dd if=/dev/zero of=/SWAPFILE bs=1024 count=4  
mkswap /SWAPFILE  
swapon –a  
Entry into /etc/fstab file.  
/SWAPFILE swap swap defaults 0 0  
  
**Q: - Tell me the steps to remove the swap file?**  
Firstly disable the swap file by “swapoff” command.  
Remove Swap file entry from /etc/fstab file.  
Now remove the swap file by “rm” command.  
  
**Q: - What can we do with “parted” command or utility?**  
- View the existing partition table  
- Add partitions from free space or additional hard drives  
- Change the size of existing partitions  
  
**Q: - How we will check free space on drive /dev/sda with parted command?**  
#parted /dev/sda  
  
**Q: - Can we resize the size of a partition?**  
Yes, we can resize the size of partition by “parted” command.  
**#parted /dev/sda**  
**print**  
To resize the partition, use the resize command followed by the minor number for the partition, the starting place in megabytes, and the end place in megabytes. For example:  
resize 3 1024 2048  
After resizing the partition, use the print command to confirm that the partition has been resized correctly, is the correct partition type, and is the correct file system type.  
  
**Q: - What is LVM?**  
LVM stands for Logical Volume Manager. LVM, is a storage management solution that allows administrators to divide hard drive space into physical volumes (PV), which can then be combined into logical volume groups (VG), which are then divided into logical volumes (LV) on which the filesystem and mount point are created.  
  
**Q: - What are the steps to create LVM?**  
- Create physical volumes by “pvcreate” command  
#pvcreate /dev/sda2  
- Add physical volume to volume group by “vgcreate” command  
#vgcreate VLG0 /dev/sda2  
- Create logical volume from volume group by “lvcreate” command.  
#lvcreate -L 1G -n LVM1 VLG0  
Now create file system on /dev/sda2 partition by “mke2fs” command.  
#mke2fs -j /dev/VLG0/LVM1  
  
**Q: - What is the difference between LVM and RAID?**  
RAID provides redundancy but LVM doesn’t provide Redundancy.  
  
**Q: - What are LVM1 and LVM2?**  
LVM1 and LVM2 are the versions of LVM.   
LVM2 uses device mapper driver contained in 2.6 kernel version.  
LVM 1 was included in the 2.4 series kernels.  
  
**Q: - What is Volume group (VG)?**  
The Volume Group is the highest level abstraction used within the LVM. It gathers together a collection of Logical Volumes and Physical Volumes into one administrative unit.  
  
**Q: - What is physical extent (PE)?**  
Each physical volume is divided chunks of data, known as physical extents; these extents have the same size as the logical extents for the volume group.  
  
**Q: - What is logical extent (LE)?**  
Each logical volume is split into chunks of data, known as logical extents. The extent size is the same for all logical volumes in the volume group.  
  
**Q: - Explain LVM snapshot?**  
LVM snapshots allow the administrator to create a new block device which presents an exact copy of a logical volume, frozen at some point in time.  
  
**Q: - How you will check on Your server or system device-mapper is installed or not?**  
Check the following file.  
#cat /proc/misc  
if this file contains "device-mapper" term it means device mapper is installed on your system.  
  
**Q: - How are snapshots in LVM2 different from LVM1?**  
In LVM2 snapshots are read/write by default, whereas in LVM1, snapshots were read only.  
  
**Q: - What is the maximum size of a single LV?**  
For 2.4 based kernels, the maximum LV size is 2TB.   
For 32-bit CPUs on 2.6 kernels, the maximum LV size is 16TB.  
For 64-bit CPUs on 2.6 kernels, the maximum LV size is 8EB.   
  
**Q: - If a volume group named as VG0 already exists but i need to extend this volume group up to 4GB.Explain all steps?**  
Firstly create Physical volume (/dev/sda7) of size 4GB.  
Now run following command.  
vgextend VG0 /dev/sda7  
  
**Q: - If a volume group VG0 have 3 PV's (/dev/sda6, /dev/sda7, /dev/sda8) but i want to remove /dev/sda7 pv from this VG0?**  
vgreduce VG0 /dev/sda7  
  
**Q: - Which command is used to extend a logical volume?**  
lvextend --size +<addsize> /dev/<vgname>/<lvname>  
resize2fs /dev/<vgname>/<lvname>  
  
**Q: - Tell me all steps to remove a LVM?**  
To remove a logical volume from a volume group, first unmount it with the umount command:  
umount /dev/<vgname>/<lvname>  
and then use the lvremove command:  
lvremove /dev/<vgname>/<lvname>  
  
**Q: - Which command is used to create LVM Snapshot?**  
vcreate --size <size> -s -n <snapshotname> <lvname>  
The lvcreate command is used to create a new logical volume, meaning there must be  
free physical extents in the logical volume group to create a snapshot. The -s option  
means that the LV is a snapshot, <snapshotname> is the name of the new LV created, and  
< lvname> is the name of the LV from which to create the snapshot.  
  
**Q: - Is there any relation between modprobe.conf file and network devices?**  
Yes, This file assigns a kernel module to each network device.  
For Example :-   
[root@localhost ~]# cat /etc/modprobe.conf  
alias eth0 b44  
Here b44 is the kernel module for network device eth0.  
We can Confirm by following command (This module “b44” is present or not).  
[root@localhost ~]# lsmod |grep b44   
b44 29005 0  
  
**Q: - What is the location of "network" file and what does this contains?**  
location :- /etc/sysconfig/network  
This file contains following fields  
NETWORKING=yes  
NETWORKING\_IPV6=no  
HOSTNAME=localhost.localdomain  
  
**Q: - Which deamon is required to start Network services?**  
network  
/etc/init.d/network start  
  
**Q: - What is the role of /etc/resolv.conf file?**  
In this file we sets the DNS servers (using their IP addresses) and the search domain. The values of the DNS servers are often added when the network is activated because the data can be provided by DHCP or a similar service.  
  
**Q: - What "neat" command will do?**  
neat command provides Graphical interface to change network settings for network devices.  
  
**Q: - Which protocol is required to allow local printing and print sharing?**  
Internet Printing Protocol (IPP) is required to allow local printing and print sharing.  
  
**Q: - What is CUPS?**  
CUPS stands for "Common UNIX Printing System". CUPS is a open source printing system developed by Apple Inc. CUPS uses the Internet Printing Protocol (IPP) to allow local printing and print sharing.  
  
**Q: - What is the location of log files for CUPS?**  
The log files for the CUPS printing system are located in the /var/log/cups/ directory.  
  
**Q: - What is YUM?**  
YUM stands for Yellow dog Updater, Modified because it is based on YUP, the Yellow dog Updater. Where does the name Yellow dog come from? Yellow Dog is a version of Linux for the Power Architecture hardware and is RPM-based, just like Red Hat Enterprise Linux and Fedora. YUP, and later YUM, were written by the Linux community as a way to maintain an RPM-based system.   
  
**Q: - What are the advantages of YUM?**  
- Automatic resolution of software dependencies.  
- Multiple software locations at one time.  
- Ability to specify particular software versions or architectures.  
  
**Q: - How you will install software by YUM?**  
yum install <pkgname>  
  
**Q: - Which option is required to assume the answer "yes" to any questions asked during installation of package dependencies for YUM?**  
The "-y" option is used to assume the answer "yes".  
For Example  
yum -y install squid  
  
**Q: - How to remove a software by YUM?**  
yum remove <pkgname>  
  
**Q: - How Many Run Levels present in Linux?**  
There are 7 run levels, with each having its own properties.  
- 0: Halt the system  
- 1: Single-user mode   
- 2: Not used  
- 3: Multi-user mode with text login  
- 4: Not used  
- 5: Multi-user mode with graphical login  
- 6: Reboot  
  
**Q: - Which configuration file is required to change the Run Level of Server or system?**  
/etc/inittab  
To change the default run level, modify this line.  
id:5:initdefault:  
  
**Q: - Explain architectures required for RPMs?**  
noarch Architecture-independent, can run on any architecture  
i386 Generic build for a 32-bit x86 system  
i586 Sometimes used when building kernels for older x86 processors  
Intel® Pentium ® II, Intel Pentium III, Intel Pentium 4, AMD Athlon, and  
i686 AMD Duron systems (Most RPMs for these architectures are built using the i386 architecture, with the kernel for these architectures being built with the  
i686 for optimal performance.)  
x86\_64 64-bit processors such as AMD Athlon64, AMD Opteron, and Intel EM64T  
ia64 Intel® Itanium  
ppc 32-bit IBM® POWER, IBM eServer„ pSeries®, and IBM eServer iSeries  
s390x 64-bit IBM eServer System z  
  
**Q: - How to install Linux software’s by RPM?**  
rpm -ivh test-1.0-1.i386.rpm  
  
**Q: - If a file associated with test-1.0-1.i386.rpm deleted, than How we will recover that file?**  
We can reinstall this rpm again.  
  
**Q: - If you are getting error "package is already installed" but you have to install package any how. what option you will use?**  
rpm -ivh test-1.0-1.i386.rpm  
Preparing... ########################################### [100%] package test-1.0-1 is already installed  
In this case you can use "--replacepkgs" option.  
rpm -ivh –replacepkgs test-1.0-1.i386.rpm  
  
**Q: - Which options are required to upgrade a RPM?**  
Upgrading a package is similar to installing one. Type the following command at a shell prompt:  
rpm -Uvh test-2.0-1.i386.rpm  
  
**Q: - In which directory RPM database stored?**  
/var/lib/rpm   
  
**Q: - Explain the command "rpm -qa"?**  
It will queries all currently installed packages.  
  
**Q: - Explain the command "rpm -qf "?**  
it queries the RPM database for which package owns <filename>. When specifying a file, specify the absolute path of the file.  
  
**Q: - How to verify all installed packages?**  
rpm -Va  
  
**Q: - How to verify the signature of an rpm?**  
rpm -K test-1.0-1.i386.rpm  
  
**Q: - How to list PCI Devices on your server or System?**  
use "lspci" command.  
  
**Q: - What is the role of "Kudzu"?**  
Kudzu is used to Detect new Hardware  
  
**Q: - What happens when you add a new device after installation?**  
The Kudzu program runs each time the system boots and performs a hardware probe. If new hardware is found, Kudzu attempts to map it to a kernel module. If successful, the information is saved, and the device is configured.  
  
**Q: - How to Enable ACLs for /home partition?**  
Add following entry in /etc/fstab  
LABEL=/home /home ext3 acl 1 2  
Now remount /home partition with acl option.  
mount -t ext3 -o acl /dev/sda3 /home  
  
**Q: - How to View ACLs for a file(test\_file)?**  
getfacl test\_file  
  
**Q: - How to remove an ACL?**  
setfacl --remove-all <file-name>

**20 Tips to Linux Server Hardening Security**

**Linux Server Hardening**  
Securing your Linux server is important to protect your data, intellectual property, and time, from the hands of crackers (hackers). The system administrator is responsible for security Linux box. In this first part of a Linux server security series, I will provide 20 hardening tips for default installation of Linux system.  
  
