If you are preparing for interviews for linux admin jobs you should be familiar with **below concepts..**

1) Port number of different servers {cat /etc/services}
2) Linux Installation(through FTP,HTTP,NFS)
3) Boot process
4) Diff b/w ext3 and ext2
5) RAID LEVELS and Selection of raid
6) backup methods
7) Package management such as Yum server
8) Kernel Tuning
9) IPTABLES
10) TCP WRAPPERS
11) DIFFERENT RUN LEVELS
12) USER AND GROUP MANAGEMENT
13) QUOTA SETTING(user and group)
14) DIFF B/W CRON AND AT
15) BASIC SHELL SCRIPTING
16) Troubleshooting different issues.
17) Tell me why we should hire you?
18) DAILY ACTIVITES IN YOUR CURRENT COMPANY
19) RECENTLY SOLVED CRITICAL ISSUE
20) LVM (Very Imp)
21) vertias Volume manager
22) cluster basic like HAD , GAB , LLT , HEARTBEAT , CONFIG FILES , RESOURSE , SERVICE GROUPS etc
23) kernel panic troubleshooting
24) Process management
25)Configuration part of NFS , NIS , Samba , DHCP , DNS,Apache, Sendmail etc.
26)Remote administration experience.

Linux Interview Questions and Answers

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.

Linux Interview Questions and Answers

In order to run fsck on the root partition, the root partition must be mounted as
readonly

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.

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.

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.

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

when you create a user in linux , the default settings comes from ----------

1) /etc/skel.

2)name the DNS records

2) Mx records.

3)What is the difference between hard links and soft links

3) Hard links for files only and soft links are for both directoris and files.

4)what is the difference between name base and ip base virtual hosting

4) in ip base you are running more than one web site on the same server machine,and in name base you have to put more than one DNS record for your IP address in the DNS.

5)where are the kernel parameters stored in linux

5) in /boot.

6) you want to deploy linux on identical machines , which method you will use

Unattendend Installation Method With the help of PXE Server & NFS server.

7)Name of the file which describe the kickstart installation

Anaconda ks.cfg

8) How you give another Ip address on the same NIC (network card)

copy a file in /etc/sysconfig/network-script/ifcfg-eth0 to ifcfg-eth0:1 .

9)you defined samba shares and you want these shares to be available on network , you don't want to restart samba server
which command you will use ??

Service SMB restart

10)you want to monitor systems on your network ,what utility you will use

TOP and ps

11) you want to backup a test.bak file on 11 PM every Sunday what you will do?

Edit the cron tab entry

12) can you define the linux boot process

1. BIOS: The Basic Input/Output System is the lowest level interface between the computer and peripherals.
   The BIOS performs integrity checks on memory and seeks instructions on the Master Boor Record (MBR) on the floppy drive or hard drive.
2. The MBR points to the boot loader (GRUB or LILO: Linux boot loader).
3. Boot loader (GRUB or LILO) will then ask for the OS label which will identify which kernel to run and where it is located (hard drive and partition specified). The installation process requires to creation/identification of partitions and where to install the OS. GRUB/LILO are also configured during this process. The boot loader then loads the Linux operating system.
4. The first thing the kernel does is to execute init program. Init is the root/parent of all processes executing on Linux.
5. The first processes that init starts is a script /etc/rc.d/rc.sysinit
6. Based on the appropriate run-level, scripts are executed to start various processes to run the system and make it functional

Boot process takes place in 4 scenes with 4 main characters.

Scene 1

when the computer is switched on,it automatically invokes BIOS[a ROM chip embedded in the motherboard].The BIOS will start the processor and perform a

POST[power on self test] to check whether the connected device are ready to use and are working properly.
Once the POST is completes BIOS will jump to a specified location in the RAM and check for the booting device.The boot sector is always the first sector of the hard disk and BIOS will load the MBR into the memory.

Scene 2
Here the boot loader takes the control of the booting process.LILO or GRUB are the boot loaders commonly available. It will help the user to select various boot options.Depending on the boot option selected the kernel is loaded.

scene 3

After kernel is loaded the kernel will take the control of the booting process and it will initialize all the hardwares including I/O processors etc.kernel then creates a root device and mounts the partitions.

Scene 4
INIT is loaded.

13)what is initrd

initrd image is the initial ram disk image While the system getting booted the kernel image will get loaded into the main memory.

14)can you name of the actual kernel in linux

vmlinuxz.

15) how you get the kernel version

uname -r .

16)how you change run levels in linux

/etc/inittab

17) you want /dev/hda10 mounted whenever your system boots what you will do

put the entry in fstab with proper drivers and mount point(/dev/hda10 mount point ext2/3 defaults 0 0).

18) you want bind to be run at boot time ,which command you will use

chkconfig.

19)which utility will give you information about running process at run time

top command and ps -el.

20) you want to know if nfs package is installed on your system

rpm -qa nfs and you can check export file in /etc.

21) what is the difference between rpm , yum and RHEN

rpm required dependency software and yum can install automatically with dependancy

22) what is a proc directory

/proc directory are not real files--they are hooks to look at information available to the kernel.

23) what is the difference between current directory and home directory

home directory is one over which user have complete controland it is its default working directory when its logs in.while the current directory is the users current directorywhich may or may not be his home directory.

24)what is exit status in linux

You can use $? to find out the exit status of command(`$ echo $?`).

25)you have a dual boot system with windows XP and

Fedora Linux , you want to access windows partition which is on fat32 file system , what you will do ??

1.
Differences between TCP and UDP

TCP
1)TCP -Transmission control protocol
2)TCP is a connection oriented protocol.
3)Three way handshake happens between client and server.
4)TCP is a reliable data transfer
5)slow transmission of data compare to UDP.
6)TCP is used to send file like database,where reliability play the first role
UDP
1)UDP -User Datagram protocol
2)UDP is connectionless protocol
3)NO 3 way handshake
4)NOt a reliable data transer
5)Faster than TCP
6)used to send data like video,audio

1. DNS (Domian name server)
DNS resolves hostname to IP address (forward lookup),
resolves IP address to hostname (reverse lookup), it allows machines to logically grouped by name domain, provides email routing.
DNS port: 53
dameon: named

What utility can you use to automate rotation of logs?

Logrotate

Any user who is listed in the /etc/shutdown.allow file will be able to run the shutdown command without being root.

As the system administrator you have created a directory containing some scripts that you have written. You want to have all your users to be able to run this scripts. Which file should you edit to ensure that the scripts will run without your users having to type the complete path to the script?

Choose one:

a. ~/.profile

b. /etc/profile

c. /etc/bash

d. ~/.bash

b. /etc/profile

What are the files to be used in the network installation of linux os?

/etc/sysconfig/network,/etc/resolv.conf,/etc/hosts

: What is the command to see the installed rpm's in the linux system.

you can view the installed rpm in your linux box by :

rpm -qa | grep rpm name

Please explain the file structure of linux?

root - The home directory for the root user
home - Contains the user's home directories along with directories for services
ftp
HTTP
samba
george
bin - Commands needed during bootup that might be needed by normal users
sbin - Like bin but commands are not intended for normal users. Commands run by LINUX.
proc - This filesystem is not on a disk. It is a virtual filesystem that exists in the kernels imagination which is memory.
1 - A directory with info about process number 1. Each process has a directory below proc.
usr - Contains all commands, libraries, man pages, games and static files for normal operation.
bin - Almost all user commands. some commands are in /bin or /usr/local/bin.
sbin - System admin commands not needed on the root filesystem. e.g., most server programs.
include - Header files for the C programming language. Should be below /user/lib for consistency.
lib - Unchanging data files for programs and subsystems
local - The place for locally installed software and other files.
man - Manual pages
info - Info documents
doc - Documentation
tmp
X11R6 - The X windows system files. There is a directory

similar to usr below this directory.
X386 - Like X11R6 but for X11 release 5
boot - Files used by the bootstrap loader, LILO. Kernel images are often kept here.
lib - Shared libraries needed by the programs on the root filesystem
modules - Loadable kernel modules, especially those needed to boot the system after disasters.
dev - Device files
etc - Configuration files specific to the machine.
skel - When a home directory is created it is initialized with files from this directory
sysconfig - Files that configure the linux system for devices.
var - Contains files that change for mail, news, printers log files, man pages, temp files
file
lib - Files that change while the system is running normally
local - Variable data for programs installed in /usr/local.
lock - Lock files. Used by a program to indicate it is using a particular device or file
log - Log files from programs such as login and syslog which logs all logins and logouts.
run - Files that contain information about the system that is valid until the system is next booted
spool - Directories for mail, printer spools, news and other spooled work.
tmp - Temporary files that are large or need to exist for longer than they should in /tmp.
catman - A cache for man pages that are formatted on demand
mnt - Mount points for temporary mounts by the system administrator.
tmp - Temporary files. Programs running after bootup should use /var/tmp.

