Top Answers to Linux Interview Questions

1. Compare Linux & Windows

Criteria	Linux	Windows
Type of OS	Open Source	Proprietary
Customization	High level of customization	Cannot be changed
Security	Excellent	Cannot be changed

2. What is LILO?

- LILO is Linux Loader is a boot loader for Linux. It is used to load Linux into the memory and start the Operating system. LILO can be configured to boot other operating systems as well. LILO is customizable, which means that if the default configuration is not correct, it can be changed. Config file for LILO is lilo.conf.
- LILO is also a code snippet which loads PC BIOS into the main memory at the time of starting the computer system. **It handles the following tasks :**
  1. Locating Linux kernel.
  2. Identifying other supporting programs and loading them in the memory.
  3. Starting Kernel.
- The selection of various kernel images and boot routines is supported by LILO. For this reason, it is known as boot manager.

3. You wish to print a file 'draft' with 60 lines on a page. What command would you use?

The command used : pr -l60 draft

- The default page length when using pr is 66 lines.
- The -l option specifies a different length.

4. What is LD_LIBRARY_PATH?

- LD_LIBRARY_PATH is an environment variable. It is used for debugging a new library or a non-standard library. It is also used to identify what directories need to be searched. Path to search for directories needs to given.
- The variable can be set using setenv**—LD_LIBRARY_PATH–$PATH.**
- It is used to search for the shared objects / dynamic libraries by the operating system for extendable functionality at runtime.

5. Name a service that you should disable (which acts both as Web and FTP Server) on a Linux Server.

The **finger service** should be disabled because a remote user can get important information about the system by using that command.

6. What does Sar provide? Where are Sar logs stored?

Sar collects, reports, or saves system activity information, sar serves to log and evaluate a variety of information regarding system activity. With performance problems, sar also permits retroactive analysis of the load values for various sub-systems (CPUs, memory, disks, interrupts, network interfaces and so forth) and limitation of problems in this manner. If CPU utilization is near 100 % (user + nice + system), the workload sampled is CPU-bound.
By default, log files of Sar command is located at /var/log/sa/sadd file, where dd parameter indicates the current day.

7. How to check Memory stats and CPU stats as a Linux admin?

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

8. How to reduce or shrink the size of LVM partition?

Below are the logical steps to reduce size of LVM partition :

- Unmount the filesystem using unmount command,
- Use resize2fs command , e.g **resiz2fs /dev/mapper/myvg-mylv 10G**
- Now use the lvreduce command as **lvreduce -L 10G /dev/mapper/myvg-mylv**

The above Command will shrink the size LVM partition and fixes the filesystem size to 10GB.Most in-depth, industry-led curriculum in linux.

9. What are the different modes of Network bonding in Linux?

Below are list of modes used in Network Bonding :

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

10. How to check and verify the status of the bond interface?

Using the command '**cat /proc/net/bonding/bond0,**' we can check what mode is enabled and what LAN cards are used in this bond. In this example, we have one one bond interface. However, we can have multiple bond interfaces like bond1, bond2 and so on.

11. How can you enhance the security of password file?

Linux keep user account information in a text file called /etc/passwd. This file also stores one way encrypted password. It is accessed by several tools to get user information, which is a security risk, so file need to 'Word Readable.' To minimize the security risk, you can use shadow password format. This method saves account information in regular file /etc/passwd.

However, the password is stored as a single "x" character (not actually stored in this file). A second file, called "/etc/shadow" contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account and is therefore less of a security risk

12. What command can you use to make a tape archive file of a /home directory and send it to the /dev/tape device?

The correct command is tar -cvf /dev/tape /home.
The -xvf option is used to extract files from an archive.Expert Linux Professionals are in much demand.

13. Suppose your FTP Server is hacked and the entire server needs to be restored. How should you restore the original kernel system files?

You cannot restore the entire operating system from tape backup device. So you should reinstall the core operating system, and then restore system configuration files and user data from tape backup device.

14. Why should you avoid Telnet to administer a Linux system remotely?

Telnet uses most insecure method for communication. It sends data across the network in plain text format and anybody can easily find out the password using the network tool. In the case of Telnet, these include the passing of login credentials in plain text, which means anyone running a sniffer on your network can find the information he needs to take control of a device in a few seconds by eavesdropping on a Telnet login session.