**#1: Encrypt Data Communication**  
  
All data transmitted over a network is open to monitoring. Encrypt transmitted data whenever possible with password or using keys / certificates.  
1. Use scp, ssh, rsync, or sftp for file transfer. You can also mount remote server file system or your own home directory using special sshfs and fuse tools.  
2. GnuPG allows to encrypt and sign your data and communication, features a versatile key managment system as well as access modules for all kind of public key directories.  
3. Fugu is a graphical frontend to the commandline Secure File Transfer application (SFTP). SFTP is similar to FTP, but unlike FTP, the entire session is encrypted, meaning no passwords are sent in cleartext form, and is thus much less vulnerable to third-party interception. Another option is FileZilla - a cross-platform client that supports FTP, FTP over SSL/TLS (FTPS), and SSH File Transfer Protocol (SFTP).  
4. OpenVPN is a cost-effective, lightweight SSL VPN.  
5. Lighttpd SSL (Secure Server Layer) Https Configuration And Installation  
6. Apache SSL (Secure Server Layer) Https (mod\_ssl) Configuration And Installation  
  
**#1.1: Avoid Using FTP, Telnet, And Rlogin / Rsh**  
Under most network configurations, user names, passwords, FTP / telnet / rsh commands and transferred files can be captured by anyone on the same network using a packet sniffer. The common solution to this problem is to use either OpenSSH , SFTP, or FTPS (FTP over SSL), which adds SSL or TLS encryption to FTP. Type the following command to delete NIS, rsh and other outdated service:  
# yum erase inetd xinetd ypserv tftp-server telnet-server rsh-serve  
  
**#2: Minimize Software to Minimize Vulnerability**  
Do you really need all sort of web services installed? Avoid installing unnecessary software to avoid vulnerabilities in software. Use the RPM package manager such as yum or apt-get and/or dpkg to review all installed set of software packages on a system. Delete all unwanted packages.  
# yum list installed  
# yum list packageName  
# yum remove packageName  
OR  
# dpkg --list  
# dpkg --info packageName  
# apt-get remove packageName  
  
**#3: One Network Service Per System or VM Instance**  
Run different network services on separate servers or VM instance. This limits the number of other services that can be compromised. For example, if an attacker able to successfully exploit a software such as Apache flow, he / she will get an access to entire server including other services such as MySQL, e-mail server and so on. See how to install Virtualization software:  
• Install and Setup XEN Virtualization Software on CentOS Linux 5  
• How To Setup OpenVZ under RHEL / CentOS Linux  
  
**#4: Keep Linux Kernel and Software Up to Date**  
Applying security patches is an important part of maintaining Linux server. Linux provides all necessary tools to keep your system updated, and also allows for easy upgrades between versions. All security update should be reviewed and applied as soon as possible. Again, use the RPM package manager such as yum and/or apt-get and/or dpkg to apply all security updates.  
# yum update  
OR  
# apt-get update && apt-get upgrade  
You can configure Red hat / CentOS / Fedora Linux to send yum package update notification via email. Another option is to apply all security updates via a cron job. Under Debian / Ubuntu Linux you can use apticron to send security notifications.  
  
**#5: Use Linux Security Extensions**  
Linux comes with various security patches which can be used to guard against misconfigured or compromised programs. If possible use SELinux and other Linux security extensions to enforce limitations on network and other programs. For example, SELinux provides a variety of security policies for Linux kernel.  
**#5.1: SELinux**  
I strongly recommend using SELinux which provides a flexible Mandatory Access Control (MAC). Under standard Linux Discretionary Access Control (DAC), an application or process running as a user (UID or SUID) has the user's permissions to objects such as files, sockets, and other processes. Running a MAC kernel protects the system from malicious or flawed applications that can damage or destroy the system. See the official Redhat documentation which explains SELinux configuration.  
  
**#6: User Accounts and Strong Password Policy**  
Use the useradd / usermod commands to create and maintain user accounts. Make sure you have a good and strong password policy. For example, a good password includes at least 8 characters long and mixture of alphabets, number, special character, upper & lower alphabets etc. Most important pick a password you can remember. Use tools such as "John the ripper" to find out weak users passwords on your server. Configure pam\_cracklib.so to enforce the password policy.  
  
**#6.1: Password Aging**  
The chage command changes the number of days between password changes and the date of the last password change. This information is used by the system to determine when a user must change his/her password. The /etc/login.defs file defines the site-specific configuration for the shadow password suite including password aging configuration. To disable password aging, enter:  
chage -M 99999 userName  
To get password expiration information, enter:  
chage -l userName  
Finally, you can also edit the /etc/shadow file in the following fields:  
{userName}:{password}:{lastpasswdchanged}:{Minimum\_days}:{Maximum\_days}:{Warn}:{Inactive}:{Expire}:  
Where,  
1. Minimum\_days: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password.  
2. Maximum\_days: The maximum number of days the password is valid (after that user is forced to change his/her password).  
3. Warn : The number of days before password is to expire that user is warned that his/her password must be changed.  
4. Expire : Days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.  
I recommend chage command instead of editing the /etc/shadow by hand:  
# chage -M 60 -m 7 -W 7 userName  
Recommend readings:  
• Linux: Force Users To Change Their Passwords Upon First Login  
• Linux turn On / Off password expiration / aging  
• Lock the user password  
• Search for all account without password and lock them  
• Use Linux groups to enhance security  
  
**#6.2: Restricting Use of Previous Passwords**  
You can prevent all users from using or reuse same old passwords under Linux. The pam\_unix module parameter remember can be used to configure the number of previous passwords that cannot be reused.  
  
**#6.3: Locking User Accounts After Login Failures**  
Under Linux you can use the faillog command to display faillog records or to set login failure limits. faillog formats the contents of the failure log from /var/log/faillog database / log file. It also can be used for maintains failure counters and limits.To see failed login attempts, enter:  
faillog  
To unlock an account after login failures, run:  
faillog -r -u userName  
Note you can use passwd command to lock and unlock accounts:  
# lock account  
passwd -l userName  
# unlocak account  
passwd -u userName  
  
**#6.4: How Do I Verify No Accounts Have Empty Passwords?**  
Type the following command  
# awk -F: '($2 == "") {print}' /etc/shadow  
Lock all empty password accounts:  
# passwd -l accountName  
  
**#6.5: Make Sure No Non-Root Accounts Have UID Set To 0**  
Only root account have UID 0 with full permissions to access the system. Type the following command to display all accounts with UID set to 0:  
# awk -F: '($3 == "0") {print}' /etc/passwd  
You should only see one line as follows:  
root:x:0:0:root:/root:/bin/bash  
If you see other lines, delete them or make sure other accounts are authorized by you to use UID 0.  
  
**#7: Disable root Login**  
Never ever login as root user. You should use sudo to execute root level commands as and when required. sudo does greatly enhances the security of the system without sharing root password with other users and admins. sudo provides simple auditing and tracking features too.  
  
**#8: Physical Server Security**  
You must protect Linux servers physical console access. Configure the BIOS and disable the booting from external devices such as DVDs / CDs / USB pen. Set BIOS and grub boot loader password to protect these settings. All production boxes must be locked in IDCs (Internet Data Center) and all persons must pass some sort of security checks before accessing your server. See also:  
• 9 Tips To Protect Linux Servers Physical Console Access.  
  
**#9: Disable Unwanted Services**  
Disable all unnecessary services and daemons (services that runs in the background). You need to remove all unwanted services from the system start-up. Type the following command to list all services which are started at boot time in run level # 3:  
# chkconfig --list | grep '3:on'  
To disable service, enter:  
# service serviceName stop  
# chkconfig serviceName off  
  
**#9.1: Find Listening Network Ports**  
Use the following command to list all open ports and associated programs:  
netstat -tulpn  
OR  
nmap -sT -O localhost  
nmap -sT -O server.example.com  
Use iptables to close open ports or stop all unwanted network services using above service and chkconfig commands.  
  
**#9.2: See Also**  
• update-rc.d like command on Redhat Enterprise / CentOS Linux.  
• Ubuntu / Debian Linux: Services Configuration Tool to Start / Stop System Services.  
• Get Detailed Information About Particular IP address Connections Using netstat Command.  
  
**#10: Delete X Windows**  
X Windows on server is not required. There is no reason to run X Windows on your dedicated mail and Apache web server. You can disable and remove X Windows to improve server security and performance. Edit /etc/inittab and set run level to 3. Finally, remove X Windows system, enter:  
# yum groupremove "X Window System"  
  
**#11: Configure Iptables and TCPWrappers**  
Iptables is a user space application program that allows you to configure the firewall (Netfilter) provided by the Linux kernel. Use firewall to filter out traffic and allow only necessary traffic. Also use the TCPWrappers a host-based networking ACL system to filter network access to Internet. You can prevent many denial of service attacks with the help of Iptables:  
• Lighttpd Traffic Shaping: Throttle Connections Per Single IP (Rate Limit).  
• How to: Linux Iptables block common attack.  
• psad: Linux Detect And Block Port Scan Attacks In Real Time.  
  
**#12: Linux Kernel /etc/sysctl.conf Hardening**  
/etc/sysctl.conf file is used to configure kernel parameters at runtime. Linux reads and applies settings from /etc/sysctl.conf at boot time. Sample /etc/sysctl.conf:  
# Turn on execshield  
kernel.exec-shield=1  
kernel.randomize\_va\_space=1  
# Enable IP spoofing protection  
net.ipv4.conf.all.rp\_filter=1  
# Disable IP source routing  
net.ipv4.conf.all.accept\_source\_route=0  
# Ignoring broadcasts request  
net.ipv4.icmp\_echo\_ignore\_broadcasts=1  
net.ipv4.icmp\_ignore\_bogus\_error\_messages=1  
# Make sure spoofed packets get logged  
net.ipv4.conf.all.log\_martians = 1  
  
**#13: Separate Disk Partitions**  
Separation of the operating system files from user files may result into a better and secure system. Make sure the following filesystems are mounted on separate partitions:  
• /usr  
• /home  
• /var and /var/tmp  
• /tmp  
Create separate partitions for Apache and FTP server roots. Edit /etc/fstab file and make sure you add the following configuration options:  
1. noexec - Do not set execution of any binaries on this partition (prevents execution of binaries but allows scripts).  
2. nodev - Do not allow character or special devices on this partition (prevents use of device files such as zero, sda etc).  
3. nosuid - Do not set SUID/SGID access on this partition (prevent the setuid bit).  
Sample /etc/fstab entry to to limit user access on /dev/sda5 (ftp server root directory):  
/dev/sda5 /ftpdata ext3 defaults,nosuid,nodev,noexec 1 2  
**#13.1: Disk Quotas**  
Make sure disk quota is enabled for all users. To implement disk quotas, use the following steps:  
1. Enable quotas per file system by modifying the /etc/fstab file.  
2. Remount the file system(s).  
3. Create the quota database files and generate the disk usage table.  
4. Assign quota policies.  
5. See implementing disk quotas tutorial for further details.  
  
**#14: Turn Off IPv6**  
Internet Protocol version 6 (IPv6) provides a new Internet layer of the TCP/IP protocol suite that replaces Internet Protocol version 4 (IPv4) and provides many benefits. Currently there are no good tools out which are able to check a system over network for IPv6 security issues. Most Linux distro began enabling IPv6 protocol by default. Crackers can send bad traffic via IPv6 as most admins are not monitoring it. Unless network configuration requires it, disable IPv6 or configure Linux IPv6 firewall:  
• RedHat / Centos Disable IPv6 Networking.  
• Debian / Ubuntu And Other Linux Distros Disable IPv6 Networking.  
• Linux IPv6 Howto - Chapter 19. Security.  
• Linux IPv6 Firewall configuration and scripts are available here.  
  