The Linux system contains thousand of files located within many directories. All directories are organized in a tree-structure like manner.

* The 'trunk' of the tree is the root directory.
* The root directory is simply identified as a "/".
* All other directories 'branch' off from the trunk.

The following lists the most common directories and their intended contents.

* / - root directory
* /home - where directories are contained for each user, example:
* /usr - pronounced 'user' and contains Linux commands and utilities
    - o /bin - binary executable programs
    - o /lib - program libraries, similar to Windows 'dll' files
    - o /sbin - more executable programs and Linux utilities for administrative purposes
    - o /doc - documentation
    - o /src - source code to programs
* /tmp - temporary work files

```
    * /etc - configuration files
          o /rc.d - scripts used during boot and shutdown
process
          o /sysconfig - default configuration files
          o /sysconfig/network-scripts - network scripts
          o /sysconfig/daemons - special programs that run
in background, such as print spooling
    * /bin - binary executable programs that all users need
    * /dev - device files that control drives, terminals and
any equipment attached to the server
    * /var - user specific files
          o /log - log files containing system usage and errors
          o /spool - where spooled files are stored during
print spooling process
          o /mail - where Email files are stored until
retrieved by client Email program
    * /proc - system files
    * /root - root's home directory
    * /opt - other options
    * /sbin - more executable programs and utilities
```

What is Kernel? Explain the task it performs.

Answer

Kernel is used in UNIX like systems and is considered to be the heart of the operating system. It is responsible for communication between hardware and software components. It is primarily used for managing the systems resources as well.

Kernel Activities:

- The Kernel task manager allows tasks to run concurrently.
- Managing the computer resources: Kernel allows the other programs to run and use the resources. Resources include i/o devices, CPU, memory.
- Kernel is responsible for Process management. It allows multiple processes to run simultaneously allowing user to multitask.
- Kernel has an access to the systems memory and allows the processes to access the memory when required.
- Processes may also need to access the devices attached to the system. Kernel assists the processes in doing so.
- For the processes to access and make use of these services, system calls are used.

Linux - What does nslookup do? Explain its two modes - August 21, 2008 at 22:00 pm by Rajmeet Ghai

What does nslookup do? 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, servers etc. It sends a domain name query packet to the corresponding DNS.

Nslookup has two modes. Interactive and non interactive. Interactive mode allows the user to interact by querying information about different hosts and domains.

Non interactive mode is used to fetch information about the specified host or domain.

Interactive mode:

Nslookup [options] [server]

What is Linux and why is it so popular?

Answer

Linux is an operating system that uses UNIX like Operating system. However, unlike UNIX, Linux is an open source and free software. Linux was originally created by Linus Torvalds and commonly used in servers.

Popularity of Linux is because of the following reasons

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

What is 'inode'?

Each file in UNIX has a unique number called as an inode. Using this number the file information like user, group, ownership and access mode information can be found. A files inode number can be found using the following command:

Ls –i

If the inode number is known, the following command can be used to get details of the file:

Ls –l

What is use of sed command?

Sed command in UNIX is commonly used for processing of files. Sed stands for Stream Editor which parses text files and used for making textual transformations to a file. The command specified to Sed, is applied on the file line by line.

Example:

To replace all matching occurrences of some text to another.

sed -e 's/olddata/newdata/g' inputFileName > outputFileName

Here, g is global which replaces ALL occurrences.

What are the main differences between RHEL4 & RHEL5?

Answer:
Difference between RHEL 4 and RHEL 5 :
1) In RHEL 4 SELinux Block only 13 services, But on RHEL 5 SElinux Block 80 services.

2) RHEL 4 have ext2 filesystem, but RHEL 5 we have ext3 filesystem that support Journal.

3) RHEL 4 have no virtualization Feature, but in RHEL 5 we have virtualization with Hypervisor-V.

4) In RHEL 4 we have no Yum, But in RHEL 5 we have Yum available.

Any many more..... need more time to describe it

(or)

rhel4	rhel5
no yum server	yum server
selinux	Advanced selinux
secure	more secure
no cdkey	cd key

---	virtualization
mim 256 mb ram	512 ram
---	better support for
	Red Hat Directory
	Ext4 (on latest version)

What is the difference between Telnet and SSH?

Answer:
SSH using PORT 22 and telnet using Port 23 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.

How to recover a deleted file in linux ?

Answer:
Determine the partition in which the file you wish to recover was located by using the command pwd (present work directory) and unmount the current directory by using the command umount. Use the "debugfs" command. The "debugfs" command is used to handle most major errors and bugs that can occur in Linux by using #debugfs /usr/directory name.Use the "lsdel" once you have begun the debug of the file system. Recover those files you wish to undelete and take backup of that file.

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

Answer:
Well in my opinion is case if minimum nukber of partition is asked then better answer would be
/
/boot
/swap

1)How do you find out what's your shell? - echo $SHELL
2)What's the command to find out today's date? - date

3)How do you find out the current directory you're in? - pwd
4)How do you find out your own username? - whoami/who am i
5)How do you send a mail message to somebody? - mail surendra.anne@gmail.com -s 'Your subject' -c 'test@gmail.com'

6)What's the command to find out users on the system? - who/users
7)How do you remove a file? - rm
8)How do you remove a - rm -rf
9)How do you count words, lines and characters in a file? - wc
10)How do you search for a string inside a given file? - grep string filename

11)How do you search for a string inside a directory? - grep string *

12)How do you search for a string in a directory with the subdirectories recursed? - grep -r string *
13)What are PIDs? - They are process IDs given to processes. A PID can vary from 0 to 65535.
14)How do you list currently running process? - ps
15)How do you stop a process? - kill pid

16)How do you find out about all running processes? - ps -ag
17)How do you stop all the processes, except the shell window? - kill 0
18)How do you fire a process in the background? - ./process-name &
19)How do you refer to the arguments passed to a shell script? - $1, $2 and so on. $0 is your script name.
20)What's the conditional statement in shell scripting? - if {condition} then … fi

21)How do you do number comparison in shell scripts? - -eq, -ne, -lt, -le, -gt, -ge
22)How do you test for file properties in shell scripts? - -s filename tells you if the file is not empty, -f filename tells you whether the argument is a file, and not a directory, -d filename tests if the argument is a directory, and not a file, -w filename tests for writeability, -r filename tests for readability, -x filename tests for excitability
23)How do you do Boolean logic operators in shell scripting? - ! tests for logical not, -a tests for logical and, and -o tests for logical or.
24)How do you find out the number of arguments passed to the shell script? - $#
25)What's a way to do multilevel if-else's in shell scripting? - if {condition} then {statement} elif {condition} {statement} fi

26)How do you write a for loop in shell? - for {variable name} in {list} do {statement} done
27)How do you write a while loop in shell? - while {condition} do {statement} done
28)How does a case statement look in shell scripts? - case {variable} in {possible-value-1}) {statement};; {possible-value-2}) {statement};; esac
29)How do you read keyboard input in shell scripts? - read {variable-name}
30)How do you define a function in a shell script? - function-name() { #some code here return }

31)How does getopts command work? - The parameters to your script can be passed as -n 15 -x 20.Inside the script, you can iterate through the getopts array as while getopts n:x option, and the variable $option contains the value of the entered option.

1)What is the difference between TFTP and FTP servers?

A)Both are file transfer servers but slight difference is **TFTP** server uses **UDP** protocol and **FTP** uses **TCP** protocol. **TFTP** is good for slow connection paths.

2)What is the port no for FTP?

A)20 for Data and **21** for Control(normally when an interviewer ask's ftp port number just say **21.**

3)What is the port no for TFTP?

A)69.

4) How to restrict users to their home directories?

A)By setting up **"chroot_local_user=YES".**

5)How to restrict total number of users accessing FTP server?

A1) If **Vsftpd** is running under xinted service, then you can use **xineted** to get per-service per **IP** connection limits or

A2) If you run **vsftpd** in **"standalone"** mode with the **"setting listen=YES"**, then you can investigate the setting (e.g.) : **"max_clients=10"**

6)I want to copy multiple files with out prompting for any info, how can I do that one?

A)Simply do **"ftp -i ftpserver"** this command will suppress any info displayed on ftp server.

or you can just type prompt **ftp** prompt to suppress info messages have a look here.

7) Some times Local users cannot log in. How to resolve this issue?

A) Check **"local_enable=YES"** in your **/etc/vsftpd/vsftpd**. conf to allow local users to log in.

