1.What is the best RAID level?

RAID 0 for performance
RAID 5 for High availability
RAID 6 even better High Availability if the budget is fine

2.What is MAC address and How to check the MAC address in linux?

A mac address means media access control address.It is a unique address assigned to almost all networking hardware such as Ethernet cards, router etc.
Most layer 2 network protocols use one of three numbering spaces which are designed to be globally unique.

Linux Command to see MAC address:
Ifconfig is used to configure network interfaces.

```
$ /sbin/ifconfig grep HWaddr

Output: eth0 Link encap:Ethernet HWaddr 00:0F:EA:91:04:07
```

OR

```
$ /sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:0F:EA:91:04:07 <<< THIS IS THE MAC
ADDRESS
inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20f:eaff:fe91:407/64 Scope:Link
```

OR as a root user type following command:

```
# grep eth0 /var/log/dmesg

eth0: RealTek RTL8139 at 0xc000, 00:0f:ea:91:04:07, IRQ 18 <<< this line 2 component
from this side is MAC address
eth0: Identified 8139 chip type 'RTL-8100B/8139D'
eth0: link up, 100Mbps, full-duplex, lpa 0x45E1
```

3.how to assign a permanent IP to a client which is presently in DHCP in Linux?

```
/sbin/ifconfig eth0 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
```

In this command we are assigning 192.168.10.1 IP to ethernet interface(NIC card) eth0.

Also in redhat linux terminal you can type comand "setup" & launch a Wizard type interface in which u can choose network & configure IP

You can use the GUI tool /usr/bin/neat - Gnome GUI network administration tool. It handles all interfaces and configures for both static assignment as well as dynamic assignment using DHCP.

4. How to exclude some ip address range in DHCP?

To exclude the range of IP address in a subnet is to split the address range of subnet into two.

Example:

```
subnet 1.1.1.0 netmask 255.255.255.0
{
range 1.1.1.10 1.1.1.15
range 1.1.1.21 1.1.1.40
}
```

so in the above example automatically the IP 16-20 will be excluded from the list.

5.What is the default serial number of DNS ?

Are based on ISO dates. Every time the data in the database is changed, the serial number must be increased in order that the slave servers know the zone has changed

6.how to pull the data to the secondary nis server from master server?

ypxfr is a pull command which runs on each slave server to make that server import the map from master nis server

7.what file need to be changed in nis client if you are changing the machine from one subnetwork to other subnetwork?

/etc/yp.conf

8.how to see memory usage?

Commands "top" and "free -m"

9.how to increase the filesystem ?

Using command # fdisk

# As the system administrator you need to review Bob’s cronjobs. What command would you use? Choose one:

a. crontab -lu bob

b. crontab -u bob

c. crontab -l

d. cronq -lu bob

# In order to schedule a cronjob, the first task is to create a text file containing the jobs to be run along with the time they are to run. Which of the following commands will run the script MyScript every day at 11:45 pm? Choose one:

a. * 23 45 * * MyScript

b. 23 45 * * * MyScript

c. 45 23 * * * MyScript

d. * * * 23 45 MyScript

# Which daemon must be running in order to have any scheduled jobs run as scheduled? Choose one:

a. crond

b. atd

c. atrun

d. crontab

# You want to ensure that your system is not overloaded with users running multiple scheduled jobs. A policy has been established that only the system administrators can create any scheduled jobs. It is your job to implement this policy. How are you going to do this? Choose one:

a. create an empty file called /etc/cron.deny

b. create a file called /etc/cron.allow which contains the names of those allowed to schedule jobs.

c. create a file called /etc/cron.deny containing all regular usernames.

d. create two empty files called /etc/cron.allow and /etc/cron.deny

# You notice that your server load is exceptionally high during the hours of 10 am to 2 noon. When investigating the cause, you suspect that it may be a cron job scheduled by one of your users. What command can you use to determine if your suspicions are correct? Choose one:

a. crontab -u

b. crond -u

c. crontab -l

d. crond -l

# One of your users, Bob, has created a script to reindex his database. Now he has it scheduled to run every day at 10:30 am. What command should you use to delete this job. Choose one:

a. crontab -ru bob

b. crontab -u bob

c. crontab -du bob

d. crontab -lu bob

# What daemon is responsible for tracking events on your system?

# What is the name and path of the default configuration file used by the syslogd daemon?

# You have made changes to the /etc/syslog.conf file. Which of the following commands will cause these changes to be implemented without having to reboot your computer? Choose one:

a. kill SIGHINT `cat /var/run/syslogd.pid`

b. kill SIGHUP `cat /var/run/syslogd.pid`

c. kill SIGHUP syslogd

d. kill SIGHINT syslogd

# Which of the following lines in your /etc/syslog.conf file will cause all critical messages to be logged to the file /var/log/critmessages? Choose one:

a. *.=crit /var/log/critmessages

b. *crit /var/log/critmessages

c. *=crit /var/log/critmessages

d. *.crit /var/log/critmessages

# You wish to have all mail messages except those of type info to the /var/log/mailmessages file. Which of the following lines in your /etc/syslogd.conf file would accomplish this? Choose one:

a. mail.*;mail!=info /var/log/mailmessages

b. mail.*;mail.=info /var/log/mailmessages

c. mail.*;mail.info /var/log/mailmessages

d. mail.*;mail.!=info /var/log/mailmessages

# What is the name and path of the main system log?

# Which log contains information on currently logged in users? Choose one:

a. /var/log/utmp

b. /var/log/wtmp

c. /var/log/lastlog

d. /var/log/messages

# You have been assigned the task of determining if there are any user accounts defined on your system that have not been used during the last three months. Which log file should you examine to determine this information? Choose one:

a. /var/log/wtmp

b. /var/log/lastlog

c. /var/log/utmp

d. /var/log/messages

# You have been told to configure a method of rotating log files on your system. Which of the following factors do you not need to consider? Choose one:

a. date and time of messages

b. log size

c. frequency of rotation

d. amount of available disk space

# What utility can you use to automate rotation of logs?

# You wish to rotate all your logs weekly except for the /var/log/wtmp log which you wish to rotate monthly. How could you accomplish this. Choose one:

a. Assign a global option to rotate all logs weekly and a local option to rotate the /var/log/wtmp log monthly.

b. Assign a local option to rotate all logs weekly and a global option to rotate the /var/log/wtmp log monthly.

c. Move the /var/log/wtmp log to a different directory. Run logrotate against the new location.

d. Configure logrotate to not rotate the /var/log/wtmp log. Rotate it manually every month.