**#15: Disable Unwanted SUID and SGID Binaries**  
All SUID/SGID bits enabled file can be misused when the SUID/SGID executable has a security problem or bug. All local or remote user can use such file. It is a good idea to find all such files. Use the find command as follows:  
#See all set user id files:  
find / -perm +4000  
# See all group id files  
find / -perm +2000  
# Or combine both in a single command  
find / \( -perm -4000 -o -perm -2000 \) -print  
find / -path -prune -o -type f -perm +6000 -ls  
  
You need to investigate each reported file. See reported file man page for further details.  
  
**#15.1: World-Writable Files**  
Anyone can modify world-writable file resulting into a security issue. Use the following command to find all world writable and sticky bits set files:  
find /dir -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print  
You need to investigate each reported file and either set correct user and group permission or remove it.  
  
**#15.2: Noowner Files**  
Files not owned by any user or group can pose a security problem. Just find them with the following command which do not belong to a valid user and a valid group  
find /dir -xdev \( -nouser -o -nogroup \) -print  
You need to investigate each reported file and either assign it to an appropriate user and group or remove it.  
  
**#16: Use A Centralized Authentication Service**  
Without a centralized authentication system, user auth data becomes inconsistent, which may lead into out-of-date credentials and forgotten accounts which should have been deleted in first place. A centralized authentication service allows you maintaining central control over Linux / UNIX account and authentication data. You can keep auth data synchronized between servers. Do not use the NIS service for centralized authentication. Use OpenLDAP for clients and servers.  
  
**#16.1: Kerberos**  
Kerberos performs authentication as a trusted third party authentication service by using cryptographic shared secret under the assumption that packets traveling along the insecure network can be read, modified, and inserted. Kerberos builds on symmetric-key cryptography and requires a key distribution center. You can make remote login, remote copy, secure inter-system file copying and other high-risk tasks safer and more controllable using Kerberos. So, when users authenticate to network services using Kerberos, unauthorized users attempting to gather passwords by monitoring network traffic are effectively thwarted. See how to setup and use Kerberos.  
  
**#17: Logging and Auditing**  
You need to configure logging and auditing to collect all hacking and cracking attempts. By default syslog stores data in /var/log/ directory. This is also useful to find out software misconfiguration which may open your system to various attacks. See the following logging related articles:  
1. Linux log file locations.  
2. How to send logs to a remote loghost.  
3. How do I rotate log files?.  
4. man pages syslogd, syslog.conf and logrotate.  
  
**#17.1: Monitor Suspicious Log Messages With Logwatch / Logcheck**  
Read your logs using logwatch or logcheck. These tools make your log reading life easier. You get detailed reporting on unusual items in syslog via email. A sample syslog report:  
################### Logwatch 7.3 (03/24/06) ####################  
Processing Initiated: Fri Oct 30 04:02:03 2009  
Date Range Processed: yesterday  
( 2009-Oct-29 )  
Period is day.  
Detail Level of Output: 0  
Type of Output: unformatted  
Logfiles for Host: www-52.nixcraft.net.in  
##################################################################  
--------------------- Named Begin ------------------------  
\*\*Unmatched Entries\*\*  
general: info: zone XXXXXX.com/IN: Transfer started.: 3 Time(s)  
general: info: zone XXXXXX.com/IN: refresh: retry limit for master ttttttttttttttttttt#53 exceeded (source ::#0): 3 Time(s)  
general: info: zone XXXXXX.com/IN: Transfer started.: 4 Time(s)  
general: info: zone XXXXXX.com/IN: refresh: retry limit for master ttttttttttttttttttt#53 exceeded (source ::#0): 4 Time(s)  
---------------------- Named End -------------------------  
--------------------- iptables firewall Begin ------------------------  
Logged 87 packets on interface eth0  
From 58.y.xxx.ww - 1 packet to tcp(8080)  
From 59.www.zzz.yyy - 1 packet to tcp(22)  
From 60.32.nnn.yyy - 2 packets to tcp(45633)  
From 222.xxx.ttt.zz - 5 packets to tcp(8000,8080,8800)  
---------------------- iptables firewall End -------------------------  
--------------------- SSHD Begin ------------------------  
Users logging in through sshd:  
root:  
123.xxx.ttt.zzz: 6 times  
---------------------- SSHD End -------------------------  
--------------------- Disk Space Begin ------------------------  
Filesystem Size Used Avail Use% Mounted on  
/dev/sda3 450G 185G 241G 44% /  
/dev/sda1 99M 35M 60M 37% /boot  
---------------------- Disk Space End -------------------------  
###################### Logwatch End #########################  
(Note output is truncated)  
**#17.2: System Accounting with auditd**  
The auditd is provided for system auditing. It is responsible for writing audit records to the disk. During startup, the rules in /etc/audit.rules are read by this daemon. You can open /etc/audit.rules file and make changes such as setup audit file log location and other option. With auditd you can answers the following questions:  
1. System startup and shutdown events (reboot / halt).  
2. Date and time of the event.  
3. User respoisble for the event (such as trying to access /path/to/topsecret.dat file).  
4. Type of event (edit, access, delete, write, update file & commands).  
5. Success or failure of the event.  
6. Records events that Modify date and time.  
7. Find out who made changes to modify the system's network settings.  
8. Record events that modify user/group information.  
9. See who made changes to a file etc.  
See our quick tutorial which explains enabling and using the auditd service.  
  
**#18: Secure OpenSSH Server**  
The SSH protocol is recommended for remote login and remote file transfer. However, ssh is open to many attacks. See how to secure OpenSSH server:  
• Top 20 OpenSSH Server Best Security Practices.  
  
**#19: Install And Use Intrusion Detection System**  
A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.  
It is a good practice to deploy any integrity checking software before system goes online in a production environment. If possible install AIDE software before the system is connected to any network. AIDE is a host-based intrusion detection system (HIDS) it can monitor and analyses the internals of a computing system.  
Snort is a software for intrusion detection which is capable of performing packet logging and real-time traffic analysis on IP networks.  
  
**#20: Protecting Files, Directories and Email**  
Linux offers excellent protections against unauthorized data access. File permissions and MAC prevent unauthorized access from accessing data. However, permissions set by the Linux are irrelevant if an attacker has physical access to a computer and can simply move the computer's hard drive to another system to copy and analyze the sensitive data. You can easily protect files, and partitons under Linux using the following tools:  
• To encrypt and decrypt files with a password, use gpg command.  
• Linux or UNIX password protect files with openssl and other tools.  
• See how to encrypting directories with ecryptfs.  
• TrueCrypt is free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X and Linux.  
• Howto: Disk and partition encryption in Linux for mobile devices.  
• How to setup encrypted Swap on Linux.  
  
**#20.1: Securing Email Servers**  
You can use SSL certificates and gpg keys to secure email communication on both server and client computers:  
• Linux Securing Dovecot IMAPS / POP3S Server with SSL Configuration.  
• Linux Postfix SMTP (Mail Server) SSL Certificate Installations and Configuration.  
• Courier IMAP SSL Server Certificate Installtion and Configuration.  
• Configure Sendmail SSL encryption for sending and receiving email.  
• Enigmail: Encrypted mail with Mozilla thunderbird.  
Other Recommendation:  
• Backups - It cannot be stressed enough how important it is to make a backup of your Linux system. A proper offsite backup allows you to recover from cracked server i.e. an intrusion. The traditional UNIX backup programs are dump and restore are also recommended.  
• How to: Looking for Rootkits.  
• Howto: Enable ExecShield Buffer Overflows Protection.  
• Subscribe to Redhat or Debian Linux security mailing list or RSS feed.  
Recommend readings:  
1. Red Hat Enterprise Linux - Security Guide.  
2. Linux security cookbook- A good collections of security recipes for new Linux admin.  
3. Snort 2.1 Intrusion Detection, Second Edition - Good introduction to Snort and Intrusion detection under Linux.  
4. Hardening Linux - Hardening Linux identifies many of the risks of running Linux hosts and applications and provides practical examples and methods to minimize those risks.  
5. Linux Security HOWTO.  
In the next part of this series I will discuss how to secure specific applications (such as Proxy, Mail, LAMP, Database) and a few other security tools. Did I miss something? Please add your favorite system security tool or tip in the comments

**1) How to find all the links in a folder in UNIX or Linux ?**

This is a *tricky UNIX question* as there is no specific command to find all symbolic links. Though you have [ln command for creating and updating soft links](http://javarevisited.blogspot.sg/2011/04/symbolic-link-or-symlink-in-unix-linux.html) but nothing which gives you all the links in a directory. You need to use ls command which list everything in directory and then you need to list all the links, as they starts with "l" as first characters, as shown in above article .

here is the actual UNIX command to find all links in a directory :

linux@nyj872:~ ls -lrt

total 2.0K

-rw-r--r-- 1 Linux Domain Users 0 Dec 6 2011 a

drwxr-xr-x+ 1 Linux Domain Users 0 Sep 19 12:30 java/

lrwxrwxrwx 1 Linux Domain Users 4 Sep 19 12:31 version\_1.0 -> java/

linux@nyj872:~ ls -lrt | grep '^l'

lrwxrwxrwx 1 Linux Domain Users 4 Sep 19 12:31 version\_1.0 -> java/

**2) How to find a process and kill that ?**

Another classic UNIX interview questions. Answer of this question is simple if you are familiar with ps, grep and kill command. by using "ps -ef" you can get list of all process and then use grep to find your process and get the PID of that process. Once you got PID you can use kill command to kill that process as shown in this [example of kill command in UNIX](http://javarevisited.blogspot.sg/2011/12/kill-command-unix-linux-example.html).

**3) How to run a program in background in UNIX or Linux ?**

an easy UNIX or Linux interview question, only when you know. You can use &amp; to run any process in background and than you can use jobs to find the job id for that process and can use fg and bg command to bring that process into foreground and background.

**4) How to sort output of a command in reverse order in Linux or UNIX ?**

One more Linux command interview question which checks knowledge of frequently used command. you can use sort command in UNIX to sort output of any command by using PIPE. By using -r option with sort command you can sort output of any command in reverse order. See these [sort command examples](http://javarevisited.blogspot.sg/2011/08/unix-sort-command-example-tutorial.html) for more details.

**5) How to create archive file in UNIX or Linux Operating System ?**

Another interview question based on knowledge of UNIX or Linux command. you can use [tar command](http://www.blogger.com/javarevisited.blogspot.sg/2011/11/tar-command-in-unix-linux-example.html) to great archives in UNIX or Linux. you can even combine tar and gzip to create a compressed archive in UNIX.

**6) What is meaning of a file has 644 permission ?**

To answer this UNIX or Linux interview question, you must know basics of files and directories in UNIX. 644 represents permission 110 for owner, permission 100 for group and 100 for others which means read + write for owner who create that file and read only permission for group and others. See this [tutorial on UNIX file permission](http://javarevisited.blogspot.sg/2011/11/file-permissions-in-unix-linux-example.html) for more details.

**7) How will you remove empty files or directories from /tmp ?**

See [how to delete empty directory and files in UNIX](http://javarevisited.blogspot.sg/2012/08/delete-empty-files-directories-unix.html) to answer this UNIX command interview questions.