8) How do we integrate with LDAP(Lightweight Directory Access Protocol) users and login?

A) Use vsftpd's(Very Secure FTPD) **PAM(Pluggable Authentication Modules)** integration to do this, and have PAM authenticate against an LDAP repository.

9) Can we host different ftp sites on single machine, I mean virtual hosting concept like Apache?

A1) Yes. If you integrate **vsftpd** with **xinetd**, you can use xinetd to bind to several different IP addresses. For each IP address, get xinetd to launch vsftpd with a different config file. This way, you can get different behavior per virtual address.

A2) Alternatively, run as many copies as vsftpd as necessary, in standalone mode. Use **"listen_address=x.x.x.x"** to set the virtual IP.

10) How to restrict different users with different permissions in vsftpd

A) By setting up **"user_config_dir"** entry in **"vsftpd.conf".**

11)How to change vsftpd default port?

A)By setting "**listen_port"** option in **"vsftpd.conf"**.

12) Vsftpd is reporting times as GMT times and not local times!. How to resolve this?

A) This behavior can be changed with the setting **"use_localtime=YES".**

13) How to disable certain FTP commands?

A) There are some individual settings **(e.g. dirlist_enable)** or you can specify a complete set of allowed commands with **"cmds_allowed".**

14) How does vsftpd support per-IP limits?

A1) If you are running vsftpd standalone, there is a **"max_per_ip"** setting.

A2) Yes. If you are running vsftpd via xinetd, there is an xinetd config variable **"per_source".**

15) How Does vsftpd can do bandwidth limiting?

A) settings such as **"anon_max_rate"** and **"local_max_rate"** can be used to set this limits.

16) How to restrict some IP's not use my FTP server?

A1) vsftpd can integrate with **tcp_wrappers** (if built with this support). It is enabled with the setting **"tcp_wrappers=YES".**

17) Does vsftpd support IPv6?

A) Yes, as of **"version 1.2.0"**.

18) Help! I'm getting messages along the lines of "500 OOPS: vsf_sysutil_bind" when trying to do downloads (particularly lots of small files).

A) "vsftpd-1.2.1" should sort this out.

19) Can we use vsftpd to hiding or denying certain files?

A) Yes. Look at the **hide_file** and **deny_file** options.

20)How you can check if there is any syntax error in vsftpd.conf file?

A)Just type **vsftpd** with out quoats.

```
A common misconception: the place/protocol you use to fetch your
email
is the same place/protocol that you use to send your email:
   - sending email uses SMTP
   - reading email uses POP3 or IMAP
   - they can be completely separate machines

   http://wiki.mutt.org/?MailConcept

Q: T/F, unlike POP3, SMTP can be used to both send and receive email.
Q: T/F, unlike SMTP, POP3 can be used to both receive and send email.

   - may be completely different servers
   - though note POP-before-SMTP (SMTP-after-POP) requires coupling:

   http://tools.ietf.org/html/rfc2476 (section 3.3)

   "Requiring a POP [POP3] authentication (from the same IP address)
    within some amount of time (for example, 20 minutes) prior to the
    start of a message submission session has also been used, but
this
    does impose restrictions on clients as well as servers which may
    cause difficulties.  Specifically, the client must do a POP
    authentication before an SMTP submission session, and not all
clients
    are capable and configured for this.  Also, the MSA must
coordinate
    with the POP server, which may be difficult.  There is also a
window
```

during which an unauthorized user can submit messages and appear to
be a prior authorized user."

Q: Describe briefly how POP-before-SMTP works to authenticate an SMTP session.

MUA - Mail User Agent (email client)
- the user's interface to the protocols - "presentation layer"
- usually gives access to functionality of both MTA and MRA/MAA
- but may not itself implement any protocols (may read/write file system)

http://en.wikipedia.org/wiki/Mail_user_agent
"An e-mail client, also called a Mail User Agent (MUA), is a computer
program that is used to read and send e-mail.

Originally, the MUA was intended to be a simple program to read the user's
mail messages, which the mail delivery agent (MDA) in conjunction with
the mail transfer agent (MTA) would transfer into a local mailbox.

The most important mailbox formats are mbox and Maildir. These rather
simple protocols for locally storing e-mails make import, export and
backup of mailfolders quite easy.

E-mails to be sent would be handed over to the MTA, perhaps via
a mail submission agent [MSA], therefore an MUA would not have to
provide any transport-related functions.

*Since the various Microsoft Windows versions intended for home use never
*provided an MTA, most modern MUAs have to support protocols like POP3
*and Internet Message Access Protocol (IMAP) to communicate with a remote
*MTA located at the e-mail providers machine."

- user agents (MUAs) are user-visible email clients of all descriptions
- e.g. mutt, "mail", "Mail", "mailx", pine, elm
- e.g. KMail, Eudora, MS Outlook
- e.g. web-browser email (Netscape Messenger,Mozilla,Thunderbird)
- e.g. webmail, Horde, SqurrelMail

http://en.wikipedia.org/wiki/List_of_mail_servers#POP.2FIMAP

Q: Briefly describe the function of a mail system MUA.

MSA - Mail Submission Agent
http://tools.ietf.org/html/rfc2476
"acts as a submission server to accept messages from MUAs, and either
delivers them or acts as an SMTP client to relay them to an MTA."

- enforce policy (no open relay)

- enforce standards (no forged headers, etc.)
- enforce filtering (SpamAssassin, etc.)
- may modify messages (section 8 of RFC)

http://en.wikipedia.org/wiki/List_of_mail_servers#Mail_filtering

Q: Briefly describe the function of a mail system MSA.

MTA - Mail Transfer Agent (mail server, mail exchange server)
"A process which conforms to [SMTP-MTA], which acts as an SMTP server to
accept messages from an MSA or another MTA, and either delivers them or
acts as an SMTP client to relay them to another MTA."

http://en.wikipedia.org/wiki/Mail_transfer_agent
"It receives messages from another MTA (relaying), a mail submission agent (MSA) that itself got the mail from a mail user agent (MUA), or directly from an MUA, thus acting as an MSA itself. The MTA works behind the scenes, while the user usually interacts with the MUA. The delivery of e-mail to a user's mailbox typically takes place via a mail delivery agent (MDA); many MTAs have basic MDA functionality built in, but a dedicated MDA like procmail can provide more sophistication."

- transfers email between machines (other MTAs) via SMTP
- Internet-facing, open ports: security issues
- sendmail, postfix, qmail, exim
- may have MDA ability to transfer email to user's mailbox

http://en.wikipedia.org/wiki/List_of_mail_servers#SMTP

Q: Briefly describe the function of a mail system MTA.

MDA - Mail Delivery Agent
http://en.wikipedia.org/wiki/Mail_delivery_agent
"A Mail Delivery Agent (MDA) is software that accepts incoming e-mail
messages and distributes them to recipients' individual mailboxes (if the destination account is on the local machine), or forwards back to an SMTP server (if the destination is on a remote server).
A mail delivery agent is not necessarily a mail transfer agent (MTA),
although on many systems the two functions are implemented by the same program."
- Unix/Linux: /bin/mail, procmail

Q: Briefly describe the function of a mail system MDA.

MRA/MAA - Mail Retrieval Agent / Mail Access Agent
http://tools.ietf.org/html/rfc1939 - POP3 port 110
http://tools.ietf.org/html/rfc3501 - IMAP-V4-R1 port 143

- often built-in to mail clients (MUAs)
- can be stand-alone
  - e.g. fetchmail gets the mail; MUA reads mail from file system

Q: Briefly describe the function of a mail system MRA/MAA.

Mail server comparison

---
  http://en.wikipedia.org/wiki/List_of_mail_servers
  - see comparison near bottom

  - PUSH protocols - sending email: MTA - SMTP
  - PULL protocols - reading email: MRA/MAA - POP3, IMAP

 MDAs write local mailboxes; they may not implement Internet protocols
 (unless they have to forward off-machine without benfit of an MTA).

 Single-user PCs often don't run separate MTA or MRA/MAA programs.
 Your chose of mail reader (e.g. Pine, Elm, Outlook) itself PULLs your
 incoming email from a remote server (acting as an MRA/MAA) and then
 PUSHes your outgoing email to the remote server (acting as an MTA).

Q: What is the difference between a PUSH protocol and a PULL protocol?
Q: T/F, SMTP is a PUSH protocol.
Q: T/F, POP3 is a PUSH protocol.
Q: T/F, HTTP is a PUSH protocol.