15. What is Puppet Server?

Puppet is an open-source & enterprise software for configuration management toll in UNIX like operating system. Puppet is an IT automation software that is used to push configuration to its clients (puppet agents) using code. Puppet code can do multiple tasks from installing new software to checking file permissions to updating user accounts.

16. What is the difference between Cron and Anacron?

1. Minimum granularity with Cron is minute while it is in days with Anacron.

2. Cron job can be scheduled by any normal user while Anacron can be scheduled only by the super user (the superuser is a special user account used for system administration. Depending on the operating system (OS), the actual name of this account might be root,administrator, admin or supervisor)
3. Cron expects the system to be up and running while the Anacron doesn't expect the system to be up and running all the time. In case of Anacron, if a job is scheduled and the system is down that time, it will execute the job as soon as the system is up and running.
4. Cron is ideal for servers while Anacron is ideal for desktops and laptops.
5. Cron should be used when you want a job to be executed at a particular hour and minute while Anacron should be used in when the job can be executed irrespective of the hour and minute.

17. What command is used to check the number of files, disk space and 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. Each 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.

18. 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.

19. 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 :

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

20. 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 window manager. 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

21. How shadow passwords are given by in Linux?

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.

22. What 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.

23. What shell does a Linux Administrator 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 rejects shell login on the server as in 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 as 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 to it. But the nologin shell simply tells that no such account is available. So nologin shell is used often in Linux.

24. If a volume group named VG0 already exists and we need to extend this volume group up to 4GB. How will you do it?

- Firstly create Physical volume (/dev/sda7) of size 4GB.
- Now run following command.
  vgextend VG0 /dev/sda7

25. Is there any relation between modprobe.conf file and network devices?

Yes, this file assigns a kernel module to each network device.

For Example :-

```
[root@localhost ~]# cat /etc/modprobe.conf
alias eth0 b44
Here, b44 is the kernel module for network device eth0.
We can confirm whether this module "b44" is present or not by the following command
[root@localhost ~]# lsmod |grep b44
b44 29005 0
```

26. What is YUM?

YUM stands for Yellow dog Updater, Modified because it is based on YUP, the Yellow dog Updater. Where does the name Yellow dog come from? Yellow Dog is a version of Linux for the Power Architecture hardware and is RPM-based, just like Red Hat Enterprise Linux and Fedora. YUP, and later YUM, were written by the Linux community as a way to maintain an RPM-based system

27. What is the role of Kudzu?

Kudzu is used to detect new Hardware. RedHat Linux runs a hardware discoverer, named kudzu. When attempting to identify a serial port Kudzu resets the serial port. This stops the serial console. Kudzu is configured from the file/etc/sysconfig/kudzu.
Kudzu can be prevented from resetting hardware, by setting the configuration parameter SAFE to yes.

28. What is the difference between ext2 and ext3 file systems?

- The ext3 file system is an enhanced version of the ext2 file system.
- The most important difference between Ext2 and Ext3 is that Ext3 supports journaling.
- After an unexpected power failure or system crash (also called an unclean system shutdown), each mounted ext2 file system on the machine must be checked for consistency by the e2fsck program. This is a time-consuming process and during this time, any data on the volumes is unreachable.
- The journaling provided by the ext3 file system means that this sort of file system check is no longer necessary after an unclean system shutdown. The only time a consistency check occurs using ext3 is in certain rare hardware failure cases, such as hard drive failures. The time to recover an ext3 file system after an unclean system shutdown does not depend on the size of the file system or the number of files. Rather, it depends on the size of the journal used to maintain consistency. The default journal size takes almost a second to recover, depending on the speed of the hardware.

29. Explain /proc filesystem?

/proc is a virtual file system that provides detailed information about Linux kernel, hardware and running processes. Files under /proc directory named as Virtual files.
Since /proc contains virtual files, it is called **virtual file system**. These virtual files have unique qualities. Most of them are listed as zero bytes in size.
Virtual files such as /proc/interrupts, /proc/meminfo, /proc/mounts, and /proc/partitions provide an up-to-the-moment glimpse of the system's hardware. Others: /proc/filesystems file and the /proc/sys/ directory provide system configuration information and interfaces.

30. How do you create ext4 file system?

mke2fs -t ext4 /dev/DEV

31. How to Enable ACLs for /home partition?

Add following entry in /etc/fstab
LABEL=/home /home ext3 acl 1 2
Now remount /home partition with acl option.
mount -t ext3 -o acl /dev/sda3 /home