# You have configured logrotate to rotate your logs weekly and keep them for eight weeks. You are running our of disk space. What should you do? Choose one:

a. Quit using logrotate and manually save old logs to another location.

b. Reconfigure logrotate to only save logs for four weeks.

c. Configure logrotate to save old files to another location.

d. Use the prerotate command to run a script to move the older logs to another location

```
> 1.  You have 20 servers that need to be updated named
[...]
> Ans:

Yours is woefully unportable. For starters, you can't rely on bash.
Second, you can't rely on GNU-specific tools like seq.

> for i in `seq -w 20`

If you're using bash, why add an extra shell invocation here?

for i in {01..20} should get the same effect in recent versions of
bash2.

> 2.  How do you findout whether a command is an aliases, bash function,
> built-in like cd and type, or executable program?
>
> Ans:
>
> type -all yourcmd

This is, again, bash-specific. All common shells support the use of
which (either by builtin or, in some cases, by which(1)), which
will answer the same question.

> 3.  What is a zombie process and how do you find them?
[...]
> ps -aux, will show all processes. Look for "Z" in that stat and defunct
> under the command.

That answer's incomplete; that's relying on BSD ps(1) syntax. On
Solaris, at least, you can use /usr/ucb/ps (though it's quite slow),
but on a true SysV system, you'll need to know how to read ps -ef
output as well.

Also, BSD ps(1) syntax has long deprecated the use of the -.

> 4.  How do you find the version of Linux running and the version of gcc
> used?
> Ans:
> cat /proc/version

Why would you give a Linux-specific question, much less answer, on a
```

test for a Unix sysadmin? The POSIX way to get this information is
uname(1).

> 5. How do you setup multiple IP address on one NIC (Network Interface
> Card)...assume ethernet.
>
> Ans:
> Normally,   /etc/sysconfig/network-scripts/ifcfg-eth0 is the setup for the
> first card. To add additional IP addresses, create another file
> "ifcfg-eth0:1" with the new IP address information in it.

That's disgustingly Linux-specific. BSD systems will use
/etc/ifconfig.<foo>

> 6. What is an inode?
>
> Ans:
> The inode contains information about the file size, file location,
> ownership, etc. Plus, it contains a pointer to the first few blocks of data
> in the file.

That's true, but it neglects the FS-dependent implementation details
(sysadmins should be familiar at least with the file systems they
need to manage, and should have a basic understanding of what design
decisions are made when designing a FS) and neglects to ask the
important "and why do you care?" piece of the question.

> 7. What's the difference between a hard link and a soft link?

Why do people use the term "soft link"? The correct term is
"symbolic link".

> Ans:

[...]

> fileA and fileB have the same inode. How do you know this? Issue the stat
> command "stat fileA" and "stat fileB".

stat(1) isn't defined in POSIX, but ls's -i flag is.

> One important note about hard links. Editors like emacs will create a new
> inode for a file. So if you edit the fileB above, you won't see the changes
> in fileA. Instead, that inode becames the backup.

That's a pretty irrelevant note, I think, unless you're interested
in the internal functionings of Emacs. A salient point you neglect
to mention is what kind of links one can make across file system
boundaries.

> 8. How do you create a file that even root can't remove?
>
> Ans:
> You't can't really; but, the "chattr +i file" command can make a file
> immutable. This file can't be removed until "chatt -i file" is performed.
> True, even root can't remove a file with the immutable attribute set. But,
> root can unset this attribute, then, delete the file.

chattr(1) isn't just Linux-specific, it's ext{2,3}-specific. Some other file systems provide other ways of doing this same thing.

The real answer to the question is that you create the file and then
set a physical read-only marker on the device itself (tabs on floppy
disks and tape media, jumpers on disk devices, ro=<hostname> in
dfstab/exports on an NFS server to which the root user in question
doesn't have access).

```
> 9. How do you find all the programs, and there location, using sockets or
                                             ^^^^^
> pipes on your computer?
```

Spellcheck is insufficient. Proofread.

> Ans:
> "netstat -na" will give a list of listening connections; but, it doesn't do
> an adequate job of listing the programs. Instead, use
> "lsof"

lsof is rather portable (in that it can be built on most, if not
any, POSIX systems), but many operating systems provide a native
mechanism for this. (BSD systems have fstat(1), for instance.)

> Other items to know: What is a superblock and what kind of data is in it?

More importantly, why would you need that information?

> If someone talks about ext2 and ext3 filesystems, what are they most likely
> running Debian or Redhat?

If someone talks about ufs, what are they most likely using, SunOS
or BSD/OS?

> Using the find command, how do you find all files
> with the immunitable attribute set?

GNU-find and ext{2,3}-specific.

> How do you create a directory that's sharable to a group,

A more general question would ask what attributes can be set in a
file's mode bits and which have special implications for files that
are directories or that are executable. One should also note that
certain popular file system implementations overload certain mode
bits; for example, Sun's ufs and, because of that, Veritas's vxfs.
Explaining which of these interactions will function across NFS
between same-OS servers and clients and different-OS servers and
clients would also be desirable.

> that by default, will have each file created as sharable to a group.

This presumes changes outside of the directory's mode bits. (You
need to force a umask on the users.)

> What's an effective UID and how is it set?

Relatedly, what's a saved UID, and why would you care about them?

> Is the speed of light constant in a vacuum and does light travel in a straight line? Careful on this last one..don't let your formal education throw you off.

Heh.

On Sat, Feb 14, 2004 at 11:43:54AM -0500, Chris wrote:

> Are these questions supposed to be focused on a low end admin? Or a high position admin?

The former, we certainly hope, though my experience dictates that people referring to themselves as senior couldn't answer some of the modifications I made above.

I've attached an incomplete list of questions I would ask in an interview for a senior Unix and Linux systems administrator. These are based on a list of questions a friend of mine who prefers to remain anonymous asked for my feedback on recently. I've made some modifications to that person's questions and would prefer to make some significant additions before I made use of this list. (My friend also had questions specific to Windows 2000; I've ellided those here, but if you'd like to see them, let me know.)

There's a significant lack of file-system-related questions here, which I pointed out to my friend at the time. The questions Mike provided above aren't a bad starting point for that component of this list.

My friend's and my questions:

Sysadmin Quiz

TCP/IP Networking

- In an IP network, what is the function of a subnet mask?
- Suppose you are assigned the CIDR netblock 130.78.25.64/28.
  - How many IP addresses are useable for hosts?
    - List them.
  - Are there any IP addresses that are not useable for hosts?
    - If so, list them with the reason that that specific address is not useable for hosts.
- The default gateway address on a subnet is changing; the old address is 192.168.0.254, and the new address is 192.168.0.1. What changes would you need to make on a computer running as a DHCP server on that subnet? (The DHCP server is not acting as the gateway for this network, and the system acting as the gateway is not receiving its IP address from the DHCP server. Assume whatever operating system and DHCP server software you're familiar with, though answers for a POSIX operating system and ISC dhcpd are preferred.)
- ping(1) reports "Request timed out" when trying to check connectivity to a host, but you're able to access other services running on the same system. Give at least one possible explanation for this.
- What should be found in the /etc/hosts file? (If your answer is specific to any particular OS, please state that. More specific answers are preferred to more general ones.)
  - Sketch a brief history of the usage of this file in the Unix

operating system(s).