A History of MTAs

I. Incoming - delivering your incoming email via SMTP:

* Sending email into Unix/Linux machines:
  Unix/Linux was traditionally multi-user and ran its own MTA
  (e.g. sendmail) that accepted incoming SMTP connections. Remote systems
  could use SMTP to drop off your email with your local MTA (sendmail),
  and the MTA would hand the email to an MDA (/bin/mail, procmail)
  to put it in your mailbox in the local file system. Your MUA
  (e.g. /usr/ucb/Mail) would read the mail from your inbox (no need
  for POP3 or IMAP in any MUA). There are a few different conventions
  for inbox formats so that many different MUAs can read your email,
  all without knowing POP or IMAP.

  - sendmail (running as root!) has had many security patches
    - the first Morris Internet worm (Nov 1988) used sendmail security holes
    - http://en.wikipedia.org/wiki/Morris_worm

Q: Why don't many Unix MUAs need to know how to run POP or IMAP?

  Current single-user Unix/Linux PCs often have a local-only MTA
  that handles the sending and delivery of local on-machine email but
  doesn't accept SMTP from off-site. (Best to keep ports closed on
  Internet-facing machines!)

  On recent single-user Unix/Linux workstations, the MUAs mimic their
  Windows counterparts and include MRA/MAA features. Your chosen MUA
  (e.g. Elm, Pine, Mutt) is responsible for fetching your email via POP3
  or IMAP (this is an MRA/MAA function); or, you use an intermediate
  MRA/MAA program such as "fetchmail" and your MUA reads the mail out
  of the local file system after the MRA/MAA has put it there.

  - no Internet-facing MTA means fewer open ports and fewer attacks
    - don't run an Internet-facing MTA if you don't need it

* Sending email into MS Windows machines (or not):
  Windows had (has?) no MTA - you can't send an email to a Windows PC
  using SMTP. Your personal Windows MUA has to fetch the email itself
  via POP3 or IMAP and keep a copy in the local file system.

 - no open ports for incoming email; no open mail port security issues

* Note that MUAs that implement POP/IMAP typically store the email in
  the local file system in a format that only that MUA can handle.
  (Thunderbird can't use an Outlook mail folder, and vice-versa.)
  The concept of a common inbox format usable by different MUAs was lost.

Q: T/F, the standards for inbox formats developed under Unix were adopted
   by MUAs on PCs, so that different MUAs can read the same inbox.

II. Outgoing - sending your outgoing email via SMTP:

* Unix/Linux machines have traditionally each had their own MTA (sendmail)
  that could directly deliver email on the Internet using MX record lookup.

  Every local Unix MUA would put email into a directory where the MTA
  (sendmail) would eventually pick it up and transfer it, retrying as
  necessary. No MUA needed to know how to do SMTP; only the MTA did that.

  You could optionally tell your machine's MTA not to send mail directly
  to its destination via SMTP over the Internet, but to use a remote
  "smart" MTA that could accept your outgoing email and figure out
  how to deliver it. (You have to use such a "smart" host here at
  Algonquin; since, you cannot connect to any off-campus SMTP servers.)
  The MTA on your machine would use SMTP to drop off the queued mail at
  the smart host, and the smart host would do the MX record lookup and
  final SMTP delivery.

  Since the local Unix MTAs were separately scheduled programs, you could
  queue email from a MUA into the file system even when your machine was
  not connected to the Internet. The MUA or local MTA would queue up
  your email in the file system until your MTA was finally able to make
  a connection to deliver it off-machine. (In the days of modems, the
  Internet connection was often made late at night when rates were lower.)

Q: Why don't most Unix MUAs need to know SMTP?

```
  Current single-user Unix/Linux PCs now have MUAs that mimic their
  Windows counterparts - the MUAs ignore the file system and the
local
  MTA and expect you to give the name of a remote "smart" MTA to
which
  all email will be sent via SMTP for actual delivery.

  The Algonquin Linux lab has both types of mail systems:  Command-
line
  email (e.g. the "mail" command) queues up mail for the local
  MTA (sendmail) to send.  (This is currently broken.)  GUI MTAs
  (e.g. Thunderbird, Mozilla) ignore the local file system and the
local
  MTA and use a "smart" remote MTA (e.g.
outmail.algonquincollege.com)
  to deliver the mail.  (This supposedly still works.)

* MS Windows has no local MTA - no program exists whose job it is
just
  to deliver queued email.  Each MUA has to know how to do its own
  SMTP connection and each MUA has to be configured (separately!)
with
  the address of a smart MTA to which it connects.  MUAs on Windows
  machines all contain networking code to drop off email at some
"smart"
  MTA that does the actual delivery.  There is no local MTA queue and
  much duplication of SMTP code in all the MUAs.

  On Windows, it is up to each MUA to deal with what happens if the
  message being composed can't be dropped off right away at the
remote
  smart MTA.  Better MUAs will queue the email for later
transmission.
  Poor MUAs will tell you that your mail can't be sent.

Q: Why do MUAs on Windows all need to know how to talk SMTP?

Q: Unix/Linux mail user agents didn't need to know how to talk to
SMTP
   servers - you never had to configure your "outgoing mail"
preferences.
   All the Windows MUAs need to be configured with a mail server.
Why?
```

How to compile Apache?

2)Users come to you and they will be saying mail server is very slow, what are the necessary steps you will take to resolve this issue?

3)Which are the configuration files associate with DNS server and client?

4)Where you will provide ISP details for your network?

5)How you will configure Squid proxy?

6)How you will block pron sites using Squid proxy?

7)Give me details how to configure mail support for NAGIOS?

8)Can you use NAGIOS to send SMS? how to do that?

9)What is web-min?

A) Webmin is a web-based system configuration tool for OpenSolaris, Linux and other Unix-like systems.

10)How you will do kernel compilation? Explain each step?

11)What is the difference between SGID, SUID and sticky bit?

12)How to restrict users to set password with complexity ?

13)How do you monitor system performance?

14)Which are the configuration files of FTP server?

15)What are the different types of FTP servers?

16)What is the difference between active FTP and passive FTP?

17)How you will configure FTP in DMZ?

18)What is the use of htaccess file?

19)how do you configure website authentication for user logins?

20)Give me the steps to configure sendmail.

21)How to block particular network not to access my sendmail server?

22)How to send duplex/half duplex etc to the network card?

23)Can a web server have multiple ip add? if yes why? if no why?

24)How to configure multiple ip address for a web server?

25)What is the difference between VMWare and XEN?

)**XEN :** Xen is an open-source virtualization solution. The Xen hypervisor acts as a thin layer between the hardware and the operating system, allowing multiple virtual servers to run simultaneously on a single physical server. Each virtual server acts independently of the others, with its own allocated area of RAM and virtual disks.

VMware : VMware is a company that provides virtualization software for x86-compatible computers

26)Explain me the difference between ext2 and ext3

27)How do you configure route in Linux server?

28)How do you make routes permanent in Linux server?

29)Why you want to change your job?

31)what is the difference between soft link and hard link?

32)How to get info about the files which are not accessed from last 30days?

Q2) Write a command to find all of the files which have been accessed within the last 30 days.
A1) The Command is , find / -atime +30
A2) # find / -type f -mtime +30
A3) find / -type f -mtime -30
A4) find / -type f -atime -30 = accessed
find / -type f -ctime -30 = changed
find / -type f -ctime -30 = modified

Q3) How to schedule cron backup to run on 4th saturday of month??
A1) crontab -e
** ** ** ** /5
Q4) how to see unallocated hard disk space on linux
A1) simply type
cat /proc/partitions
A2) df -h /dev/devicename
device name could be hda,sda
Q5) find out what file systems supported by kernel?
A1) # fdisk /dev/hdx
option: t
it will show the supported FS in the kernel
A2) cat /proc/filesystems
will show all the file system types that the kernel can
handle currently. Be aware that kernel will load the
necessary modules automatically if it have, for a new file
system type present in a new device you plug into it and
then the output of the above command will vary.
A3) you can give following commands
#fdisk
then press t
this command will show all the file system with code
supported by the current linux kernel.
Q6) how do u extract files from iso cd images in linux?
A1) From ISO MAGIC
A2) mount -o loop
A3) mount -t iso9660 -o ro,loop=/dev/loop0 /home/ste/cd.iso /mnt/iso
Q7) how do u find remote machine operating system and version?
A1) XProbe
A2) by ssh to that machine then give command
#uname -r
A3) for OS,
cat /etc/issue and version, uname –r
Q8) how do you port scaning with netcat command?
A1) nc -z
Q9) how do find all failed login attempts via ssh?
A1) check network connectivity check correct ipaddress
ping ipaddress
A2) 'who' or 'w' is the command used to find the users who logged in
The system and their attempts, with the help of some options
A3) Failed ssh logs are either written in /var/log/messages, or
/var/log/secure (configurable in /etc/syslog.conf). I am
assuming that the failed login attempts are recorded in
/var/log/secure:
grep ' authentication failure' /var/log/secure | sed -e
's/^\(.*\)\(rhost.*\)$/\2/p' | tr -s " " | cut -f2 -d"=" |
cut -f1 -d" " | sort -n | uniq -c
Will show you the count, and the IP/hostname of machines that tried
to access the system via ssh
A4) The command is ,
cat /var/log/messages | grep "Failed password"