**8) I have read permission on a directory but I am not able to enter it why ?**

One more tricky UNIX questions. In order to get into a directory you need execute permission. if your directory does not have execute permission than you can not go into that directory by using cd command. read [UNIX files and directory permissions](http://javarevisited.blogspot.sg/2011/11/file-permissions-in-unix-linux-example.html) for more information.

**9) How do you find all files which are modified 10 minutes before ?**

This is another the Linux interview questions from frequently used command e.g. find and grep. you can use -mtime option of find command to list all the files which are modified 10 or m minutes before. see these [find command examples](http://javarevisited.blogspot.sg/2011/03/10-find-command-in-unix-examples-basic.html) for more details.

**10) How to do you find size of directory in UNIX or Linux ?**

This is another tricky and bit tough Linux interview question as popular ls command doesn't show complete size of directories in UNIX. you need to use du command to get full size of directories including all sub directories in UNIX. See [How to find directory size in UNIX](http://javarevisited.blogspot.sg/2012/08/delete-empty-files-directories-unix.html) for exact command and detailed explanation.

### Linux Interview Questions Along With Answers

**Q.1: What is the difference between UNIX and LINUX?**

The major difference from a common users point of view is that while Linux is an open source operating system, Unix is a proprietary system. Unix follows a lot of standards and at times the developers maybe restricted due to such standards. In case of Linux, although developers might not be restricted, freedom given to developers cause a lot of fragmentation in Linux distributions.

**Q.2: Who owns a data dictionary?**

The data dictionary is owned by the SYS user. The SYS and system users are created when the database is made.

**Q.3: What is a fork () system’s use?**

The fork () system is used to create a new process from a process which already exists. The new process is hence called a child process while the existing one is called parent process. One can judge and tell the return value from fork ().

**Q.4: What are the Linux system calls for an I/O?**

Here are some calls used for an I/O-

* open(pathname,flag,mode) – Used to open file
* creat(pathname,mode) – create file command
* close(filedes) – close an open file command
* write(filedes,buffer,bytes) – write data to an open file command
* read(filedes,buffer,bytes) – Lets you read data from an open file
* dup(filedes) – Command to duplicate an existing file descriptor

**Q.5: What is the difference between static and dynamic library?**

A collection of related objects grouped together is commonly referred to as a library. The difference between static and dynamic libraries is that the static libraries are loaded when the program is compiled and it is dynamically linked to the libraries which are loaded later in time.

**Q.6: What is an RPM?**

RPM is a Redhat package management system; it is a collection of tools to manage software packages. RPM is used to install, verify and erase individual software packages.

**Q.7: What are the Linux hotkeys you know?**

* Alt + F1 are used for application menu.
* Alt + F2 are used to open and run application window.
* Alt + F3 are used for finding anything.
* Alt + F4 are used to close application.
* Alt + F9 are used to minimize the window.
* Ctrl + L are used to clear screen.

**Q.8: How can one check which NFS version is one using?**

Here’s the command for the above question which gives you the version of the NFS,

**Rpcinfo –p localhost | grep –I nfs**

**Q.9: What are the system calls used for Process Management?**

Here are some system commands used for following actions-

* fork() To create a new process
* exit() To exit from a process execution
* wait() To wait until a created process completes its execution
* exec() To execute a new program in a process
* nice() To bias the existing priority of a process
* brk() To increase/decrease the data segment size of a process.

**Q.10: What is MX Record?**

MX Record stands for Mail eXchanger Record. You can find MX Record in [DNS](http://en.wikipedia.org/wiki/Domain_Name_System) which specifies how an email should be routed. It specifies the mail server responsible for handling emails as well as preference values when multiple mail servers are there.

**Q.11: How do you tackle the problem is Apache doesn’t work on startup?**

Run the following code to track the issue.  
chkconfig httpd on  
httpd -t  
service httpd on  
netstat -tulpn | grep 80  
tail -f /var/log/httpd/access\_log  
tail -f /var/log/httpd/error\_log

Linux System Admin Interview Questions & Answers part 3

1. Echo is used to Display message on screen. Which of the following options below should be used with echo to not output the trailing newline?

answer: -n

2. mount –r is used to mount a file in read only mode

answer: True

3. Which command is most useful when you want not only to send some data down a pipe, but also to save a copy?

Answer: tee

4. There is no difference between who and whoami command?

Correct answer: False

5. When trying to compare two files using cmp, if the files differ; what is the output?

answer: tells the first byte and line number where they differ

6. Cal is used to display calendar. If no arguments are supplied, what is displayed?

answer: The current month is displayed

7. Which of the following command is used to test a network connection?

answer: ping

8. Ping will only report damaged packets.

answer: False

9. Which of the following are valid functions of Red Hat Package Manager?

Answer: Used to verify software packages.search engine to search for software’s

10. What is the Non interactive mode of nslookup used for?

answer: Fetch information about the specified host or domain

11. Nettop is used to find network usage

Answer: True

12. In \_\_\_\_\_\_\_\_\_\_\_\_\_ state of a process, the process will be terminated and the information will still be available in the process table.

Answer: Zombie

13. Which system call is used to bias the existing property of process?

answer: bias()

14. LD\_LIBRARY\_PATH is a type of

answer: Environmental variable

15. What is the major difference between UNIX and LINUX?

answer: Linux is an open source and free software

16. What is the use of a pipe?

Answer: Several functions can be combined in a single statement.Stream input to output.

17. By default, the shell uses the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ library

answer: readline

18. The kernel cannot be updated.

answer: False

19. Which of the following below are types of shell?

answer: sh, shell

20. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_ file contains all the information of users on your system

Answer: /etc/passwd

21. Which directory is used to write messages when kernel is loading? answer: /var/log/messages

22. Which command is used to report on the status of the quotas that have set including the amount of allocated space and amount of used space?

answer: repquota -a

23. Linux Supports Virtualized File Systems Like RAID.

answer: T

**UNIX command Questions Answers asked in Interview**

**UNIX or Linux operating system** has become default Server operating system and for whichever programming job you give interview you find some UNIX command interview questions there. **These UNIX command interview questions** are mostly asked during Java development and Support role interviews on various investment banks mostly because most of **electronic trading systems** or stock trading system works on Unix servers. As we know that high volume low latency systems which wants to take advantage of little bit of volatility in market for Equity , Futures and options or Foreign exchange trading need a stable server side operating system and Redhat Linux is doing great job there. with the advent ofAlgorithmic trading this speed factor becomes more important so getting someone who has good knowledge of operating system and commands on which these trading system runs is definitely required. but these UNIX command interview questions are equally applicable for any job interview which requires some work on Unix Operating System. With the growing use of Linux in form of RedHat, Solaris and IBM AIX its must to keep you familiar with essential Linux commands available on various platforms.

[Unix and Linux Command Interview Questions and Answers](http://javarevisited.blogspot.com/2011/04/top-20-core-java-interview-questions.html)Long back I had once asked one of my friend why are you preparing Unix Command interview questions if you going for a Java Interview and he told me that this job doesn't only require knowledge of Java but also knowledge of Unix, Linux, SQL and other scripting language , which is quite true. After that I thought to collect various UNIX command interview questions asked to Java developers or trading system support interviews and this is the result of that compilation. This list of UNIX command interview questions are by means complete and would be great if you guys contribute some genuine and **good Unix Command Interview questions and answers** asked during interviews. I have divided the questions on three categories for sake of managing and keeping this list of Unix Interview questions up to date.

**Beginners UNIX Interview Questions Answers**

**1. Write command to list all the links from a directory?**

In this UNIX command interview questions interviewer is generally checking whether user knows basic use of "ls" "grep" and regular expression etc

You can write command like:

ls -lrt | grep "^l"

**2. Create a read-only file in your home directory?**

This is a simple UNIX command interview questions where you need to create a file and change its parameter to read-only by using chmod command you can also change your umask to create read only file.

touch file

chmod 400 file

read more about [**file and directory permission in unix and linux**](http://javarevisited.blogspot.com/2011/11/file-permissions-in-unix-linux-example.html) here.

**3. How will you find which operating system your system is running on in UNIX?**

By using command **"uname -a"** in UNIX

**4. How will you run a process in background? How will you bring that into foreground and how will you kill that process?**

For running a process in background use "&" in command line. For bringing it back in foreground use command "**fg jobid"** and for getting job id you use command "jobs", for killing that process find PID and use kill -9 PID command. This is indeed a good Unix Command interview questions because many of programmer not familiar with background process in UNIX.

**5. How do you know if a remote host is alive or not?**

You can check these by using either **ping** or **telnet** command in UNIX. This question is most asked in various Unix command Interview because its most basic networking test anybody wants to do it.

**6. How do you see command line history in UNIX?**

Very useful indeed, use history command along with[**grep command in unix**](http://javarevisited.blogspot.com/2011/06/10-examples-of-grep-command-in-unix-and.html)to find any relevant command you have already executed. Purpose of this Unix Command Interview Questions is probably to check how familiar candidate is from available tools in UNIX operation system.

**7. How do you copy file from one host to other?**

Many options but you can say by using "**scp**" command. You can also use **rsync** command to answer this UNIX interview question or even **sftp** would be ok.

**8. How do you find which process is taking how much CPU?**

By using "top" command in UNIX, there could be multiple follow-up UNIX command interview questions based upon response of this because “TOP” command has various interactive options to [sort](http://javarevisited.blogspot.com/2011/08/unix-sort-command-example-tutorial.html) result based upon various parameter.

**9. How do you check how much space left in current drive ?**

By using **"df"** command in UNIX. For example **"df -h ."** will list how full your current drive is. This is part of anyone day to day activity so I think this Unix Interview question will be to check anyone who claims to working in UNIX but not really working on it.

**10. What is the difference between Swapping and Paging?**

Swapping:

Whole process is moved from the swap device to the main memory for execution. Process size must be less than or equal to the available main memory. It is easier to implementation and overhead to the system. Swapping systems does not handle the memory more flexibly as compared to the paging systems.

Paging:

Only the required memory pages are moved to main memory from the swap device for execution. Process size does not matter. Gives the concept of the virtual memory. It provides greater flexibility in mapping the virtual address space into the physical memory of the machine. Allows more number of processes to fit in the main memory simultaneously. Allows the greater process size than the available physical memory. Demand paging systems handle the memory more flexibly.

**Intermediate UNIX Interview Questions Answers**

**1. What is difference between ps -ef and ps -auxwww?**

[](http://javarevisited.blogspot.com/2011/03/10-find-command-in-unix-examples-basic.html)This is indeed a good Unix Interview Command Question and I have faced this issue while ago where one culprit process was not visible by execute **ps –ef** command and we are wondering which process is holding the file.

ps -ef will omit process with very long command line while ps -auxwww will list those process as well.

**2. How do you find how many cpu are in your system and there details?**

By looking into file /etc/cpuinfo for example you can use below command:

**cat /proc/cpuinfo**

**3. What is difference between HardLink and SoftLink in UNIX?**

I have discussed this Unix Command Interview questions  in my blog post [difference between Soft link and Hard link in Unix](http://javarevisited.blogspot.com/2011/04/symbolic-link-or-symlink-in-unix-linux.html)

**4. What is Zombie process in UNIX? How do you find Zombie process in UNIX?**

When a program forks and the child finishes before the parent, the kernel still keeps some of its information about the child in case the parent might need it - for example, the parent may need to check the child's exit status. To be able to get this information, the parent calls 'wait()'; In the interval between the child terminating and the parent calling 'wait()', the child is said to be a 'zombie' (If you do 'ps', the child will have a 'Z' in its status field to indicate this.)