- What is found in a DNS zone file? (Assume BIND running on a POSIX operating system.)
- What is the purpose of an MX record?
  - What data is permissable in a standards-compliant MX record? (Also accepted: what standards-non-compliant data is frequently placed in MX records?)
- What data is transferred in a DNS zone transfer?
  - In what circumstances would you permit systems outside of your local/corporate network to perform DNS zone transfers?
  - In what circumstances would you not?

E-Mail

- Explain in what ways each of the IMAP, POP3, and SMTP protocols are used.
  - Give at least two differences between IMAP and POP3.
  - Explain at least one way that SMTP is used that does not involve a mail user agent. (Bonus points for creative answers.)
- What is an open mail relay?
  - How would you test an SMTP server to see if it is an open mail relay?
  - Name at least two types of server process that can be an open mail relay but are not SMTP server processes.
- What are the basic commands to send a message to an SMTP server? (Hint: Begin with HELO.)

OS-level Tools

- What options to (GNU) tar(1) would you use to decompress and extract everything from an archive named files.tar.gz into the current directory?
- How would you move a user's home directory from one mounted disk partition to another, preserving all file metadata, with minimal interruption to the user?
  - Can you do this with zero interruption to the user?
- What command would you use to check available disk space on all currently-mounted disk partitions?
- What command(s), with what options, would you use to discover which directory under a given disk partition was using the most space?
- Why is there an /etc/shadow (or similar, differently-named) file? What is in it, and how is it different from /etc/passwd?

I'll leave the answers as an exercise for the reader, since you should know these things by having learned them, not by having read a cheat-sheet.

--
gabriel rosenkoetter
gr@eclipsed.net

> Sysadmin Quiz TCP/IP Networking - In an IP network, what is the function of a subnet mask? - Suppose you are assigned the CIDR netblock 130.78.25.64/28. - How many IP addresses are useable for hosts? - List them. - Are there any IP addresses that are not useable for hosts? - If so, list them with the reason that that

| specific address is not useable for hosts. - The default gateway
| address on a subnet is changing; the old address is 192.168.0.254,
| and the new address is 192.168.0.1. What changes would you need to
| make on a computer running as a DHCP server on that subnet? (The
| DHCP server is not acting as the gateway for this network, and the
| system acting as the gateway is not receiving its IP address from
| the DHCP server. Assume whatever operating system and DHCP server
| software you're familiar with, though answers for a POSIX operating
| system and ISC dhcpd are preferred.) - ping(1) reports "Request
| timed out" when trying to check connectivity to a host, but you're
| able to access other services running on the same system. Give at
| least one possible explanation for this. - What should be found in
| the /etc/hosts file? (If your answer is specific to any particular
| OS, please state that. More specific answers are preferred to more
| general ones.) - Sketch a brief history of the usage of this file
| in the Unix operating system(s). - What is found in a DNS zone
| file? (Assume BIND running on a POSIX operating system.) - What is
| the purpose of an MX record? - What data is permissable in a
| standards-compliant MX record? (Also accepted: what
| standards-non-compliant data is frequently placed in MX records?) -
| What data is transferred in a DNS zone transfer? - In what
| circumstances would you permit systems outside of your
| local/corporate network to perform DNS zone transfers? - In what
| circumstances would you not? E-Mail - Explain in what ways each of
| the IMAP, POP3, and SMTP protocols are used. - Give at least two
| differences between IMAP and POP3. - Explain at least one way that
| SMTP is used that does not involve a mail user agent. (Bonus points
| for creative answers.) - What is an open mail relay? - How would
| you test an SMTP server to see if it is an open mail relay? - Name
| at least two types of server process that can be an open mail relay
| but are not SMTP server processes. - What are the basic commands to
| send a message to an SMTP server? (Hint: Begin with HELO.) OS-level
| Tools - What options to (GNU) tar(1) would you use to decompress
| and extract everything from an archive named files.tar.gz into
| the current directory? - How would you move a user's home
| directory from one mounted disk partition to another, preserving
| all file metadata, with minimal interruption to the user? - Can you
| do this with zero interruption to the user? - What command would
| you use to check available disk space on all currently-mounted disk
| partitions? - What command(s), with what options, would you use to
| discover which directory under a given disk partition was using the
| most space? - Why is there an /etc/shadow (or similar,
| differently-named) file? What is in it, and how is it different
| from /etc/passwd?
|

Here's a list of common interview questions that I've come across.

1. You have 20 servers that need to be updated named server01,server02...server20. Write a bash script to update all the computers, assuming they all use ssh, with the account bozo.

Ans:

```
 #!/bin/bash
```

```
user="bozo";
updatecmd="ls -l"; # put in rpm command here
errorfile="updatelog";
for i in `seq -w 20`
do
        ssh "${user}@server$i" $updatecmd || echo "Error on server $i >>
$errorfile";
done
```

The command seq -w 20 pads with the necessary zeros (01,02,03...09). The || executes only the left side on success. However, if the ssh fails, the right side is executed and an error message to piped to the file.

2. How do you findout whether a command is an aliases, bash function, built-in like cd and type, or executable program?

Ans:

```
type -all yourcmd
```

3. What is a zombie process and how do you find them?

Ans:

When a process creates a child process "fork() command" and that child process terminates, information about the child process (CPU time, memory, etc.) exists for the parent to fetch. The parent can use the "wait" or "waitpid" to fetch this signal. The child process becomes a zombie as soon as it finishes; but, the SIGCHLD hasn't been caught.

ps -aux, will show all processes. Look for "Z" in that stat and defunct under the command.

Note: wait may still produce zombies. This can happen of child A terminates, and it's signal has been caught. While this signal is being process child B terminates. Since these signals won't queue, child B could stay in the zombie state. It's safer to use the waitpid call.

4. How do you find the version of Linux running and the version of gcc used?

Ans:

```
cat /proc/version
```

5. How do you setup multiple IP address on one NIC (Network Interface Card)...assume ethernet.

Ans:

Normally, /etc/sysconfig/network-scripts/ifcfg-eth0 is the setup for the first card. To add additional IP addresses, create another file "ifcfg-eth0:1" with the new IP address information in it.

6. What is an inode?

Ans:

The inode contains information about the file size, file location, ownership, etc. Plus, it contains a pointer to the first few blocks of data in the file.

7. What's the difference between a hard link and a soft link?

Ans:
hard link is created by the following command

```
$ln fileA fileB
```

fileA and fileB have the same inode. How do you know this? Issue the stat command "stat fileA" and "stat fileB".

soft link is created by the following command

```
ln -s fileA fileC
```

Here fileC has a different inode than fileA. However, this "different inode" points to the same data as fileA.

One important note about hard links. Editors like emacs will create a new inode for a file. So if you edit the fileB above, you won't see the changes in fileA. Instead, that inode becames the backup.