it will show all the user which is not able to login.
Q10) How do display error messages instantly when command fails?
A1) Suppose you are trying to cat a non existing file:
cat /etc/shado 2>/dev/null || echo “Failed to open file”
command 2 "echo" is executed only if command 1 "cat" returns
a non-zero exit status
cat /etc/shado 2>/dev/null || echo "Failed to open file"
Failed to open file
#
Q11) How do find hard disk revolutions speed?
A1) A typical desktop hard disk rotate at 7,200 revolutions per
minute (RPM). A typical server hard disk spin at 10,000 or
15,000 rpm to achieve sequential media transfer speeds. You
can use hard disk model number to obtain disk RPM. For
example, a typical Seagat disk Model # ST373455SS can
provide following information:
* ST - Brand identity
* 3 - Form Factor (3 = 3.5")
* 73 - Disk size / Capacity in GB i.e. 73GB
* 4 - Reserved for future use
* 5 - RPM (5 = 15k and 0 = 10K)
* 5 - Generation
* SS - Indicates interface i.e Serial Attached SCSI
How do I find out hard disk model and serial number?
Use any one of the following command from shell prompt to
find out hard disk model number:
$ cat /proc/scsi/scsi
OR use scsi_id command to querys a SCSI device via the SCSI
INQUIRY vital product data (VPD) page 0x80 or 0x83 and uses
the resulting data to generate a value that is unique across
all SCSI devices that properly support page 0x80 or page 0x83.
$ /sbin/scsi_id -g -p 0x80 -s /block/sdd
OR
$ sudo grep -i sdd /var/log/boot.log
OR use sginfo / scsiinfo command from sg3_utiles package, enter:
sginfo -a /dev/sdd | more
Q12) when zombie process fully cleared?
A1) When the server gets restarted!
A2) Do a ps and identify the zombie processes
ps -el | grep 'Z'
Occasionally, these processes are in such a state that the
only way to get rid of them is to reboot to clear them.
In most cases, you can get rid of a zombie by normal means,
"kill -15 zombie PPID", "kill -9 zombie PPID".
Q13) how do you configure linux system as a router?
A1) Give the following command
echo 1 > /proc/sys/net/ipv4/ip_forward
A2) above anwser also write,
but must me know this,
vi /etc/sysctl.conf
Controls IP packet forwarding

net.ipv4.ip_forward = 1
save &
sysctl –p
Q14) Which priority has the process?how do u view?
A1) nice command is used to find the priority
A2) Each process has a niceness value associated with it, which is what the kernel uses to determine which processes require more processor time than others. The higher the nice value, the lower the priority of the process. In other words, the "nicer" the program, the less CPU it will try to take from other processes; programs that are less nice tend to demand more CPU time than other programs that are nicer.
The priority is noted by a range of -20 (the highest) to 20 (the lowest). Using ps, you can see the current nice value of all programs:
ps axl
F UID PID PPID PRI NI VSZ RSS WCHAN STAT TTY TIME COMMAND
4 0 1 0 16 0 2648 112 - S ? 0:01 init [3]
1 0 2 1 34 19 0 0 ksofti SN ? 0:02 [ksoftirqd/0]
5 0 3 1 10 -5 0 0 worker S< ? 0:00 [events/0]
You can see that init has a nice value of 0, while other kernel tasks associated with PID 2 and 3 have a nice value of 19 and -5 respectively.
Typically, a program inherits its nice value from its parent; this prevents low priority processes from spawning high priority children
Q15) Any one example of uninteruptable sleeping process?
A1) init (PID 1)
Q16) how many limitations of under directories in ext2/3 linux file system?
A1) Ext2 Limits
==========
Max file size: 2-64 TiB
Max number of files: 10 raised 18
Max filename length: 255 characters
Max volume size: 16-32 TiB
Allowed characters in filenames: Any byte except NULL and '/'
Ext3 Limits
==========
Max file size: 2 TiB
Max number of files: Variable, allocated at creation time[1]
Max filename length: 255 bytes
Max volume size: 2 TiB – 16 TiB
Allowed characters in filenames: All bytes except NULL
Q17) what is a superblock ?
A1) A superblock is a record of the characteristics of a filesystem, including its size, the block size, the empty

and the filled blocks and their respective counts, the size
and location of the inode tables, the disk block map and
usage information, and the size of the block groups.
Q18) what is the command to check network interfaces in our system?
how to set etho to 10 full duplex speed?
A1) ifconfig, ifconfig -a, ip dev ls,
ethtool -s eth0 speed 10 duplex full
to watch the info on eth0 (mii-diag --watch eth0)
Q19) 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?
A1) 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 >
Q20) what is soft mount and hard mount? i have to make permanent
nfs mount permanent what shall i do?
A1) to make permanent nfs mount, write it into /etc/fstab
Server nfsmount mountpoint filesystem defaults 0 0
192.168.0.1 /var/ftp/pub /mnt nfs defaults 0 0
A2) This is a UNIX terminology as to what the client does when
it can't talk to an NFS Server. If you just mount a file
system without specifying hard or soft, the default is a
hard mount. Hard mounts are preferable because of the
stateless nature of NFS. If a client sends an I/O request to
the server (such as an ls -la), and the server gets
rebooted, the client will wait until the server comes back
on line. This preserves data transfers in the event of a
server failure. There are disadvantages to this, as a simple
mount request could hang. A soft link will return with an
error and fail. This kills the wait time, but can cause
problems with data transfers.
To make permanent nfs mount, the above answer is right
Q21) what is major and minor?
A1) Major number
==========
A number indicating which device driver should be used to
access a particular device. All devices controlled by the
same device driver have a common major device number.
Minor number
==========
A number serving as a flag to a device driver.The minor
device numbers are used to distinguish between different
devices and their controllers.
Eg:
ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 2008-09-04 08:28 /dev/sda1
rigel:~# ls -l /dev/sda2
brw-rw---- 1 root disk 8, 2 2008-09-04 08:28 /dev/sda2
You can see the major and minor device number (8,1) and

(8,2) in the ls listing for /dev/sdax
ls -l /dev/scd0
brw-rw---- 1 root cdrom 11, 0 2008-09-04 08:28 /dev/scd0
You can see the major and minor device number (11,0)in the
ls listing for /dev/scd0
Q22) what is the command to make a process to run in the
background from foreground?
A1) To make the command run in the background suppose the
Command is "command_name" then the syntax for the same will
be such as follows;
[root@neo root]# command_name &
Q23) 1.what is Kernel parameters?
2.how many cpu have use in your machine?
A1) Kernal parameters are nothing but all the parameters in
/etc/system hear we can edit according to our requrement.
to check the how many cpus in the machine jus type this command
#psrinfo
to check the cpu speec #psrinfo –v
A2) 1.kernel parameters
parameters provide mechanisms to adjust the functiong of linux kernel.
the sysctl command used to view kernel parameters.
2.simply type in root
cat /proc/cpuinfo
Q24) 1.I want to change runlevel but the Users shall not be disturbed?how?
2.Disk have 5gb disk utilization even though files unable to reate, why?
3.what are the internal and external command in linux?
4.sar command o/p?
5.how list the open files?
6.what is kernel compiling?
7.How do u See complete configuration in ur system?
8.how will u make a daily updates with cron daily?
9.which port is associated with ttys0?
10.specific some problems linux admin(if u are linuxadmin)faced
And how did u overcome it?
A1) 1. For changing the runlevel you should have to go in
/etc/inittab. There you can change the runlevel what you
want.It will not affecting current user. After restarting
system your system will boot in which run level you have set.
3. Internel command means whichever command are builtin the
system BIOS. And External command means Which are
nonbuiltin.It outside the shell. It require shell.
4. VMstat & sar are showing the free memory of the system.
5. ls command is use list a file & cat & vi is to open a file.
6.
A2) 1) Same answer as above
2) Question not understood, may be ACLs
3) It is not BIOS,
A built-in (internal/resident) command is one that is
contained within the bash tool set and execute faster than
external commands.
An non-built-in (external/non-resident) command is a command