**Zombie : The process is dead but have not been removed from the process table.**

**5. What is "chmod" command? What do you understand by this line “r-- -w- --x?**

**6. There is a file some where in your system which contains word "UnixCommandInterviewQuestions” How will find that file in Unix?**

By using find command in UNIX for details see here [10 example of using find command in Unix](http://javarevisited.blogspot.com/2011/03/10-find-command-in-unix-examples-basic.html)

**7. In a file word UNIX is appearing many times? How will you count number?**

grep -c "Unix" filename

**8. How do you set environment variable which will be accessible form sub shell?**

By using **export**   for example export count=1 will be available on all sub shell.

**9. How do you check if a particular process is listening on a particular port on remote host?**

By using telnet command for example “telnet hostname port”, if it able to successfully connect then some process is listening on that port. To read more about telnet read [networking command in UNIX](http://javarevisited.blogspot.com/2010/10/basic-networking-commands-in-linuxunix.html)

**10. How do you find whether your system is 32 bit or 64 bit ?**

Either by using **"uname -a"** command or by using "**arch**" command.

**Advanced UNIX Interview Questions and Answers**

**1. How do you find which processes are using a particular file?**

By using **lsof** **command** in UNIX. It wills list down PID of all the process which is using a particular file.

**2. How do you find which remote hosts are connecting to your host on a particular port say 10123?**

By using **netstat command** execute netstat -a | grep "port" and it will list the entire host which is connected to this host on port 10123.

**3. What is nohup in UNIX?**

**4. What is ephemeral port in UNIX?**

Ephemeral ports are port used by Operating system for client sockets. There is a specific range on which OS can open any port specified by ephemeral port range.

**5. If one process is inserting data into your MySQL database? How will you check how many rows inserted into every second?**

Purpose of this Unix Command Interview is asking about **"watch" command** in UNIX which is repeatedly execute command provided with specified delay.

**6. There is a file Unix\_Test.txt which contains words Unix, how will you replace all Unix to UNIX?**

You can answer this Unix Command Interview question by using SED command in UNIX for example you can execute **sed s/Unix/UNIX/g fileName.**

**7. You have a tab separated file which contains Name, Address and Phone Number, list down all Phone Number without there name and Addresses?**

To answer this Unix Command Interview question you can either you AWK or CUT command here. CUT use tab as default separator so you can use

**cut -f3 filename.**

**8. Your application home directory is full? How will you find which directory is taking how much space?**

By using disk usage (DU) command in Unix for example du **–sh . | grep G**  will list down all the directory which has GIGS in Size.

**9. How do you find for how many days your Server is up?**

By using **uptime** command in UNIX

**10. You have an IP address in your network how will you find hostname and vice versa?**

This is a standard UNIX command interview question asked by everybody and I guess everybody knows its answer as well. By using **nslookup** command in UNIX, you can read more about [**Convert IP Address to hostname in Unix**](http://javarevisited.blogspot.com/2011/09/find-hostname-from-ip-address-to.html) here.

I hope this ***UNIX command interview questions and answers*** would be useful for quick glance before going for any UNIX or Java job interview. Please share any interesting UNIX command interview you have come across and I will add into this list. If you are going for any Unix interview on brokerage firm or stock trading company or any Investment bank you can have a quick look here, though most of questions you might already know but its good to review it. if you like this you can see my other [unix command tutorial for beginners](http://javarevisited.blogspot.com/2011/04/unix-commands-tutorial-and-tips-for.html) as well 

# [10 Examples of tar command in UNIX and Linux](http://javarevisited.blogspot.in/2011/11/tar-command-in-unix-linux-example.html)

tar command in UNIX or Linux is one of the important command which provides archiving functionality in unix. we can use UNIX tar command to create compressed or uncompressed archive files by using either gzip or bzip2. In this **unix tar command tutorial** we will see examples of unix tar command related to basic archiving task e.g. **How to create tar archive in Unix and Linux**, How to extract files from tar archive in unix, How to view contents of tar file in Unix and Linux or how to update and existing tar file in Unix. Examples of tar command in unix are kept simple and easy to understand and master each of basic task using **unix tar command**.

I thought about this article when I written [how to be productive in UNIX](http://javarevisited.blogspot.com/2011/03/unix-command-tutorial-working-fast-in.html) and [UNIX command tutorial and Example for beginners](http://javarevisited.blogspot.com/2011/04/unix-commands-tutorial-and-tips-for.html) but somehow it gets delayed and now I am happy to see this published.

Ok enough introduction now let's see some *real life examples of tar command in Unix and Linux*:

[](http://javarevisited.blogspot.com/2011/06/vi-editor-in-unix-example-tutorial-and.html)

**How to use tar command in Unix**

Using tar command in UNIX is simple and it has similar syntax like any other UNIX command. below is the syntax of tar command in UNIX:

tar  [options] [name of tar file to be created] [list of files and directories to be included]

This **syntax of tar command** is for easy understanding you can also check detailed syntax by using command "tar --usage" in unix machine.

**tar command examples in Linux**

**Unix tar command line options**

---------------------------------------

In this section of UNIX tar command tutorial we will see some useful options of tar command in Linux and we will use this options on our example to understand usage of this option along-with tar command.

c -- create, for creating tar file

v -- verbose, display name of files including,excluding from tar command

f -- following, used to point name of tar file to be created. it actually tells tar command that name of the file is "next" letter just after options.

x -- extract, for extracting files from tar file.

t -- for viewing content of tar file

z -- zip, tells tar command that create tar file using gzip.

j –- another compressing option tells tar command to use bzip2 for compression

r -- update or add file or directory in already existed .tar file

wildcards -- to specify patters in unix tar command

**How to create tar archive or tar file in Unix**

-------------------------------------------------------

Most of use use either winzip or winrar in windows machine to zipping or creating archives of content so when we move to command line interface like Unix or Linux we struggle without those tools. UNIX tar command is similar to winzip or winrar and you can use UNIX tar command to create both compressed or uncompressed (zipped) archives in UNIX.

In this example of tar command we will create tar file including all the files and directories or selected files and directories in Unix.

here is our directory

stock\_trader@system:~/test **ls -lrt**

total 0

-r--r--r--  1 stock\_trader Domain Users 0 Jul 15 11:42 equity

drwxrwxrwx+ 1 stock\_trader Domain Users 0 Jul 15 14:33 stocks/

-r--r--r--  1 stock\_trader Domain Users 0 Jul 15 15:30 currency

it has two files and one directory. now we will create a tar file with all these contents.

stock\_trader@system:~/test **tar -cvf trading.tar \***

currency

equity

stocks/

stocks/online\_stock\_exchanges.txt

You see unix tar command is creating tar file with name "**trading**" with contents shown above. just to review here "-c" is used to create tar file "v" is used to be verbose and "f" is used to tell tar file name. You can see the tar file here

stock\_trader@system:~/test **ls -lrt**

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 11:42 equity

drwxrwxrwx+ 1 stock\_trader Domain Users   0 Jul 15 14:33 stocks/

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 15:30 currency

-rw-r--r--  1 stock\_trader Domain Users 10K Jul 18 12:29 trading.tar

**How to view contents of tar file in Unix or Linux**

-------------------------------------------------------------

In earlier example of tar command in Unix or Linux we have created a uncompressed tar file called "trading.tar" now in this example we will see the actual content of that tar file.

stock\_trader@system:~/test **tar -tvf trading.tar**

-r--r--r-- stock\_trader/Domain Users 0 2011-07-15 15:30 currency

-r--r--r-- stock\_trader/Domain Users 0 2011-07-15 11:42 equity

drwxrwxrwx stock\_trader/Domain Users 0 2011-07-15 14:33 stocks/

-rwxrwxrwx stock\_trader/Domain Users 0 2011-07-15 14:33 stocks/online\_stock\_exchanges.txt

here option "t" is used to display content of tar file in unix while options "v" and "f" are for "verbose" and "following". now you can clearly see that all the files which we wanted to be included in tar file are there.

**How to extract contents from a tar file in Unix**

-----------------------------------------------------------

In this example of unix tar command we will see how to extract files or directories from a tar file in unix or Linux. We will use same trading.tar file created in earlier example. In this example we will create a directory "trading" and extract contents of trading.tar on that directory.

stock\_trader@system:~/test/new **ls -lrt**

total 12K

-rw-r--r-- 1 stock\_trader Domain Users 10K Jul 18 12:37 trading.tar

Now the directory is empty just trading.tar file

stock\_trader@system:~/test/new **tar -xvf trading.tar**

currency

equity

stocks/

stocks/online\_stock\_exchanges.txt

This unix tar command will extract content of trading.tar in current directory. "x" is used for extracting. "v" is again for verbose and optional parameter in all our example.

stock\_trader@system:~/test/new **ls -lrt**

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 11:42 equity

drwxr-xr-x+ 1 stock\_trader Domain Users   0 Jul 15 14:33 stocks/

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 15:30 currency

-rw-r--r--  1 stock\_trader Domain Users 10K Jul 18 12:37 trading.tar

Now you can see that all the files and directories which were included in tar file (stocks, equity and currency) has been extracted successfully.

**How to create tar file in Unix with just specified contents**

-------------------------------------------------------------------------

In above example of tar command in unix we have created tar file with all the contents available in current directory but we can also create tar file with selective content as shown in above example.

Now in our current directory we have both files and directories and we just want to include two files equity and currency in our tar file.

stock\_trader@system:~/test **ls -lrt**

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 11:42 equity

drwxrwxrwx+ 1 stock\_trader Domain Users   0 Jul 15 14:33 stocks/

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 15:30 currency

-rw-r--r--  1 stock\_trader Domain Users 10K Jul 18 12:29 trading.tar

drwxr-xr-x+ 1 stock\_trader Domain Users   0 Jul 18 12:46 new/

stock\_trader@system:~/test **tar -cvf equitytrading.tar equity currency**

equity

currency

you see only two files equity and currency are included in our tar file.