8. How do you create a file that even root can't remove?

Ans:
You't can't really; but, the "chattr +i file" command can make a file immutable. This file can't be removed until "chatt -i file" is performed. True, even root can't remove a file with the immutable attribute set. But, root can unset this attribute, then, delete the file.

9. How do you find all the programs, and there location, using sockets or pipes on your computer?

Ans:
"netstat -na" will give a list of listening connections; but, it doesn't do an adequate job of listing the programs. Instead, use
"lsof"

10. How do you create directory and subdirectories when the parent directory may exist, in one command? In other words, create the following directory structure.
/home/user/one/two
The command should work whether /home/user exists or not.

Ans:
mkdir -p /home/user/one/two The -p or "parents" makes the parent directory as needed.

Personal note: You want interviewers to ask good questions. If you get the job it's a sign you'll be working with knowledgeable people. And, if you don't get the job, you'll at least learn from the interview process.

Other items to know: What is a superblock and what kind of data is in it? If someone talks about ext2 and ext3 filesystems, what are they most likely running Debian or Redhat? Using the find command, how do you find all files with the immunitable attribute set? How do you create a directory that's sharable to a group, that by default, will have each file created as sharable to a group. What's an effective UID and how is it set? How do you pass and use a command variable to an awk script? How can you easily print quotes in an awk script? Using a sed script print only the data betwee "<start>.....</start>" in a file. How do you keep cron jobs from sending mail on output? How do you create a C like for loop in Bash? How do you find the length of an array in bash? Using the find command how do you find directory names that "do not contain" a particular file? Is the speed of light constant in a vacuum and does light travel in a straight line? Careful on this last one..don't let your formal education throw you off.

Regards,

Mike Chirico

1. How are devices represented in UNIX?

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

2. What is 'inode'?

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

Inode consists of the following fields:

- File owner identifier
- File type
- File access permissions
- File access times
- Number of links

- File size
- Location of the file data

3. Brief about the directory representation in UNIX

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

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

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

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

5. How do you change File Access Permissions?

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

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

(user permission-group permission-others permission)
r-read, w-write, x-execute
To change the access mode, we use chmod(filename,mode).

Example 1:

To change mode of myfile to 'rw-rw-r–' (ie. read, write permission for user - read,write permission for group - only read permission for others) we give the args as: chmod(myfile,0664) .

Each operation is represented by discrete values

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

Therefore, for 'rw' the value is 6(4+2).

Example 2:

To change mode of myfile to 'rwxr–r–' we give the args as:

```
chmod(myfile,0744).
```

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

A link is a second name (not a file) for a file. Links can be used to assign more than one name to a file, but cannot be used to assign a directory more than one name or link filenames on different computers.

Symbolic link 'is' a file that only contains the name of another file.Operation on the symbolic link is directed to the file pointed by the it.Both the limitations of links are eliminated in symbolic links.

Commands for linking files are:

```
Link ln filename1 filename2
Symbolic link ln -s filename1 filename2
```

7. What is a FIFO?

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

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

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

9. Discuss the mount and unmount system calls

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

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

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

11. What is a shell?

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

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

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

- the process dispatcher,
- vhand and
- dbflush

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

13. What are various IDs associated with a process?

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

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

14. Explain fork() system call.

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

15. Predict the output of the following program code

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

Answer:

```
Hello World!Hello World!
```

Explanation:

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

16. Predict the output of the following program code

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

Answer:

"Hello World" will be printed 8 times.

Explanation:

2^n times where n is the number of calls to fork()

17. List the system calls used for process management:

System calls Description

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

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

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

19. How can a parent and child process communicate?

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

20. What is a zombie?

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

21. What are the process states in Unix?

As a process executes it changes state according to its circumstances. Unix processes have the following states:

Running : The process is either running or it is ready to run .

Waiting : The process is waiting for an event or for a resource.

Stopped : The process has been stopped, usually by receiving a signal.

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

What command should you use to check your filesystem?

Answer: fsck
The fsck command is used to check the integrity of the filesystem on your disk.

You want to print out a text file called vacations however the lines are of varying length. What text filter could you use to even out the length of the lines?

Answer: fmt
The fmt text utility attempts to make all the lines the same lenght by joining or splitting lines.

You need to locate a file called salesdata that one of your user’s created in his home directory but you do not know which one. How could you use the find command to locate this file?

Answer: find /home -name salesdata
When using the find command to locate a file by name you must specify the starting place in the directory heirarchy and the -name option to specify the file to search for.

What command would you type to use the cpio to create a backup called backup.cpio of all the users' home directories?

Answer: 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.

You want to create a compressed backup of the users' home directories so you issue the command gzip /home/* backup.gz but it fails. The reason that it failed is that gzip will only compress one ________ at a time.

Answer: file
The gzip utility cannot compress multiple files in a single operation.

You have three files in the /home/ben/memos directory called letters, tom, betty. How could you determine each file's type by issuing only one command?

Answer: file letters tom betty
The file utility will display the file's type for each filename that is passed as an argument.

In order to display the last five commands you have entered using the fc command, you would type ____________.

Answer: fc -5
The fc command can be used to edit or rerun commands you have previously entered. To specify the number of commands to list, use -n.

Each command has two types of output. There are standard output and standard ___________.

Answer: error
By default, each command sends its result as standard output and any error messages as standard error.

What can you type at a command line to determine which shell you are using?

Answer: 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

Answer: 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.

What would you type to send the last 20 lines of a text file to STDIN?

A) end -n 20 filename
B) last -n 20 filename
C) head -20 filename
D) end -20 filename
E) tail -20 filename

Answer: E – Use the command tail -20 filename to see the last 20 lines of a file. The answers for a and d both point to an invalid command. The answer for b points to a valid command. Typing this answer in with a valid file name will even give you some output. However, the last command tells you who is logged in, it does not actually list the contents of any file named in the command. The answer for c, the head command, is used to look at the beginning of a file, not the end.

Which command works in almost all distributions to create a boot disk?

A) mkboot
B) make bootdsk
C) make boot
D) mkbootdsk
E) mkbootdisk

Answer: E – The mkbootdisk command creates a boot disk. Answers b and c are incorrect. The make package is used to compile software, not create boot disks. Answers a and d point to invalid commands.

Which command do you use to change runlevels?

A) initlevel
B) runlevel
C) level
D) run
E) init

Answer: E – The command used to change runlevels is init. Answers a, c, and d point to invalid commands. Answer b is a valid command, but does not set the current runlevel. The runlevel command displays the current runlevel, and the one that was used directly before entering this one.

You have a new, empty hard drive that you will use for Linux. What is the first step you use.
Choose one:

a. Create an extended partition to be used for data.
b. Format the hard drive to use the ext2 filesystem.
c. Create a swap partition of type 82.
d. Create a primary partition using fdisk.