outside the shell and requires a $PATH (environmentvariable) to findit.
4)Displays the activity for the CPU
sar
Linux 2.6.18-6-686 (server.domain.local) 09/16/2008
11:31:56 AM LINUX RESTART
5) # lsof
6)The Linux kernel is a complex program which provides the
underlying services to the rest of a Linux distribution. But
it is easy to add new features or improvements to it,
requiring a kernel recompiling. There are three reasons for
a kernel compile. Firstly, you may have some hardware that
is so new that there's no kernel module for it in on your
distribution CD. Secondly, you may have come across some
kind of bug which is fixed in a revision of the operating
system. Lastly, you may have some new software which
requires a newer version of the operating system.
7)A vague question
8) Suppose we have a daily update script called dailyupdate.sh
Copy the script to /etc/cron.daily/
cp dailyupdate.script /etc/cron.daily/
Make the file executable
chmod +x /etc/cron.daily/dailyupdat.sh
9) COM1
10) Depends...
A3) 4) Detailed sar output
Linux 2.6.18-6-686 (server.domain.local) 09/16/2008
11:31:56 AM LINUX RESTART
11:35:01 AM CPU %user %nice %system
%iowait %steal %idle
11:45:01 AM all 0.71 0.00 0.19
0.18 0.00 98.92
11:55:02 AM all 1.53 0.00 0.19
0.26 0.00 98.02
Average: all 1.12 0.00 0.19
0.22 0.00 98.47
A4) 1. use init , at runtime.
2. disk quota has been set and reached for the current user.
3. same as above
4. same as above
5. same as above
6. lay man definition, adding support for required hardware
and modules in the Linux kernel.
7. sysreport, question too generalized,
8. same as above
9. same as above
10. :)
Q25) what is user mode & kernel mode?
A1) KERNEL-MODE
The kernel-mode programs run in the background, making sure
everything runs smoothly - things like printer drivers,
display drivers, drivers that interface with the monitor,

keyboard, mouse, etc. These programs all run in such a way that you don't notice them.
When the computer boots up, Windows calls the KERNEL, the main kernel-mode program that allows all the other programs to run, even the user-mode programs.
USER-MODE
These are the programs that you run when you want specific programs - e.g., MS Paint, MS Word, and Calculator. These are heavily restricted, as to not crash the system. Windows uses memory-protection services offered by the processor to prevent malicious programs from interfering with the rest of the system and corrupting it.
A2) A process can run in two modes:
1.User Mode.
2.Kernel Mode.
1.User Mode:
=>A mode of the CPU when running a program.
=>In this mode ,the user process has no access to the memory locations used by the kernel.When a program is running in User Mode, it cannot directly access the kernel data structures or the kernel programs.
2.Kernal Mode:
=>A mode of the CPU when running a program.
=>In this mode, it is the kernel that is running on behalf of the user process and directly access the kernel data structures or the kernel programs.Once the system call returns,the CPU switches back to user mode.
When you execute a C program,the CPU runs in user mode till the system call is invoked.In this mode,the user process has access to a limited section of the computer's memory and can execute a restricted set of machine instructions.however,when the process invokes a system call,the CPU switches from user mode to a more privileged mode the kernel. In this mode ,it is the kernel that runs on behalf of the user process,but it has access to any memory location and can execute any machine Instruction. After the system call has returned,the CPU switches back to user mode.
A3) KERNEL-MODE
Kernel mode, also referred to as system mode, is one of the two distinct modes of operation of the CPU in Linux. 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 (i.e., locations in memory). The kernel (which is the core of the operating system and has complete control over everything that occurs in the system) is trusted software, but all other programs are considered untrusted software.
USER-MODE
User mode is the normal mode of operating for programs, web browsers etc. They don't interact directly with the kernel,

instead, they just give instructions on what needs to be done, and the kernel takes care of the rest. Kernel mode, on the other hand, is where programs communicate directly with the kernel. A good example of this would be device drivers. A device driver must tell the kernel exactly how to interact with a piece of hardware, so it must be run in kernel mode. Because of this close interaction with the kernel, the kernel is also a lot more vulnerable to programs running in this mode, so it becomes highly crucial that drivers are properly debugged before being released to the public

Q26) what is the diff b/w ext2 and ext3?

A1) ext3 is the advanced version of ext2
ext2+journaling=ext3
this journaling feature is very much useful while retrieving data and writing data into a File System
Latest versions of all Linux flavors are coming with ext3 compatible file systems.

A2) ext 2 & ext3 are the two file systems in linux.ext 2 will take more time while logon the system. this is bcoz ext2 will check all harddisk peripherals at the time of switch on your sytem. But ext3 is less time consuming,bcoz instead of checking all harddisk peripherals it will check only the bootloader peripherals.

Q27) what is initrd image?

A1) initrd image is the initial ram disk image While the system getting booted the kernel image will get loaded into the main memory after POST to improve I/O performance.this initrd image will contain the same version number of kernel and if we face any error in booting regardingthis initrd we can reinstall it with 'mkinitrd' command

A2) initial RAM disk (initrd) is a temporary root file system that is mounted during system boot to support the two-state boot process. The initrd contains various executables and drivers that permit the real root file system to be mounted, after which the initrd RAM disk is unmounted and its memory freed. In many embedded Linux systems, the initrd is the final root file system

A3) initrd image is a image file which has initial modules which are loaded in to the kernel while booting.

Q28) what is jumbi process? Oracle

A1) its a dead process it's parent process has been killed abruptly.

A2) zoombie process or defunct process. - Process that finish execution
Or we can say the process died but still it has entry in the process table.
A process finished execution but parent of that process is Not ready to accept the exit status from it . At that time process go to zoombie state.

Q29) My machine is running half duplex mode how to change half duplex to full duplex? ORACLE

A1) [root@ns2 ~]# mii-tool -V
mii-tool.c 1.9 2000/04/28 00:56:08 (David Hinds)
eth0: negotiated 100baseTx-FD flow-control, link ok

[root@ns2 ~]# ethtool -s eth0 duplex half autoneg off
[root@ns2 ~]# mii-tool -V
mii-tool.c 1.9 2000/04/28 00:56:08 (David Hinds)
eth0: 100 Mbit, half duplex, no link
[root@ns2 ~]# mii-tool -V
mii-tool.c 1.9 2000/04/28 00:56:08 (David Hinds)
eth0: 100 Mbit, half duplex, link ok
Q30) some one is asking my machine is slow what is your steps? ORACLE
A1) The increase in the size of SWAP partition may show you the
little effect in increasing the system speed and better run
in Single user mode rather than GUI mode
A2) use top command, then check which process use the most
resource and find the problem.
A3) Re-read all process
#killall –HUP
Q31) what is mean by system calls INFOTECH
A1) 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.
Q32) What is trusted/untrusted operating system
A1) As per my perspective , I used to say any/all UNIX flavors
rather than MS WINDOWS
Because of
1. File/Directory permission (Action:Read/Write/Execute,
permissions can be given on behalf of the particular
User/group/Others).
2. All the unix configuration as files rather than
Registry (windows)
a. which cause the application to fail when a newer
or incompatible dynamic library is installed.
b. Some times you may need to restart the entire
system to update the changes with registry.
3. Linux Strong password protection. It won't get booted
(Drop you @ the GUI) without the successful
authentication (even though you don't have any more
users rather than admin/root).In Linux setting
password to the admin/root users is must during the
installation itself.
Where as in windows, let allow you to leave the
password as blank for admin/other user, System also
booting without authenticating.
4. Linux is open source, free under GNU. It doesn't mean
that its only free to install or use, but in fact you
can have these source codes and they are allowing you
to change it and redistribute it.