**How to create compressed tar file using gzip in Unix**

------------------------------------------------------------------

In our previous example of Linux tar command we have created uncompressed tar file but most of the time we also need to create compressed tar file using gzip or bzip2. In this example of tar command in Linux we will learn about creating tar file using gzip.

stock\_trader@system:~/test **tar -zcvf trading.tgz \***

currency

equity

stocks/

stocks/online\_stock\_exchanges.txt

you see creating tar file with gzip is very easy just use "-z" option and it will crate a gzip tar. .tgz or tar.gz extension is used to denote tar file with gzip. size of a compressed tar file is far less than uncompressed one.

stock\_trader@system:~/test **ls -lrt**

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 11:42 equity

drwxrwxrwx+ 1 stock\_trader Domain Users   0 Jul 15 14:33 stocks/

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 15:30 currency

-rw-r--r--  1 stock\_trader Domain Users 219 Jul 18 13:01 trading.tgz

you can also view contents of gzip tar file by using earlier command in combination of "z" option and same is true for extracting content from gzip tar. below examples of unix tar command will show how to view contents of .tgz or .tar.gz file in unix.

stock\_trader@system:~/test **tar -ztvf trading.tgz**

-r--r--r-- stock\_trader/Domain Users 0 2011-07-15 15:30 currency

-r--r--r-- stock\_trader/Domain Users 0 2011-07-15 11:42 equity

drwxrwxrwx stock\_trader/Domain Users 0 2011-07-15 14:33 stocks/

-rwxrwxrwx stock\_trader/Domain Users 0 2011-07-15 14:33 stocks/online\_stock\_exchanges.txt

Similarly we can extract contents from a **.tgz or .tar.gz file** as shown in below example of unix tar command :

stock\_trader@system:~/test/new **tar -zxvf trading.tgz**

currency

equity

stocks/

stocks/online\_stock\_exchanges.txt

stock\_trader@system:~/test/new ls -lrt

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 11:42 equity

drwxr-xr-x+ 1 stock\_trader Domain Users   0 Jul 15 14:33 stocks/

-r--r--r--  1 stock\_trader Domain Users   0 Jul 15 15:30 currency

-rw-r--r--  1 stock\_trader Domain Users 219 Jul 18 13:07 trading.tgz

**How to create compressed tar file using bzip2 in Unix**

--------------------------------------------------------------------

bzip2 is another compression option we have which we can use with unix tar command. its exactly similar with our earlier option of compressing using gzip but instead of "z" option we need to use "j" tar option to create bzip2 file as shown in below example of tar command in unix.

stock\_trader@system:~/test **tar -jcvf trading.tar.bz2** \*

currency

equity

stocks/

stocks/online\_stock\_exchanges.txt

stock\_trader@system:~/test **ls -lrt trading.tar.bz2**

-rw-r--r--  1 stock\_trader Domain Users 593 Jul 18 13:11 trading.tar.bz2

.tar.bz2 is used to denote a tar file with bzip2 compression. for viewing contents of bzip2 tar file and extracting content we can use as shown in ***example of UNIX tar command*** with gzip compression, just replace "-z" with "-j" for bzip2.

**How to extract a particular file form .tar, .tar.gz or .tar.bzip2**

----------------------------------------------------------------------------

In previous examples of extracting contetns from tar file we have extracted everything. sometime we just need a specific file from tar file. in this example of unix tar command we will extract a particular file from a tar archive.

stock\_trader@system:~/test/new **tar -jxvf trading.tar.bz2 equity**

equity

its simple just specify name of file in this case its "equity". if your tar file is gzip one then use "-z" that's it. You can also use combination of [grep](http://javarevisited.blogspot.com/2011/06/10-examples-of-grep-command-in-unix-and.html) and [find command](http://javarevisited.blogspot.com/2011/03/10-find-command-in-unix-examples-basic.html) with tar to get more dynamic use.

**How to extract group of file or directory from form .tar, .tar.gz or .tar.bzip2 in UNIX**

**---------------------------------------------------------------------------------------------------**

you can extract a group of file form .tar, .tar.gz or .tar.bzip2 in Unix by specifying a matching pattern and using option "--wildcards". let's an example of tar command in unix with --wildcards

stock\_trader@system:~/test/new **tar -jxvf trading.tar.bz2 --wildcards "s\*"**

stocks/

stocks/online\_stock\_exchanges.txt

In above example of UNIX tar command we are extracting all files or directory which names starts with "s".

**How to update existing tar file in Linux**

**----------------------------------------------**

You can also update or append new files in already created tar file. option"-r" is used for that. Let’s see an example of updatating tar file using tar command in UNIX:

stock\_trader@system:~/test **tar -cvf sample.tar equity currency**

equity

currency

stock\_trader@system:~/test **tar -rvf sample.tar gold**

gold

stock\_trader@system:~/test tar -tvf sample.tar

-r--r--r-- stock\_trader/Domain Users 0 2011-07-15 11:42 equity

-r--r--r-- stock\_trader/Domain Users 221 2011-07-18 13:10 currency

-rw-r--r-- stock\_trader/Domain Users   0 2011-07-18 13:30 gold

Apparently can not update compressed archives.if you try to do you will get error **"tar: Cannot update compressed archives"**

**Calculating size of tar file in UNIX**

-------------------------------------------

Some time its useful to know the size of tar file before creating it and you can get it by using unix tar command as shown in below example:

stock\_trader@system:~/test **tar -cf - \* | wc -c**

20480

Size shown here is in KB and you can also calculate size for compressed tar file by using "z" for gzip and "j" for bzip2

-----------------------------------------------------------------------------

**what is the command which lets you change your password?**

**passwd**

**Posted in** [Unix commands](http://unixlinuxtesting.h2kinfosys.com/category/unix-commands/)-**Tagged** [change](http://unixlinuxtesting.h2kinfosys.com/tag/change/), [os](http://unixlinuxtesting.h2kinfosys.com/tag/os/), [passwd](http://unixlinuxtesting.h2kinfosys.com/tag/passwd/), [unix](http://unixlinuxtesting.h2kinfosys.com/tag/unix/)

# [Unix interview questions part-4](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-4/)

[Aug02  
**2011**](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-4/)[Leave a Comment](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-4/#respond)http://1.gravatar.com/avatar/10606c13a67f297fac63659e0557ca60?s=30&d=http%3A%2F%2F1.gravatar.com%2Favatar%2Fad516503a11cd5ca435acc9bb6523536%3Fs%3D30&r=G Written by [**admin**](http://unixlinuxtesting.h2kinfosys.com/author/admin/)

1.Write a command to display a file’s contents in various formats?  
$od -cbd file\_name c – character, b – binary (octal), d-decimal, od=Octal Dump.

2. What will the following command do?  
$ echo \*

It is similar to ‘ls’ command and displays all the files in the current directory.  
3. Is it possible to create new a file system in UNIX?  
Yes, ‘mkfs’ is used to create a new file system.

4. Is it possible to restrict incoming message?  
Yes, using the ‘mesg’ command.

5.. What is the use of the command “ls -x chapter[1-5]”

ls stands for list; so it displays the list of the files that starts with ‘chapter’ with suffix ’1′ to ’5′, chapter1,  
chapter2, and so on.

6. Is ‘du’ a command? If so, what is its use?  
Yes, it stands for ‘disk usage’. With the help of this command you can find the disk capacity and free space  
of the disk.

7. Is it possible to count number char, line in a file; if so, How?  
Yes, wc-stands for word count.  
wc -c for counting number of characters in a file.  
wc -l for counting lines in a file.

8. Name the data structure used to maintain file identification?

‘inode’, each file has a separate inode and a unique inode number.

9. How many prompts are available in a UNIX system?

Two prompts, PS1 (Primary Prompt), PS2 (Secondary Prompt).  
10. How does the kernel differentiate device files and ordinary files?

Kernel checks ‘type’ field in the file’s inode structure.

11. How to switch to a super user status to gain privileges?  
Use ‘su’ command. The system asks for password and when valid entry is made the user gains super user  
(admin) privileges.  
12. What are shell variables?  
Shell variables are special variables, a name-value pair created and maintained by the shell.  
Example: PATH, HOME, MAIL and TERM  
13. What is redirection?  
Directing the flow of data to the file or from the file for input or output.  
Example : ls > wc  
14. How to terminate a process which is running and the specialty on command kill 0?  
With the help of kill command we can terminate the process.  
Syntax: kill pid  
Kill 0 – kills all processes in your system except the login shell.  
15. What is a pipe and give an example?  
A pipe is two or more commands separated by pipe char ‘|’. That tells the shell to arrange for the output of  
the preceding command to be passed as input to the following command.  
Example : ls -l | pr  
The output for a command ls is the standard input of pr.  
When a sequence of commands are combined using pipe, then it is called pipeline.  
16. Explain kill() and its possible return values.  
There are four possible results from this call:  
‘kill()’ returns 0. This implies that a process exists with the given PID, and the system would allow you to  
send signals to it. It is system-dependent whether the process could be a zombie.  
‘kill()’ returns -1, ‘errno == ESRCH’ either no process exists with the given PID, or security enhancements  
are causing the system to deny its existence. (On some systems, the process could be a zombie.)  
‘kill()’ returns -1, ‘errno == EPERM’ the system would not allow you to kill the specified process. This means  
that either the process exists (again, it could be a zombie) or draconian security enhancements are present  
(e.g. your process is not allowed to send signals to \*anybody\*).  
‘kill()’ returns -1, with some other value of ‘errno’ you are in trouble! The most-used technique is to assume  
that success or failure with ‘EPERM’ implies that the process exists, and any other error implies that it  
doesn’t.  
An alternative exists, if you are writing specifically for a system (or all those systems) that provide a ‘/proc’  
filesystem: checking for the existence of ‘/proc/PID’ may wWhat is relative path and absolute path.  
Absolute path : Exact path from root directory.  
Relative path : Relative to the current path may work.

**Posted in** [Unix interview questions](http://unixlinuxtesting.h2kinfosys.com/category/unix-interview-questions/)-**Tagged** [commands](http://unixlinuxtesting.h2kinfosys.com/tag/commands/), [kernel differentiate device files](http://unixlinuxtesting.h2kinfosys.com/tag/kernel-differentiate-device-files/), [ordinary files](http://unixlinuxtesting.h2kinfosys.com/tag/ordinary-files/), [shell varaibles](http://unixlinuxtesting.h2kinfosys.com/tag/shell-varaibles/), [unix](http://unixlinuxtesting.h2kinfosys.com/tag/unix/)

# [Unix interview questions part-3](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-3/)

[Aug02  
**2011**](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-3/)[Leave a Comment](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-3/#respond)http://1.gravatar.com/avatar/10606c13a67f297fac63659e0557ca60?s=30&d=http%3A%2F%2F1.gravatar.com%2Favatar%2Fad516503a11cd5ca435acc9bb6523536%3Fs%3D30&r=G Written by [**admin**](http://unixlinuxtesting.h2kinfosys.com/author/admin/)

**1. How do you find which processes are using a particular file?**

By using **lsof** **command** in UNIX. It will list down PID of all the process which is using a particular file.

**2. How do you find which remote hosts are connecting to your host on a particular port say 10123?**

By using **netstat command** execute netstat -a | grep “port” and it will list the entire host which is connected to this host on port 10123.

**4. What is ephemeral port in UNIX?**

Ephemeral ports are port used by Operating system for client sockets. There is a specific range on which OS can open any port specified by ephemeral port range.

**5. If one process is inserting data into your MySQL database? How will you check how many rows inserted into every second?**

**“watch” command** in UNIX is repeatedly used to execute command provided with specified delay.

**6. There is a file Unix\_Test.txt which contains words Unix, how will you replace all Unix to UNIX?**

by using SED command in UNIX for example you can execute **sed s/Unix/UNIX/g fileName.**

**7. You have a tab separated file which contains Name, Address and Phone Number, list down all Phone Number without there name and Addresses?**

you can either use AWK or CUT command here.

**8. Your application home directory is full? How will you find which directory is taking how much space?**

By using disk usage  
(DU) command in Unix for example du **–sh . | grep G** will list down all  
the directory which has GIGS in Size.

**9. How do you find for how many days your Server is up?**

By using **uptime** command in UNIX

**10. You have an IP address in your network how will you find hostname and vice  
versa?**

By using  
**nslookup** command in UNIX, you can read more about networking command in UNIX here.