Answer: d
You must always first create a primary partition. Operating systems, including Linux, can only be booted from a primary partition.

You have configured logrotate to rotate your logs weekly and keep them for eight weeks. You are running our of disk space. What should you do?
Choose one:

a. Quit using logrotate and manually save old logs to another location.
b. Reconfigure logrotate to only save logs for four weeks.
c. Configure logrotate to save old files to another location.
d. Use the prerotate command to run a script to move the older logs to another location.

Answer: d
You can use the prerotate command to run a script before logs are rotated. You could have this script move the older logs to another location before rotation occurs.

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.

Answer: 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 have a directory with the following permissions
drw-rw–w- 1 root admin 7202 Sep 17 9:10 administration
and need to give everyone except root read only access to it. Which of the following commands will accomplish this?
Choose one:

a. chmod uo=r administration
b. chmod ug+r administration
c. chmod uo+r administration
d. chmod ug=r administration

Answer: d
When using symbols, the equal sign explicitly sets permissions and revokes any pre-existing permissions.

You want to know how much space is being occupied by your user's home directories. Which of the following will provide you with this information?
Choose one:

a. du -l /home
b. du -b /home
c. du -m /home
d. du -c /home

Answer: d
Using the -c option with the du command will show the grand total of used space for the designated directory.

You have entered the following cronjob. When will it run? 15 * * * 1,3,5 myscript
Choose one:

a. at 15 minutes after every hour on the 1st, 3rd and 5th of each month.
b. at 1:15 am, 3:15 am, and 5:15 am every day
c. at 3:00 pm on the 1st, 3rd, and 5th of each month
d. at 15 minutes after every hour every Monday, Wednesday, and Friday

Answer: d
This would run at 15 minutes after the hour on every Monday, Wednesday, and Friday of every month no matter what the date.

You need to see the last fifteen lines of the files dog, cat and horse. What command should you use?

Answer: 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?

Answer: 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.

Answer: 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?

Answer: 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.

Answer: 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.

Answer: 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 ___________.

Answer: 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?

Answer: top
The top utility shows a listing of all running processes that is dynamically updated.

Where is standard output usually directed?

Answer: to the screen or display
By default, your shell directs standard output to your screen or display.

You want to create a compressed backup of the users' home directories. What utility should you use?

Answer: tar
You can use the z modifier with tar to compress your archive at the same time as creating it.

You wish to restore the file memo.ben which was backed up in the tarfile MyBackup.tar. What command should you type?

Answer: 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?

Answer: tar tf MyBackup.tar
The t switch tells tar to display the contents and the f modifier specifies which file to examine.

What daemon is responsible for tracking events on your system?

Answer: 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?

Answer: 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?

Answer: 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?

Answer: 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?

Answer: 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.

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

Answer: 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?

Answer: 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?

Answer: passwd boba
The passwd command is used to change your password. If you do not specify a username, your password will be changed.

When you look at the /etc/group file you see the group kmem listed. Since it does not own any files and no one is using it as a default group, can you delete this group?

Answer: no
The kmem group manages direct access to kernel memory and is necessary for your system’s health.

What text filter can you use to display a multi-page file and place numbers at the beginning of each line.
DirContents
Using the > will redirect the output of the ls /etc command to the file DirContents.

What file defines the levels of messages written to system log files?

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

You have two files each ten lines long. What text filter could you use to combine the two files so that each line of the output contains the corresponding line from each file?

Answer: join
The join text filter will display one line for each pair of input lines from two files.

You have two files in two different directories with the same inode. What type of link is involved?
“,1]); //–>
Answer: nl
The nl text filter will divide a file into logical pages and number each line.

Question 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 ____________?

Answer: nice
Both the top and nice utilities provide the capability to change the priority of a running process.

In order to apply a filesystem to your new partitions you must format them. What command would you use to create the ext2 filesystem?

Answer: mke2fs
The mke2fs command creates the new filesystem on your partition.

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.

Answer: 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.

In order to create a file called DirContents containing the contents of the /etc directory you would type _____________.

Answer: ls /etc > DirContents
Using the > will redirect the output of the ls /etc command to the file DirContents.

What file defines the levels of messages written to system log files?

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

You have two files each ten lines long. What text filter could you use to combine the two files so that each line of the output contains the corresponding line from each file?

Answer: join
The join text filter will display one line for each pair of input lines from two files.

You have two files in two different directories with the same inode. What type of link is involved?
/interview-questions/type.asp?iType\u003d83&offset\u003d20

‶,0]); D(["ma",[1,"

Linux JOB Interview questions.doc
61K View as HTML Scanning for viruses...

","10b484103aee0819"]]); D(["ce"]); //–>
Answer: hard
Hard links all have the same inode number, unlike symbolic links.

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

Answer: 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.

= System Administrator Interview Questions =

a[[PageOutline]]

This interview is meant to be used with some easier questions that aren't revealed to the candidate beforehand. These are to distinguish between experience and Google fluency.

This interview assumes use of the commandline, since we don't keep graphical environments on our servers.

== Basic navigation ==

* To display a list of all manual pages containing the keyword "date", what command would you type?

* What command will display the first several lines of a file called "junk"?

== Users and permissions practicum ==

* Rig it so everything in the folder gets deleted tonight at 10pm. Every night at 10pm.

== Local security ==

* How do you feel about `sudo`?

* What's the difference between `telnet` and `ssh`? What's a good use for each?

* How do you ensure your users have hard-to-guess passwords?

== Filesystem ==

* What is the difference between a symbolic and hard link? When would you use each?

* I have a file named `-fr`. How do I get rid of it?

* Why did I just ask that question?

* To partition or not? How?

* What are RAID 0, 1, 5, 0+1? What level would you use for a web server and why? A database server?

== `/etc` ==

* `ls -l /etc`. What is all this stuff?

* You added a line to `/etc/aliases`, but it doesn't seem to be working. Why?

* You've created a `zope` user to run Zope under. How do you secure it so someone doesn't guess its password, log in with it, and mess with stuff?

* Bring up `/etc/passwd`. What is all this junk?

* What are shadow passwords?

== Processes ==

* How many processes are running on your machine right now?

== Shells ==

* Name as many shells as you can.

* What's your favorite shell? Why?

* Write a shell script to append "snork" to the file "test" but only if "test" already exists.

* A user performed a `cd; chmod 644 .` before logging out. What problem occurs when he logs in the next time, and what level of privilege is required to correct the problem?

== Startup ==

* Describe the boot process of your favorite Linux in as much detail as you can.

* What are runlevels?

== Social ==

* Describe an experience you had with a difficult user.

* How do you keep up with current tools and practices?

* How did you document your work at your last job so someone else could pick up where you left off?

== Totally miscellaneous ==

* When debugging a core in gdb, what does the command `bt` give: core memory, heap usage, or calling stack?

* A user complains the web site is slow. What do you do?