Windows is Lincesed os. Windows is developed by Microsoft.
5. Linux is more secure, windows is less secure than linux in case of virus, worms.
Because in Linux all the files/directory won't get executable permission, Perhaps you need to set it manually. Though by default all the incoming trojen, virus, malwares and worms won't affect the system.
6. Distribution
Linux : Linux has many distributors like Radhat, mandrake, Corel etc
Windows : whereas windows has only Micrsoft.
7. Run Level
Linux works on both GUI & Console mode (Checkout the various run levels runlevel 0 - runlevel 6 Generally known as init level)).
Windows : Only GUI.
8. By default LINUX have multiuser, multitasking, multiprocessing, multiprogramming features. Perhaps this will not be available on windows(Except some versions), In that case you need to PAY & BUY the extra features in windows.
9. You can play around the Linux through LIVE CDS on a Windows machine.
Only is a live CD that runs over windows, in RAM, and doesn't change your system at all..the other is an install disk. I've used the live CD on two XP machines and they both ran flawlessly. When you want to quit, just go to logout under system tools, and shut down.
Linux will turn itself off, eject the disk, and turn of your PC.
Remove the disk, boot up, and you're running your Windows again.
This is the way we are checking the newly bought NIC/others hardwares support with all the Linux distributors. Once it got detected, its very easy to get the device driver names and other details about that new hardwares, then compile the new kernel image (bzImage) on your own build version systems.
Q33) Working in Linux/Unix platform, if any command dose not work, say # ls reports as command not found.
what to do? GOOGLE
A1) Need to check the path first body ....
A2) reinstall that shell
A3) Check whether PATH variable as got the entry /bin
It should be something like this
==========
[root@bc ~]# echo $PATH
/usr/kerberos/sbin:/usr/kerberos/bin:/bin:/sbin:/usr/bin
==========

Q34) in unix how to change old name to new name
A1) mv // for rename the file in the same
directory
mv // for rename and
move the file in other diretory.
A2) 1. open the file /etc/sysconfig/network and change the
parameter HOSTNAME= to new name.
2. restart the network services.
3. open the file vi /etc/hosts, and change the old name to
new name.
127.0.0.1 localhost.localdomain
localhost
A3) mv
eg:-
[root@localhost]# touch file1 //created a file named file1
root@localhost]# ls //displays the file created
file1
[root@localhost]# mv file1 file2 //command to rename file1
[root@localhost]# ls //displays the renamed file
file2
A4) see there is no rename command in unix ,
so what u can use is "move" (mv) command
mv "(absolute path) old file name" "new file name
A5) rename
Q35) what is the standard output in a file as well as disply it
on the terminal options like
A)pr B) tail C) tee D)nl
A1) tail as it display ten current line
tail -f
option with this
tail -f -n 100
A2) I think, framing the question should be like
"What is the command used to write to the standard output
as well as to a file simultaneously ?
Answer) tee
It is a command that deals with pipes in unix. It
redirects the output of a command to an other command and
at the same time it redirects to a file also.
Q36) what is command like " #(cd unixos; pwd) " tell me OUTPUT
A1) first it will change the directory to unixos and then gives
the output as //unixos
A2) it is two commands runnung one by one.first the cd unixos
command will be executed,then the present working directory
will work.so the output will be showing the presentworking
dirctory that is unixos dir.
A3) WRONG when I hit this command no output or error is printed
Q37) in unix how to change old name to new name

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?

1) How to creat swap if you dont have free partation?

this is some what tricky question if you are new to Linux Administration

here is the command to create swap if you dont have free partation

before doing this you have switchoff the swap

swapoff -a

dd if=/dev/zero of=/root/swapfile bs=1k count=1024

swapon filename

2)How to see swap details?

cat /proc/swap

free

3)How to see/get info about RAM in ur system

free

cat /proc/meminfo

4)What is the difference between ext2 and ext3

I)ext3=ext2+journaling

"journaling" is an add-on to a filesystem that records changes as they are made.

II)ext2 files system is fast

III)less disk writes

IV)ext2 file system in less stable/secure

V)ext2 file system required to run fsck command if the system get crashed

5)How to convert ext2 file system to ext3?

tune2fs -j /dev/hda1

6)How convert ext3 file system to ext2

tune2fs -O^has-journal /dev/hda1

7)What is default block/chunk size for PV

4MB

8)what is the command to update the diskquota on file system

mount -o remount,rw /home

9)What is the partation type number for swap,RAID,LVM?

82(swap),fd(RAID),8e(LVM)
2)Can we install HPUX((Hewlett Packard UniX) on Vmware?
A)No. Because HPUX can be installed only on PA-RISC or Itanium and Vmware can not emulate this hardware
)What is the difference between IPchains and IPtables?
IPchains : Ipchains is a utility for Linux that System Administrators can use to create and modify the ruleset that is used for their host based firewall. These rules are used by a system to decide whether or not it is going to allow a specific remote connection.
IP tables : Iptables is a generic table structure that defines rules and commands as part of the netfilter framework that facilitates
What is INODE limit? If the file system reaches that limits how to resolve that?
A)Inode is a unique number given to a file in Unix OS. Every file in Unix has a inode number. unix treats directories/folders as a file so they are also having a inode value.
12)How to extend LV(Louis Vuitton)?
13)How to see how many VG's are there?
14)Explain the process of configure Apache.
15)How many types of chains are there in IPtables and what are they explain each?
16)What is super block?
17)What is INODE limit? If the file system reaches that limits how to resolve that?
A)Inode is a unique number given to a file in Unix OS. Every file in Unix has a inode number. unix treats directories/folders as a file so they are also having a inode value.
18)What are ACL's in Linux how to implement it in Linux?
19)How to take backup to Tape-drives?
20)How to rectify if tape drive file(hardware file) is missing?
21)What is the difference between RAID01 and RAID10?
22)When using RAID in which cases will you use RAID1 and which cases you will use RAID5?
23)How to implement password less SSH logins?
24)How a user can change a password?
25)How can you get info that my last command executed properly?
)How do you find out what's your shell? - echo $SHELL
2)What's the command to find out today's date? - date

3)How do you find out the current directory you're in? - pwd
4)How do you find out your own username? - whoami/who am i
5)How do you send a mail message to somebody? - mail surendra.anne@gmail.com -s 'Your subject' -c 'test@gmail.com'

6)What's the command to find out users on the system? - who/users
7)How do you remove a file? - rm
8)How do you remove a - rm -rf
9)How do you count words, lines and characters in a file? - wc
10)How do you search for a string inside a given file? - grep string filename

11)How do you search for a string inside a directory? - grep string *
12)How do you search for a string in a directory with the subdirectories recursed? - grep -r string *

13)What are PIDs? - They are process IDs given to processes. A PID can vary from 0 to 65535.
14)How do you list currently running process? - ps
15)How do you stop a process? - kill pid

16)How do you find out about all running processes? - ps -ag
17)How do you stop all the processes, except the shell window? - kill 0
18)How do you fire a process in the background? - ./process-name &
19)How do you refer to the arguments passed to a shell script? - $1, $2 and so on. $0 is your script name.
20)What's the conditional statement in shell scripting? - if {condition} then … fi

21)How do you do number comparison in shell scripts? - -eq, -ne, -lt, -le, -gt, -ge
22)How do you test for file properties in shell scripts? - -s filename tells you if the file is not empty, -f filename tells you whether the argument is a file, and not a directory, -d filename tests if the argument is a directory, and not a file, -w filename tests for writeability, -r filename tests for readability, -x filename tests for excitability
23)How do you do Boolean logic operators in shell scripting? - ! tests for logical not, -a tests for logical and, and -o tests for logical or.
24)How do you find out the number of arguments passed to the shell script? - $#
25)What's a way to do multilevel if-else's in shell scripting? - if {condition} then {statement} elif {condition} {statement} fi

26)How do you write a for loop in shell? - for {variable name} in {list} do {statement} done
27)How do you write a while loop in shell? - while {condition} do {statement} done
28)How does a case statement look in shell scripts? - case {variable} in {possible-value-1}) {statement};; {possible-value-2}) {statement};; esac
29)How do you read keyboard input in shell scripts? - read {variable-name}

1. **What is sed?** - sed is **s**tream **ed**itor, a Unix tool for working with streams of text data. See the awful truth about sed.

2. **How do you substitute strings with sed?** - Use 's/old/new' command, so sed 's/hello/goodbye/' would substitute the occurrence of the word hello to goodbye.

3. **How do you inject text with sed?** - & in the substitution string defines the pattern found in the search string. As an example, here's us trying to find a word 'hello' and replacing it with 'hello and how are you':
   echo 'hello there' | sed 's/^hello/& and how are you/'

4. **Can I find several patterns and refer to them in the replacement string**? - Yes, use (pattern) and then refer to your patterns as \1, \2, \3 and so on.

5. **If the string is 'old old old' and I run 's/old/new', I get 'new old old' as the result. I need 'new new new'**. - You forgot the global modifier, which would replace every occurrence of the pattern with the substitution. 's/old/new/**g**' will work.

6. **But I want 'old old new' from the previous example**. - Just use the numeric modifier saying you want the third occurrence to be replaced. 's/old/new/**3**' will work.

7. **I wrote a rather complex sed script. How do I save and run it**? - Assuming that your file is named myscript1.sed, you can invoke sed -f myscript1.sed.

8. **How do I delete trailing whitespaces from each line**? - sed 's/[\t]*$//' Here we're replacing any occurrence of a space or a tab with nothing. Check sed one-liners for more examples.

9. **How do you print just a few first lines of the file**? - sed 1q will give you just the first line, sed 10q the first 10 lines.

10. **How do you replace a pattern only if it's found, so that it's executed faster**? - Nest the replacement statement: sed '/old/ s/old/new/g' file.txt

What is LILO?