**Posted in** [Unix interview questions](http://unixlinuxtesting.h2kinfosys.com/category/unix-interview-questions/)-**Tagged** [commands](http://unixlinuxtesting.h2kinfosys.com/tag/commands/), [ephemeral port](http://unixlinuxtesting.h2kinfosys.com/tag/ephemeral-port/), [unix](http://unixlinuxtesting.h2kinfosys.com/tag/unix/)

# [Unix interview questions part-2](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-2/)

[Aug02  
**2011**](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-2/)[Leave a Comment](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-2/#respond)http://1.gravatar.com/avatar/10606c13a67f297fac63659e0557ca60?s=30&d=http%3A%2F%2F1.gravatar.com%2Favatar%2Fad516503a11cd5ca435acc9bb6523536%3Fs%3D30&r=G Written by [**admin**](http://unixlinuxtesting.h2kinfosys.com/author/admin/)

1.What is difference between ps -ef and ps -auxwww?

ps -ef will omit  
process with very long command line while ps -auxwww will list those process as  
well.

**2. How do you find how many cpu are in your system and there details?**

By looking into file  
/etc/cpuinfo for example you can use below command:

**cat /proc/cpuinfo**

**3. What is difference between HardLink and SoftLink in UNIX?**

Unix Soft links are pointers to programs, files, or directories located  
elsewhere (just like Windows shortcuts).

Unix Hard links are pointers to programs and files, but NOT directories

**4. What is Zombie process in UNIX? How do you find Zombie process in UNIX?**

When a program forks and the child finishes before the parent, the kernel still keeps some of its information about the child in case the parent might need it -

**7. In a file word UNIX is appearing many times? How will you count number?**

grep -c “Unix” filename

**8. How do you set environment variable which will be accessible form sub shell?**

By using **export** for example export count=1 will be available on all sub  
shell.

**9. How do you check if a particular process is listening on a particular port on remote host?**

By using telnet command for example “telnet hostname port”, if it suceesfully connects then some process is listening on that port.

**10. How do you find whether your system is 32 bit or 64 bit ?**

Either by using  
**“uname -a”** command or by using “**arch**” command.

**Posted in** [Unix interview questions](http://unixlinuxtesting.h2kinfosys.com/category/unix-interview-questions/)-**Tagged** [arch command](http://unixlinuxtesting.h2kinfosys.com/tag/arch-command/), [commands](http://unixlinuxtesting.h2kinfosys.com/tag/commands/), [faq](http://unixlinuxtesting.h2kinfosys.com/tag/faq/), [grep-c](http://unixlinuxtesting.h2kinfosys.com/tag/grep-c/), [hardlink](http://unixlinuxtesting.h2kinfosys.com/tag/hardlink/), [interview questions](http://unixlinuxtesting.h2kinfosys.com/tag/interview-questions/), [ps-ef](http://unixlinuxtesting.h2kinfosys.com/tag/ps-ef/), [remote host](http://unixlinuxtesting.h2kinfosys.com/tag/remote-host/), [softlink](http://unixlinuxtesting.h2kinfosys.com/tag/softlink/), [subsehell](http://unixlinuxtesting.h2kinfosys.com/tag/subsehell/), [unix](http://unixlinuxtesting.h2kinfosys.com/tag/unix/), [zombie process](http://unixlinuxtesting.h2kinfosys.com/tag/zombie-process/)

# [Unix interview questions part-1](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-1/)

[Aug02  
**2011**](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-1/)[Leave a Comment](http://unixlinuxtesting.h2kinfosys.com/unix-interview-questions/unix-interview-questions-part-1/#respond)http://1.gravatar.com/avatar/10606c13a67f297fac63659e0557ca60?s=30&d=http%3A%2F%2F1.gravatar.com%2Favatar%2Fad516503a11cd5ca435acc9bb6523536%3Fs%3D30&r=G Written by [**admin**](http://unixlinuxtesting.h2kinfosys.com/author/admin/)

**1. Write command to list all the links from a directory?**

ls -lrt | grep  
“^l”

**2. Create a read-only file in your home directory?**

chmod command you can also change your umask to  
create read only file.

touch  
file

chmod 400  
file

**3. How will you find which operating system your system is running  
on in UNIX?**

By using command  
**“uname -a”** in UNIX

**4. How will you run a process in background? How will you bring that into foreground and how will you kill that process?**

For running a process in background use “&” in command line. For bringing it back in foreground use command “**fg jobid”** and for getting job id you use command “jobs”, for killing that process find PID and use kill -9 PID command.

**5. How do you know if a remote host is alive or not?**

by using either **ping** or **telnet** command in UNIX.

**6. How do you see command line history in UNIX?**

use history command along with grep to find any relevant command you have already executed.

**7. How do you copy file from one host to other?**

Many options but you can say by using “**scp**” command.

**8. How do you find which process is taking how much CPU?**

By using “top” command in UNIX.

**9. How do you check how much space left in current drive ?**

By using **“df”**  
command in UNIX. For example **“df -h .”** will list how full your current  
drive is.

**10. What is the difference between Swapping and Paging?**

Swapping:

Whole process is moved from the swap device to the main memory for execution. Process size must be less than or equal to the available main memory. It is easier to implementation and overhead to the system. Swapping systems does not handle the memory more flexibly as compared to the paging systems.

Paging:

Only the required memory pages are moved to main memory from the swap device for execution. Process size does not matter. Gives the concept of the virtual memory. It provides greater flexibility in mapping the virtual address space into the physical memory of the machine. Allows more number of processes to fit in the main memory simultaneously. Allows the greater process size than the available physical memory.

# **Linux Interview Questions and Answers**

There are seven fields in the /etc/passwd file. Which of the following lists all the fields in the correct order?  **Choose one:  
a. username, UID, GID, home directory, command, comment  
b. username, UID, GID, comment, home directory, command  
c. UID, username, GID, home directory, comment, command  
d. username, UID, group name, GID, home directory, comment**Answer: b   
The seven fields required for each line in the /etc/passwd file are username, UID, GID, comment, home directory, command. Each of these fields must be separated by a colon even if they are empty.

Which of the following commands will show a list of the files in your home directory including hidden files and the contents of all subdirectories? **Choose one:  
a. ls -c home  
b. ls -aR /home/username  
c. ls -aF /home/username  
d. ls -l /home/username**  
  
Answer: b   
The ls command is used to display a listing of files. The -a option will cause hidden files to be displayed as well. The -R option causes ls to recurse down the directory tree. All of this starts at your home directory.

In order to prevent a user from logging in, you can add a(n) **\_\_\_\_\_\_\_\_**at the beginning of the password field.   
Answer: asterick   
  
If you add an asterick at the beginning of the password field in the /etc/passwd file, that user will not be able to log in.

You have a directory called /home/ben/memos and want to move it to /home/bob/memos so you issue the command mv /home/ben/memos /home/bob. What is the results of this action? **Choose one:  
a. The files contained in /home/ben/memos are moved to the directory /home/bob/memos/memos.  
b. The files contained in /home/ben/memos are moved to the directory /home/bob/memos.  
c. The files contained in /home/ben/memos are moved to the directory /home/bob/.  
d. The command fails since a directory called memos already exists in the target directory.**   
  
Answer: a   
When using the mv command to move a directory, if a directory of the same name exists then a subdirectory is created for the files to be moved.

Which of the following tasks is not necessary when creating a new user by editing the /etc/passwd file?  **Choose one:  
a. Create a link from the user's home directory to the shell the user will use.  
b. Create the user's home directory  
c. Use the passwd command to assign a password to the account.  
d. Add the user to the specified group.**  
  
Answer: a   
There is no need to link the user's home directory to the shell command. Rather, the specified shell must be present on your system.

You issue the following command useradd -m bobm But the user cannot logon. What is the problem? **Choose one:  
a. You need to assign a password to bobm's account using the passwd command.  
b. You need to create bobm's home directory and set the appropriate permissions.  
c. You need to edit the /etc/passwd file and assign a shell for bobm's account.  
d. The username must be at least five characters long.**  
  
Answer: a   
The useradd command does not assign a password to newly created accounts. You will still need to use the passwd command to assign a password.

You wish to print the file vacations with 60 lines to a page. Which of the following commands will accomplish this? Choose one: **a. pr -l60 vacations | lpr  
b. pr -f vacations | lpr  
c. pr -m vacations | lpr  
d. pr -l vacations | lpr**  
  
Answer: a   
The default page length when using pr is 66 lines. The -l option is used to specify a different length.

Which file defines all users on your system?  **Choose one:  
a. /etc/passwd  
b. /etc/users  
c. /etc/password  
d. /etc/user.conf**  
  
Answer: a   
The /etc/passwd file contains all the information on users who may log into your system. If a user account is not contained in this file, then the user cannot log in.

Which two commands can you use to delete directories?  **A) rm  
B) rm -rf  
C) rmdir  
D) rd  
E) rd -rf**  
  
Answer(s): B, C - You can use rmdir or rm -rf to delete a directory. Answer a is incorrect, because the rm command without any specific flags will not delete a directory, it will only delete files. Answers d and e point to a non-existent command.

Which partitioning tool is available in all distributions?  **A) Disk Druid  
B) fdisk  
C) Partition Magic  
D) FAT32  
E) System Commander**  
  
Answer(s): B - The fdisk partitioning tool is available in all Linux distributions. Answers a, c, and e all handle partitioning, but do not come with all distributions. Disk Druid is made by Red Hat and used in its distribution along with some derivatives. Partition Magic and System Commander are tools made by third-party companies. Answer d is not a tool, but a file system type. Specifically, FAT32 is the file system type used in Windows 98.

Which partitions might you create on the mail server's hard drive(s) other than the root, swap, and boot partitions?  **[Choose all correct answers]  
A) /var/spool  
B) /tmp  
C) /proc  
D) /bin  
E) /home**  
Answer(s): A, B, E - Separating /var/spool onto its own partition helps to ensure that if something goes wrong with the mail server or spool, the output cannot overrun the file system. Putting /tmp on its own partition prevents either software or user items in the /tmp directory from overrunning the file system. Placing /home off on its own is mostly useful for system re-installs or upgrades, allowing you to not have to wipe the /home hierarchy along with other areas. Answers c and d are not possible, as the /proc portion of the file system is virtual-held in RAM-not placed on the hard drives, and the /bin hierarchy is necessary for basic system functionality and, therefore, not one that you can place on a different partition.

When planning your backup strategy you need to consider how often you will perform a backup, how much time the backup takes and what media you will use. What other factor must you consider when planning your backup strategy? **\_\_\_\_\_\_\_\_\_**   
  
what to backup   
Choosing which files to backup is the first step in planning your backup strategy.

**What utility can you use to automate rotation of logs?**   
Answer: logrotate   
The logrotate command can be used to automate the rotation of various logs.

In order to display the last five commands you have entered using the history command, you would type **\_\_\_\_\_\_\_\_\_\_\_** .  
  
Answer: history 5   
The history command displays the commands you have previously entered. By passing it an argument of 5, only the last five commands will be displayed.

**What command can you use to review boot messages?**   
Answer: dmesg   
The dmesg command displays the system messages contained in the kernel ring buffer. By using this command immediately after booting your computer, you will see the boot messages.

**What is the minimum number of partitions you need to install Linux?**   
Answer: 2   
Linux can be installed on two partitions, one as / which will contain all files and a swap partition.

**What is the name and path of the main system log?**   
Answer: /var/log/messages   
By default, the main system log is /var/log/messages.