== Apache ==

* How do you rig Apache to start up on boot?

* Apache doesn't start up on boot, and the thing above checks out okay. How do you track down the problem?

* http://weblion.psu.edu/stuff.html used to exist, but now it's moved to http://weblion.psu.edu/junk.html. Name as many ways as you can to get the old URL to still work. Which way is your favorite?

* These URLs used to exist: http://weblion.psu.edu/a.html, http://weblion.psu.edu/b.html, ..., http://weblion.psu.edu/z.html. But we want to access them from URLs like these: http://weblion.psu.edu/alphabet/a, http://weblion.psu.edu/alphabet/b, ..., http://weblion.psu.edu/alphabet/z. How can we pull that off without renaming the files?

* How do I tell if the web site is busy right now?

What is the default Window system / Windows manager used in Linux?
Code:

```
X.org
```

What command is used to list the contents of directory?
Code:

```
ls
ls -l
```

What command is used to list the top 10 files / directories size wise?
Code:

```
for X in $(du -s * | sort -nr | cut -f 2); do du -hs $X ; done
```

What command is used to display a list of currently running processes?
Code:

```
ps
top
pstree
pgrep
/proc file system
```

What is a login shell?
A program get executed when a user logs into UNIX box. E.g. bash, sh, ksh, csh

What is UID?
User identification number which is assigned to each UNIX / Linux user; it may or may not be unique (unique number is recommended to avoid security related issues). UID and user relationship defined in /etc/passswd file.
Code:

```
man id
man users
man groups
```

What GID? What is EUID? What SUID? What is RUID?
Linux > More on USER ID, Password, and Group management
Understanding /etc/passwd file format
Understanding /etc/ shadow file

Explain Unix User security concept
Permissions - chmod and chown
User groups - group management - user management
Read su, sudo man page

What PID?
Process identification number; use ps command to see PID. It is a number used by Unix kernels and Windows operating systems to identify a process.

Explain process ID zero and process ID 1?
All the idle task has process ID zero, and never exits.
The init process, with process ID 1, which does nothing but wait around for its child processes to die. Usually started for /etc/inittab

Explain wheel group usage along with an example?
Code:

```
man su
```

What command is used to check a file system for errors?
Code:

```
fsck
fsck.ext3
fsck.nfs
fsck.ext2
fsck.vfat
fsck.reiserfs
fsck.msdos
```

Is Linux / UNIX file system case sensitive? Give one example
Yes, test.txt and TEST.txt are two different files

What file contains the list of drives that are mounted at boot?
/etc/fstab - Linux / Other UNIX version
/etc/vfstab - Solaris UNIX

Explain the usage of the fourth field in /etc/fstab?
It is formatted as a comma separated list of options. Read mount command man page for all the option.

What is /etc/inittab file? In what file is the default run level defined?

System V init examines the '/etc/inittab' file for an 'initdefault' entry, which tells init whether there is a default runlevel. init is the program on Unix that spawns all other processes. It runs as a daemon and typically has PID 1.
Code:

```
man init
cat /etc/inittab
```

Common runlevle values on RHEL
Code:

```
    0. Halt
    1. Single user mode
    6. Reboot
    3. Default text
    5. Default GUI
```

To check the current runlevel:
Code:

```
who -r
runlevel
```

What command is used to get help about command? What command is used to read manual page for a given command?
Code:

```
info command-name
man command-name
command-name -h
command-name --help
```

What command form or symbol used to redirect output to a file?
Use the > symbol
Code:

```
command-name > output.txt
```

Use the < symbol to read input from a file

What is ssh? Specify ssh command syntax to execute command over a TCP/IP network?
SSH is Application layer protocol which allows data to be exchanged over a secure channel between two computers.
Sshh - Wikipedia, the free encyclopedia
Code:

```
ssh user@remote.box command-name
```

Explain steps for password less login? How do you set-up SSH with DSA / RSA public key authentication?
Howto Linux / UNIX setup SSH with DSA public key authentication (password less login)

Explain BSD-style init?

Read rc man page. There are no runlevels; the 'rc' file determines how init is to be run.
Runlevel - Wikipedia, the free encyclopedia

Explain Sys-V style init?
Read init man page
Runlevel - Wikipedia, the free encyclopedia

Explain Unix philosophy
Unix philosophy description by The Linux Information Project (LINFO)

What is POSIX? Name 2 POSIX-oriented operating systems?
Portable Operating System Interface is the collective name of a family of related standards specified by the IEEE to define the application programming interface (API). HP-UX, Solaris, AIX etc

Linux and BSD not certified as POSIX but conform to standard.

Explain Raw device and command s to configure Raw device
Block device file that allows accessing a storage device such as a hard drive directly. For example /dev/hda. Use commands
Code:

```
mknod
fdisk
mkfs
mkfs.ext3
```

Explain File descriptor
File descriptor - Wikipedia, the free encyclopedia

Explain Unix file types
Directory
Pipes
Fifo
Symbolic link
Named pipe
Socket
Device file
Door
Regular file

Explain inode, superblock and hard links
Understanding UNIX / Linux file system

Explain Unix domain socket
Unix Sockets
MySQL and many programs uses domain socket to make client / server communication.
Usually fast as compare to TCP/IP

Explain UNIX software pipeline concept
See shell or bash man page
Code:

```
cat /etc/passwd | grep username
mount | grep cdrom
```

Explain XYZ Unix daemons
Where XYZ can be any one of the following:
Code:

```
init
httpd
dhcpd
lpd
nfsd
ntpd
syslogd
ypbind
ftpd
telnetd
sshd
named
```

Explain udev in Kernel 2.6?
udev - Wikipedia, the free encyclopedia

Explain Process management and related commands

Explain Memory management and related commands

What is Open Group standards?

Secify seciaal usage for each one of the following file
/dev/null - Send unwanted output
/dev/random - Random number generation
/dev/zero - Cache or Destroy data on a partition - dd if=/dev/zero of=/dev/sda98

What is SELinux?

Write a command to find all of the files which have been accessed within the last 10 days.

What is LILO?

What is Grub?

Explain the difference between LILO and Grub

What is NFS?

What is NAMED?

What is MySQLD?

What is mysql?

What is CVS?

Why You Shouldn't Use the root Login for everyday work?

Describe the default partition scheme in Redhat Linux?

Describe the default partition scheme in Solaris? What is the slice number?

Describe all default mount point?

What is boot block?

What is logical block?

Describe the process for adding a new hard disk to UNIX box?

Describe the process for adding a new hard disk to Linux box?

Describe the process for adding a new hard disk to Linux LVM to grow /home?

Explain one major difference between a regular file system and a journaling file system?

Define JFS

Define UFS

How do you lock and unlock user account / password?

Describe RPM and command to install / remove / update Linux system?

Explain difference between rpm and up2date command.

Explain difference between rpm and apt-get command.

Explain difference between rpm and yum command.