LILO stands for Linux boot loader. It will load the MBR, master boot record, into the memory, and tell the system which partition and hard drive to boot from.

What is the main advantage of creating links to a file instead of copies of the file?

A: The main advantage is not really that it saves disk space (though it does that too) but, rather, that a change of permissions on the file is applied to all the link access points. The link will show permissions of lrwxrwxrwx but that is for the link itself and not the access to the file to which the link points. Thus if you want to change the permissions for a command, such as su, you only have to do it on the original. With copies you have to find all of the copies and change permission on each of the copies.

what is the command for finding the higest memory occupied file in linux? Top command will show the memory occupied by a file.When top is showing the output press shift+m to show the file or process which is using larger memory.

difference between nfs soft and hard mouniting points?

hard mount option:- If the client fails to access the server,then connection hang it, after the system up then it access the server.

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

Hard mounting : Providing entry in /etc/fstab is called hard mounting. Using hard mounting when client system boots at booting time client will try to mount the entry in /etc/fstab if the server is down client pc willnot boot until the server is up. mounting at boot time is called hard mounting.

Soft mounting : Providing entry in /etc/auto.master and /etc/auto.misc is called soft mounting. When client sys boot it will try to mount if unable to mount just gives the error message and it will continue the boot process. Mounting at boot time or by user request is called soft mounting

in redhat Linux wat is the command to check at ahich date and time file was created?

stat filename

```
ls -ltr" gives you detail information of files and
```
directories.

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?

Netstat

```
cat /etc/services |grep udp
```
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 -I INPUT -s 172.168.0.1 -p tcp --dport 80 -d 192.168.0.2 -j
ACCEPT
```
how many limitations of under directories in ext2/3 linux file system?

```
Ext2 Limits
============
Max file size: 2-64 TiB
Max number of files:   10 raised 18
Max filename length:   255 characters
Max volume size:       16-32 TiB
Allowed characters in filenames: Any byte except NULL and '/'

Ext3 Limits
===========
Max file size: 2 TiB
Max number of files:   Variable, allocated at creation time[1]
Max filename length:   255 bytes
Max volume size:       2 TiB - 16 TiB
```
Allowed characters in filenames: All bytes except NULL

what are the linux boot files?

```
Grub.conf
2.Vmlinuz
```
3.initrd.img

```
soft mount is to mount for limited time or temporary,
whereas hard mount is mount permanently.
```

what is soft mount and hard mount? i have to make permanent nfs mount permanent what shall i do?

```
To make nfs permanent mount go to /etc/fstab & put the entry
& run a cmd to make it mount permanent #mount -a.
to make permanent nfs mount, write it into /etc/fstab
server<ip>    nfsmount   mountpoint  filesystem defaults 0 0
192.168.0.1  /var/ftp/pub   /mnt      nfs       defaults 0 0
```
how do find all failed login attempts via ssh?

```
tail -f /var/log/secure | grep Failed
 lastb" is the command to find all failed login attempts
```
how do u find remote machine operating system and version?

#nmap -A -v station1

what is the diff b/w ext2 and ext3?

```
ext3 is the advanced version of ext2
```

ext2+journaling=ext3
this journaling feature is very much useful while retrieving data and writing data into a File System
Latest versions of all Linux flavors are coming with ext3 compatible file systems.
ext 2 & ext3 are the two file systems in linux.ext 2 will take more time while logon the system. this is bcoz ext2 will check all harddisk peripherals at the time of switch on your sytem. But ext3 is less time consuming,bcoz instead of checking all harddisk peripherals it will check only the bootloader peripherals.
Availability
Integrity
Speed
easy transition

In ext2 filesystem, the filesystem is not mounted until its consistency is checked by e2fsck program. the amount of time taken to run e2fsck program is determined by the size of file system. The more files you have on the file system, the longer the consistency check takes.

ext3 does not require a file system check even after a unclean shutdown. the time to recover an ext3 file system after an unclean shutdown does not depend on size, rather it depends on size of "journal" used to maintain consistency.
the default journal takes about a second to recover.

What is an inode?

An inode is a data structure holding information about files in a Linux file system. There is an inode for each file, and a file is uniquely identified by the file system on which it resides and its inode number on that system.

what is the command to make a process to run in the background from foreground?

when the process is running, press "control+Z" . Now at the command prompt , type "bg"

what is a superblock ?

A superblock is a record of the characteristics of a filesystem, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups.

how do you configure linux system as a router?

vi /etc/sysctl.conf

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

save &

sysctl -p

1st answer is correct till you boot your Linux machine, once rebooted, its gone coz the /proc is a fs that is resident on memory, thus if you want to forward your packets permanently then you have to alter the net.ipv4.ip_forward parameter to reflect the changes each time machine is booted. # sysctl -p makes it effective without reboot.

follow following command

1.) vi /etc/sysctl.conf

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

save (:wq!)

You should have a Two physical LAN card, if You have't two Lan cat. You have to creat virtual Lan card

2.) cp -arvf /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth0:1

3.) Set a diffrent Class IP in virtual Lan card

4.) start network service

```
/etc/init.d/network restart
```

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 >

What u know abt tar Command?

tar command is file archiving cmd and extracting cmd in linux.

create

```
tar -cvf /tmp/ram.tar /etc/passwd
```

this command makes compress the /etc/passwd datas and stored in /tmp/ram.tar

Extract

```
tar -xvf /tmp/ram.tar
```

extract the data in existing file is /tmp/ram.tar

How do you read ext2/3 file system in windows?

Using Software Winscp ,we can access Linux machine from Windows.it is an windows software.
through SAMBA, we can share the linux partition or directory, for windows.

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

netstat -anpc

a:all listening ports and established connections
n:numeric host:port values
p:programs
c:continuous monitor

What is the status code 403,404 represented in apache server

403 represent forbidden error, means if files misses some selinux security context is missing.

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

Difference between swap partition and swap file?

Swap partition maintained seperate partition.
same swap partition can be used in two OS within single machine.
If system crashes their is a chance to recover itor may not be 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 system crashes their is a huge chance to lost the swap file system.

what is nis server?

Network Information Services is well known as NIS server which is based on Linux and Unix environment network. NIS Server create the user name and password to share across the network for centralize authentication. The best thing is that passwords can change be changed on NIS server not on client desktop systems.

How can I only see the first 14 lines of a file?

head -n14 filename

Compare between SYS V launched processes and Xinetd processes in Linux.

Answer is based on RHEL

SYS V processes	xinetd processes
1) daemons (run in background)	processes started on request
2) Managed by "service" wrapper command	Managed by "xinetd" daemon
3) Script files in "/etc/rc.d" directory	script files in /etc/xinetd.d directory

what is the command to make a process to run in the foreground from background?

Fg

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

specify the user in /etc/vsftpd/user_list.
then in /etc/vsftpd/vsftpd.conf ,add userlist_deny=NO,,,,
then restart d service..... set d selinux for the accessing home directory.....

what are the Linux-based security tools?

. Clam AntiVirus
It is an open source (GPL) anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways.

2. SpamAssassin
It is a computer program released under the Apache License 2.0 used for e-mail spam filtering based on content-matching rules.

3. Chkrootkit is a powerful tool to scan your Linux server for trojans

4. rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors and possible local exploits

what is a command to display top 10 users who are using Huge Space?

du -s /home/* | sort -nr |head -10

In which File is Static IP address given so that it becomes Permanent ?

just go to system-config-network

and type ip address
or

go
vi /etc/sysconfig/network-scripts/ifcfg-eth0

edit in this file it will become permanent.

what are the features of Linux?

The following feature of linux:-
Some of its features include:
1)Virtual memory, allowing the system to use disk room the same as RAM memory.

2)Networking with TCP/IP and other protocols.

3)Multiple user capability.

4)Protected mode so programs or user's can't access

5)unauthorized areas.

6)Shared libraries

7)True multitasking

8)X - A graphical user interface similar to windows, but supports remote sessions over a network.

9)Advanced server functionality:-
- FTP server
- Telnet server
- BOOTP server
- DHCP server
- Samba server
- DNS server
- SNMP services
- Mail services
- Network file sharing
- much, much more...

Support of filesystems that other operating systems use such as DOS (FAT), Windows95,98 (FAT32), Windows NT, 2000 (NTFS), Apple, minix, and others

some one is asking my machine is slow what is your steps?

The increase in the size of SWAP partition may show you the little effect in increasing the system speed and better run in Single user mode rather than GUI mode
use top command, then check which process use the most resource and find the problem.
Re-read all process
#killall -HUP
use ps aux command and check which process is using much space
and check is there any partition is going to be full disk check by df -HT command