# **Linux Interview Questions and Answers**

What key combination can you press to suspend a running job and place it in the background?ctrl-z   
  
Using ctrl-z will suspend a job and put it in the background.

The easiest, most basic form of backing up a file is to **\_\_\_\_\_** it to another location.  
copy   
  
The easiest most basic form of backing up a file is to make a copy of that file to another location such as a floppy disk.

What type of server is used to remotely assign IP addresses to machines during the installation process?  **A) SMB  
B) NFS  
C) DHCP  
D) FT  
E) HTTP**  
  
C - You can use a DHCP server to assign IP addresses to individual machines during the installation process. Answers a, b, d, and e list legitimate Linux servers, but these servers do not provide IP addresses. The SMB, or Samba, tool is used for file and print sharing across multi-OS networks. An NFS server is for file sharing across Linux net-works. FTP is a file storage server that allows people to browse and retrieve information by logging in to it, and HTTP is for the Web.

Which password package should you install to ensure that the central password file couldn't be stolen easily?  **A) PAM  
B) tcp\_wrappers  
C) shadow  
D) securepass  
E) ssh**  
  
C - The shadow password package moves the central password file to a more secure location. Answers a, b, and e all point to valid packages, but none of these places the password file in a more secure location. Answer d points to an invalid package.

When using useradd to create a new user account, which of the following tasks is not done automatically. **Choose one:  
a. Assign a UID.  
b. Assign a default shell.  
c. Create the user's home directory.  
d. Define the user's home directory.**  
  
c   
  
The useradd command will use the system default for the user's home directory. The home directory is not created, however, unless you use the -m option.

You want to enter a series of commands from the command-line. What would be the quickest way to do this?  **Choose One  
a. Press enter after entering each command and its arguments  
b. Put them in a script and execute the script  
c. Separate each command with a semi-colon (;) and press enter after the last command  
d. Separate each command with a / and press enter after the last command**  
  
c   
  
The semi-colon may be used to tell the shell that you are entering multiple commands that should be executed serially. If these were commands that you would frequently want to run, then a script might be more efficient. However, to run these commands only once, enter the commands directly at the command line.

You attempt to use shadow passwords but are unsuccessful. What characteristic of the /etc/passwd file may cause this?  **Choose one:  
a. The login command is missing.  
b. The username is too long.  
c. The password field is blank.  
d. The password field is prefaced by an asterisk.**   
  
c   
  
The password field must not be blank before converting to shadow passwords.

When you install a new application, documentation on that application is also usually installed. Where would you look for the documentation after installing an application called MyApp? **Choose one:  
a. /usr/MyApp  
b. /lib/doc/MyApp  
c. /usr/doc/MyApp  
d. In the same directory where the application is installed.**  
  
c   
  
The default location for application documentation is in a directory named for the application in the /usr/doc directory.

What file would you edit in your home directory to change which window manager you want to use?  **A) Xinit  
B) .xinitrc  
C) XF86Setup  
D) xstart  
E) xf86init**  
  
Answer: B - The ~/.xinitrc file allows you to set which window man-ager you want to use when logging in to X from that account.   
Answers a, d, and e are all invalid files. Answer c is the main X server configuration file.

What command allows you to set a processor-intensive job to use less CPU time?  **A) ps  
B) nice  
C) chps  
D) less  
E) more**  
  
Answer: B - The nice command is used to change a job's priority level, so that it runs slower or faster. Answers a, d, and e are valid commands but are not used to change process information. Answer c is an invalid command.

While logged on as a regular user, your boss calls up and wants you to create a new user account immediately. How can you do this without first having to close your work, log off and logon as root?  **Choose one:  
a. Issue the command rootlog.  
b. Issue the command su and type exit when finished.  
c. Issue the command su and type logoff when finished.  
d. Issue the command logon root and type exit when finished.**   
  
Answer: b   
You can use the su command to imitate any user including root. You will be prompted for the password for the root account. Once you have provided it you are logged in as root and can do any administrative duties.

# **Linux Interview Questions and Answers**

In order to run fsck on the root partition, the root partition must be mounted asreadonly   
  
You cannot run fsck on a partition that is mounted as read-write.

**In order to improve your system's security you decide to implement shadow passwords. What command should you use?**   
pwconv   
  
The pwconv command creates the file /etc/shadow and changes all passwords to 'x' in the /etc/passwd file.

**Bob Armstrong, who has a username of boba, calls to tell you he forgot his password. What command should you use to reset his command?**   
passwd boba   
  
The passwd command is used to change your password. If you do not specify a username, your password will be changed.

The top utility can be used to change the priority of a running process? Another utility that can also be used to change priority is **\_\_\_\_\_\_\_\_\_\_\_**?   
nice   
  
Both the top and nice utilities provide the capability to change the priority of a running process.

**What command should you type to see all the files with an extension of 'mem' listed in reverse alphabetical order in the /home/ben/memos directory.**   
ls -r /home/ben/memos/\*.mem   
  
The -c option used with ls results in the files being listed in chronological order. You can use wildcards with the ls command to specify a pattern of filenames.

**What file defines the levels of messages written to system log files?**   
kernel.h   
  
To determine the various levels of messages that are defined on your system, examine the kernel.h file.

**What command is used to remove the password assigned to a group?**   
gpasswd -r   
  
The gpasswd command is used to change the password assigned to a group. Use the -r option to remove the password from the group.

**What command would you type to use the cpio to create a backup called backup.cpio of all the users' home directories?**   
find /home | cpio -o > backup.cpio   
  
The find command is used to create a list of the files and directories contained in home. This list is then piped to the cpio utility as a list of files to include and the output is saved to a file called backup.cpio.

**What can you type at a command line to determine which shell you are using?**   
echo $SHELL   
  
The name and path to the shell you are using is saved to the SHELL environment variable. You can then use the echo command to print out the value of any variable by preceding the variable's name with $. Therefore, typing echo $SHELL will display the name of your shell.

What type of local file server can you use to provide the distribution installation materials to the new machine during a network installation? **A) Inetd  
B) FSSTND  
C) DNS  
D) NNTP  
E) NFS**   
E - You can use an NFS server to provide the distribution installation materials to the machine on which you are performing the installation. Answers a, b, c, and d are all valid items but none of them are file servers. Inetd is the superdaemon which controls all intermittently used network services. The FSSTND is the Linux File System Standard. DNS provides domain name resolution, and NNTP is the transfer protocol for usenet news.

If you type the command cat dog & > cat what would you see on your display? **Choose one:   
a. Any error messages only.  
b. The contents of the file dog.  
c. The contents of the file dog and any error messages.  
d. Nothing as all output is saved to the file cat.**  
d   
  
When you use & > for redirection, it redirects both the standard output and standard error. The output would be saved to the file cat.

You are covering for another system administrator and one of the users asks you to restore a file for him. You locate the correct tarfile by checking the backup log but do not know how the directory structure was stored. What command can you use to determine this?  **Choose one:  
a. tar fx tarfile dirname  
b. tar tvf tarfile filename  
c. tar ctf tarfile  
d. tar tvf tarfile**   
  
d   
  
The t switch will list the files contained in the tarfile. Using the v modifier will display the stored directory structure.

You have the /var directory on its own partition. You have run out of space. What should you do? Choose one: **a. Reconfigure your system to not write to the log files.  
b. Use fips to enlarge the partition.  
c. Delete all the log files.  
d. Delete the partition and recreate it with a larger size.**   
  
d   
  
The only way to enlarge a partition is to delete it and recreate it. You will then have to restore the necessary files from backup.

You have a new application on a CD-ROM that you wish to install. What should your first step be?  **Choose one:  
a. Read the installation instructions on the CD-ROM.  
b. Use the mount command to mount your CD-ROM as read-write.  
c. Use the umount command to access your CD-ROM.  
d. Use the mount command to mount your CD-ROM as read-only.**   
  
d   
  
Before you can read any of the files contained on the CD-ROM, you must first mount the CD-ROM.

When you create a new partition, you need to designate its size by defining the starting and ending **\_\_\_\_\_\_\_\_\_\_\_\_\_**.  
cylinders   
  
When creating a new partition you must first specify its starting cylinder. You can then either specify its size or the ending cylinder.

**You need to see the last fifteen lines of the files dog, cat and horse. What command should you use?**tail -15 dog cat horse   
  
The tail utility displays the end of a file. The -15 tells tail to display the last fifteen lines of each specified file.

**Who owns the data dictionary?**   
The SYS user owns the data dictionary. The SYS and SYSTEM users are created when the database is created.

**You routinely compress old log files. You now need to examine a log from two months ago. In order to view its contents without first having to decompress it, use the \_\_\_\_\_\_\_\_\_ utility.**   
zcat   
  
The zcat utility allows you to examine the contents of a compressed file much the same way that cat displays a file.

**You suspect that you have two commands with the same name as the command is not producing the expected results. What command can you use to determine the location of the command being run?**   
which   
  
The which command searches your path until it finds a command that matches the command you are looking for and displays its full path.

**You locate a command in the /bin directory but do not know what it does. What command can you use to determine its purpose.**   
whatis   
  
The whatis command displays a summary line from the man page for the specified command.

**You wish to create a link to the /data directory in bob's home directory so you issue the command ln /data /home/bob/datalink but the command fails. What option should you use in this command line to be successful.**   
Use the -F option   
  
In order to create a link to a directory you must use the -F option.

**When you issue the command ls -l, the first character of the resulting display represents the file's \_\_\_\_\_\_\_\_\_\_\_.**   
type   
  
The first character of the permission block designates the type of file that is being displayed.

**What utility can you use to show a dynamic listing of running processes? \_\_\_\_\_\_\_\_\_\_**   
top   
  
The top utility shows a listing of all running processes that is dynamically updated.

**Where is standard output usually directed?**   
to the screen or display   
  
By default, your shell directs standard output to your screen or display.

**You wish to restore the file memo.ben which was backed up in the tarfile MyBackup.tar. What command should you type?**   
tar xf MyBackup.tar memo.ben   
  
This command uses the x switch to extract a file. Here the file memo.ben will be restored from the tarfile MyBackup.tar.

**You need to view the contents of the tarfile called MyBackup.tar. What command would you use?**  
tar tf MyBackup.tar   
  
The t switch tells tar to display the contents and the f modifier specifies which file to examine.

**You want to create a compressed backup of the users' home directories. What utility should you use?**   
tar   
  
You can use the z modifier with tar to compress your archive at the same time as creating it.

**What daemon is responsible for tracking events on your system?**   
syslogd   
  
The syslogd daemon is responsible for tracking system information and saving it to specified log files.

**You have a file called phonenos that is almost 4,000 lines long. What text filter can you use to split it into four pieces each 1,000 lines long?**   
split   
  
The split text filter will divide files into equally sized pieces. The default length of each piece is 1,000 lines.

**You would like to temporarily change your command line editor to be vi. What command should you type to change it?**   
set -o vi   
  
The set command is used to assign environment variables. In this case, you are instructing your shell to assign vi as your command line editor. However, once you log off and log back in you will return to the previously defined command line editor.

**What account is created when you install Linux?**   
root   
  
Whenever you install Linux, only one user account is created. This is the superuser account also known as root.

**What command should you use to check the number of files and disk space used and each user's defined quotas?**   
  
repquota   
  
The repquota command is used to get a report on the status of the quotas you have set including the amount of allocated space and amount of used space.