Describe usage for pkgadd, pkginfo and pkgchk command

How do you find files on UNIX or Linux system?

Explain /etc/rc3.d

Explain ntsysv or chkconfig command

How do you get rid of process if kill PID is not working for you?

What is the purpose of the command?
grep
sed
awk
ifconfig

netstat
df
du
prtvtoc
fdisk -l
umaks
getfacl
setfacl
sudo
fsck
probe-scsi
vmstat

Explain LVM

1) What is a superblock ?
2) What is a parity bit?
3) What is an inod?
4) Explain top command ?
5) How to disable the root login in SSH ?
6) use of sysctl command ?
7) LVM how to ?
😎 Different RAID levels ?

1) What is a superblock ?
2) What is a parity bit?
3) What is an inod?
4) Explain top command ?
5) How to disable the root login in SSH ?
6) use of sysctl command ?
7) LVM how to ?
😎 Different RAID levels ?

Linux admin interview questions

By *admin* | March 4, 2005

1. How do you take a single line of input from the user in a shell script?
2. Write a script to convert all DOS style backslashes to UNIX style slashes in a list of files.
3. Write a regular expression (or sed script) to replace all occurrences of the letter 'f', followed by any number of characters, followed by the letter 'a', followed by one or more numeric characters, followed by the letter 'n', and replace what's found with the string "UNIX".
4. Write a script to list all the differences between two directories.
5. Write a program in any language you choose, to reverse a file.
6. What are the fields of the password file?
7. What does a plus at the beginning of a line in the password file signify?
8. Using the man pages, find the correct ioctl to send console output to an arbitrary pty.
9. What is an MX record?
10. What is the prom command on a Sun that shows the SCSI devices?

11. What is the factory default SCSI target for /dev/sd0?
12. Where is that value controlled?
13. What happens to a child process that dies and has no parent process to wait for it and what's bad about this?
14. What's wrong with sendmail? What would you fix?
15. What command do you run to check file system consistency?
16. What's wrong with running shutdown on a network?
17. What can be wrong with setuid scripts?
18. What value does spawn return?
19. Write a script to send mail from three other machines on the network to root at the machine you're on. Use a 'here doc', but include in the mail message the name of the machine the mail is sent from and the disk utilization statistics on each machine?
20. Why can't root just cd to someone's home directory and run a program called a.out sitting there by typing "a.out", and why is this good?
21. What is the difference between UDP and TCP?
22. What is DNS?
23. What does nslookup do?
24. How do you create a swapfile?
25. How would you check the route table on a workstation/server?
26. How do you find which ypmaster you are bound to?
27. How do you fix a problem where a printer will cutoff anything over 1MB?
28. What is the largest file system size in solaris? SunOS?
29. What are the different RAID levels?

how to find the Os version and architechture?

cat /etc/issue and cat /etc/redhat-relase

uname -r and getconf LONG_BIT

Descibe the linux boot process?

how will start any process?

What are different run levels?

when you create a user account which files will be updated?

/etc/passwd,/etc/shadow,/etc/groups

what is sticky bit and what is setuid and setgid?

How will you debug domain not resolving issue?

What is .htaccess in apache?

How will you check the consistency of the httpd.conf file?

```
apachectl configtest
```

How will include a module dynamically in apache?

How to find all the installed modules in apache?

What is virtual hosting and what are the different types and which one is useful?

what is dns and what are important files in dns?

Explain the differnt fields in the named.conf file?

how will you configure dns client?

How will you find the memory used ?

```
free -m
```

for virual memory

```
vmstat
```

How will you find whether a process is started?
top and ps

what is nice and renice in linux?

what is selinux and how it will effect different services?

What are files used for configuring network?

```
/et/hosts
/etc/sysconfig/network
/etc/sysconfig/network=scripts/ifcfg-eth0
```

what is the Syntax in /etc/resolv.conf file?
Ans:

```
domain lfix.co.uk
nameserver 194.72.192.1
nameserver 194.72.192.3
```

What is the syntax in /etc/hosts file?

IP_number Node_name Alias....

```
193.195.30.7    elsie.lfix.co.uk elsie
```

What are the default filesystems available in linux?

how will you reduce the logical volume size?

What is nfs and what are the advantages and dis advantages of nfs?

How will you find whether a file is being used?

lsof -i filename

Scenario based questions:

Only one nfs client is not able to access nfs mount how will you debug?

restrict a ftp user to his home directory(he should not be able to view any other folders except his home directory)?

When you tried to access a website it was not loaded completed some icons were missing how you will fix the issue?

Ans:This may be caused due the browser

So update the pluggins
reinstall the browser
check if browser compatibility

How will you fix if ftp service is down?

restart the xinetd service
Check whether ftp service is enable in xinetd file in plesk it was ftp_psa if it is not enable it and restart xinetd
check the logs /var/log/messages

what will be daily tasks for a system administrator?

Port number for ftp,dns,dhcp,apache,pop3,imap,https?

How ssh works?

What are rsa and dsa keys?

What is sudo and how will you create sudo users?

What is the difference between yum and rpm?

How will you installa package using rpm?

How will you upgrade the linux kernel?

How will find the which ports listening in your system?

netstat -tulp | grep listen

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

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

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

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

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

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

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

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

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

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

d

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

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

d

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

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

d

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

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

d

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

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

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

1. How do you take a single line of input from the user in a shell script?

2. Write a script to convert all DOS style backslashes to UNIX style slashes in a list of files.

3. Write a regular expression (or sed script) to replace all occurrences of the letter ‘f’, followed by any number of characters, followed by the letter ‘a’, followed by one or more numeric characters, followed by the letter ‘n’, and replace what’s found with the string “UNIX”.

4. Write a script to list all the differences between two directories.

5. Write a program in any language you choose, to reverse a file

6. What are the fields of the password file?

7. What does a plus at the beginning of a line in the password file signify?

8. Using the man pages, find the correct ioctl to send console output to an arbitrary pty.

9. What is an MX record?

10. What is the prom command on a Sun that shows the SCSI devices?

11. What is the factory default SCSI target for /dev/sd0?

12. Where is that value controlled?

13. What happens to a child process that dies and has no parent process to wait for it and what's bad about this?

14. What's wrong with sendmail? What would you fix?

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

16. What's wrong with running shutdown on a network?

17. What can be wrong with setuid scripts?

18. What value does spawn return?

19. Write a script to send mail from three other machines on the network to root at the machine you're on. Use a 'here doc', but include in the mail message the name of the machine the mail is sent from and the disk utilization statistics on each machine?

20. Why can't root just cd to someone's home directory and run a program called a.out sitting there by typing "a.out", and why is this good?

21. What is the difference between UDP and TCP?

22. What is DNS?

23. What does nslookup do?

24. How do you create a swapfile?

25. How would you check the route table on a workstation/server?

26. How do you find which ypmaster you are bound to?

27. How do you fix a problem where a printer will cutoff anything over 1MB?

28. What is the largest file system size in solaris? SunOS?

29. What are the different RAID levels?

1. Advantages/disadvantages of script vs compiled program.

2. Name a replacement for PHP/Perl/MySQL/Linux/Apache and show main differences.

3. Why have you choosen such a combination of products?

4. Differences between two last MySQL versions. Which one would you choose and when/why?

5. Main differences between Apache 1.x and 2.x. Why is 2.x not so popular? Which one would you choose and when/why?

6. Which Linux distros do you have experience with?

7. Which distro you prefer? Why?

8. Which tool would you use to update Debian / Slackware / RedHat / Mandrake / SuSE ?

9. You're asked to write an Apache module. What would you do?

10. Which tool do you prefer for Apache log reports?

11. Your portfolio. (even a PHP guest book may work well)

12. What does 'route' command do?

13. Differences between ipchains and iptables.

14. What's eth0, ppp0, wlan0, ttyS0, etc.

15. What are different directories in / for?

16. Partitioning scheme for new webserver. Why?

inux interview - August 21, 2008 at 22:00 pm by Rajmeet Ghai

What is Linux and why is it so popular?

Answer - Linux is an operating system that uses UNIX like Operating system.......

Unix interview questions with answers

Discuss the mount and unmount system calls, What are the process states in Unix?, What is use of sed command?, What is 'inode'?,What are the Unix system calls for I/O?, How are devices represented in UNIX?, Brief about the directory representation in UNIX ......

What is LILO?

Answer - LILO is Linux Loader is a boot loader for Linux. It is used to load Linux into the memory and start the Operating system.......

What is the difference between home directory and working directory?

Answer - Home directory is the default working directory when a user logs in. On the other hand, working directory is the user’s current directory.......

What is the difference between internal and external commands?

Answer - Internal commands are commands that are already loaded in the system. They can be executed any time and are independent.......

Explain the difference between a static library and a dynamic library.

Answer - Static libraries are loaded when the program is compiled and dynamically-linked libraries are loaded in while......

What is LD_LIBRARY_PATH?

Answer - LD_LIBRARY_PATH is an environment variable. It is used for debugging a new library or a non standard library.......

What is the file server in Linux server?

Answer - File server is used for file sharing. It enables the processes required fro sharing.......

What is NFS? What is its purpose?

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

How do I send email with linux?

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

Explain RPM (Red Hat Package Manager) features.

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

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.......

What is Linux Shell? What is Shell Script?

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

What are Pipes? Explain use of pipes.

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

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

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

What Stateless Linux server? What feature it offers?

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

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,......

What is Bash Shell?

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

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

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

How does the linux file system work?

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

What are the process states in Linux?

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

What is a zombie?

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

Explain each system calls used for process management in linux.

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

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

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

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

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

How secured is Linux? Explain.

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

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

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

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

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

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

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

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

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

Which command is used to review boot messages?

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

```
dmesg [options]
```

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

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

logrotate command is used to make automate rotation of log.
Syntax of the command is:
logrotate [-dv] [-f|] [-s|] config_file+
It allows automatic rotation, compression, removal, and mailing of log files. This command is mainly used for rotating and compressing log files. This job is done every day when a log file becomes too large. This command can also be run by giving on command line. We can done force rotation by giving –f option with this command in command line. This command is also used for mailing. We can give –m option for mailing with this command. This option takes two arguments one is subject and other is recipient name.

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

The main partitions are done firstly which are root, swap and boot partition. But for the mail server three different partitions are also done which are as follows:
1. /var/spool- This is done so that if something goes wrong with the mail server or spool than the output cannot overrun the file system.
2. /tmp- putting this on its own partition prevents any user item or software from overrunning the system files.
3. /home- putting this on its own is useful for system upgrades or reinstalls. It allow not to wipe off the /home hierarchy along with other areas.

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

It contains all the information of the users who log into the system. It contains a list of the system's accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc. It should have general read permission as many utilities, like ls use it to map user IDs to user names, but write access only for the superuser (root). The main fields of /etc/passwd file are:
1. Username: It is used when user logs in. It should be between 1 and 32 characters in length.
2. Password: An x character indicates that encrypted password is stored in /etc/shadow file.
3. User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
4. Group ID (GID): The primary group ID (stored in /etc/group file)
5. User ID Info: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.
6. Home directory: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /
7. Command/shell: The absolute path of a command or shell (/bin/bash). Typically, this is a shell.

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

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

How to change window manager by editing your home directory?

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

How documentation of an application is stored?

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

How shadow passwords are given?

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

How do you create a new user account?

useradd command is used for creating a new user account. When invoked without the
-D option, the useradd command creates a new user account using the values specified on the command line and the default values from the system. The new user account will be entered into the system files as needed, and initial files copied, depending on the command line options. This command uses the system default as home directory. If –m option is given then the home directory is made.

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

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

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

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

Which daemon is responsible for tracking events on Linux system?

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

Which daemon is used for scheduling of the commands?

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

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

Options
-l List - display the current crontab entries.

-r Remove the current crontab.

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

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

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

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

It is represented in octal numbers. We can simply use this command without arguments to see the current file permissions. To change the permissions, mode is given in the arguments. The default umask used for normal user is 0002. The default umask for the root user is 0022. For calculating the original values, the values shown by the umask must be subtracted by the default values. It is mainly used for masking of the file and directory permission. The /etc/profile script is where the umask command is usually set for all users. The –S option can be used to see the current default permissions displayed in the alpha symbolic format.
For example, umask 022 ensures that new files will have at most 755 permissions (777 NAND 022).
The permissions can be calculated by taking the NAND of original value with the default values of files and directories.

1.When do you need a virtual hosting ?

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

2.In which port telnet is listening?

23

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

4.How to block and openrelay ?

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

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

5.What is sandwitch configuration in qmail ?

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

6.Advantages of Qmail ?

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

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

7.What is the difference between POP3 and IMAP ?

The Difference

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

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

Scenarios of Use

POP3

- You only check e-mail from one computer.
- You want to remove your e-mail from the mail server.

IMAP

- You check e-mail from multiple locations.
- You use Webmail.

8.How to drop packets using iptables ?

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

9.Daily routines of Linux Administrators ?

*.Check the health of servers

*.Check for updates

*.Check the Backup

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

*.Troubleshoot if there any problem

*.Installation of new servers, if needed.

*.Report to the Boss

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

```
Mysqldump databasename > dumpname
```

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

Top, uptime

12.How to bind another IP in a NIC ?

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

13.Transparently proxy all web-surfing through Squid box

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

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

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

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

15 Howto Activate the forwarding

```
echo 1 >/proc/sys/net/ipv4/ip_forward
```

16.Kill spoofed packets

```
for f in /proc/sys/net/ipv4/conf/*/rp_filter; do

echo 1 > $f
```