Important Linux Interview Questions With Answers

Basic Questions

1. What is Linux?

- Linux is an open-source, Unix-like operating system kernel that serves as the core of many Unix-like systems. It was created by Linus Torvalds and has since gained popularity for its stability, security, and flexibility.

2. What is Kernel?

- The kernel is the core component of an operating system that manages system resources, acts as an intermediary between hardware and software, and facilitates communication between different parts of the computer.

3. What is Bash?

- Bash, short for "Bourne Again SHell," is a command-line interpreter and scripting language for Unix-like operating systems. It provides a text-based interface to interact with the operating system.

4. Can you explain about LILO?

- LILO (Linux Loader) is a boot loader for Linux systems. It is responsible for loading the Linux kernel into memory and initiating the boot process. However, LILO is becoming less common, with GRUB (Grand Unified Bootloader) being more widely used.

5. What is SHELL?

- A shell is a command-line interface that allows users to interact with the operating system. Bash is an example of a shell in Linux.

6. What is SWAP?

- Swap is a space on a hard disk used as virtual memory when the physical memory (RAM) is full. It allows the system to move data from RAM to disk and vice versa, helping to avoid memory shortages.

7. Type of File Permission in Linux?

- The types of file permissions in Linux are read (r), write (w), and execute (x). These permissions are assigned to three entities: owner, group, and others.

8. Which type of Service acts as FTP and Web in Linux?

- The service that acts as FTP (File Transfer Protocol) and Web (HTTP) in Linux is typically the vsftpd service for FTP and Apache or Nginx for web services.

9. What is Zombie Process?

- A Zombie process is a process that has completed execution but still has an entry in the process table. It is a child process that has not been completely removed.

10. What is INODE? Can you share the command to check?

- An inode is a data structure on a filesystem that stores information about a file or directory. The command to check inode information is `ls -i` for a specific file or directory.

11. Name the first process that starts whenever the kernel boots and what is the PID for that?

- The first process that starts when the kernel boots is `init`. Its PID is 1.

12. What is Set UID, SGID, and Sticky bit?

- Set UID (Set User ID), SGID (Set Group ID), and Sticky bit are special permission bits. Set UID allows a program to run with the privileges of the file owner, SGID allows a program to inherit the group ownership of the parent directory, and Sticky bit is used to restrict deletion of files in a directory.

13. Share the roles of a directory in Linux?

- In Linux, directories serve as containers for files, help organize the file system, and provide a hierarchical structure. They also control access to files through permissions.

14. What is KERNEL PANIC?

- Kernel Panic is a critical error that occurs when the Linux kernel encounters a problem from which it cannot recover. It results in the system halting to prevent further damage.

15. What is UMASK?

- UMASK (User File-Creation Mask) is a set of permissions that subtracts from the default permissions of newly created files and directories.

16. Explain in detail the /etc/shadow file?

- The `/etc/shadow` file in Linux stores encrypted user passwords and related information, providing an additional layer of security compared to storing passwords in the `/etc/passwd` file.

17. What does SAR provide? Where are the logs stored?

- SAR (System Activity Reporter) provides system performance data, including CPU, memory, disk, and network usage. SAR logs are typically stored in `/var/log/sa/`.

18. How to reset the password?

- The password for a user can be reset using the `passwd` command. For example, `passwd username` will prompt for a new password for the specified user.

19. Command to check the password policy?

- The password policy in Linux can be checked using the `passwd` command with the `-S` option, like `passwd -S username`.

20. How to unlock the username?

- To unlock a user account, the `passwd` command with the `-u` option can be used, like `passwd -u username`.

21. How to set a user to NO LOGIN?

- The `usermod` command with the `-s` option can be used to set a user to NO LOGIN. For example, `usermod -s /sbin/nologin username`.

22. Which command is used to shutdown and halt the systems?

- The `shutdown` command is used to shut down the system. For example, `shutdown -h now` will shut down the system immediately.

23. What Daemon controls the print spoiling process?

- The `cupsd` daemon controls the print spooling process in Linux. It manages print jobs and provides printing services.

24. What is FSTAB?

- `/etc/fstab` is a configuration file that contains information about disk drives and partitions. It is used by the `mount` command to automatically mount filesystems at boot.

25. Command to remove, install, and update RPM package?

- The `rpm` command is used to remove (`rpm -e`), install (`rpm -i`), and update (`rpm -U`) RPM packages in Linux.

26. What are the process states in Linux?

- The process states in Linux are Running, Sleeping, Stopped, Zombie, and Dead.

27. What are the types of Kernels?

- The types of kernels are Monolithic Kernel, Microkernel, and Hybrid Kernel.

28. Explain Symlink and Hardlink?

- A symlink (symbolic link) is a reference to another file, while a hard link is a directory entry that points to the same inode as another directory entry.

29. What is `w`, `pcpu`, and `jcpu` command?

- The `w` command shows information about currently logged-in users. `pcpu` and `jcpu` refer to the percentage of CPU time used by a process and the cumulative CPU time used by a process, respectively.

30. What is `nice` and `renice` command?

- The `nice` command is used to launch a program with a specified priority. The `renice` command is used to change the priority of an already running process.

LVM Questions:

1) What is Logical Volume Management (LVM)?

Logical Volume Management (LVM) is a storage management technology that allows for dynamic and flexible management of disk space on Linux systems. It provides a layer of abstraction between the physical storage devices and the file systems, enabling features such as creating, resizing, and moving logical volumes without affecting data.

2) What are the steps involved in setting up LVM on a Linux system?

The steps involved in setting up LVM on a Linux system typically include:

a. Install LVM Tools:

```bash
sudo apt-get install lvm2    # For Debian/Ubuntu
sudo yum install lvm2        # For Red Hat/Fedora
```

b. Initialize Physical Volumes (PVs):

```bash
sudo pvcreate /dev/sdX      # Replace /dev/sdX with the appropriate disk
```

c. Create a Volume Group (VG):

```bash
sudo vgcreate vg_name /dev/sdX   # Replace vg_name with your desired name
```

d. Create Logical Volumes (LVs):

```bash
sudo lvcreate -n lv_name -L sizeG vg_name   # Replace lv_name and sizeG accordingly
```

e. Format the Logical Volume:

```bash
sudo mkfs.ext4 /dev/vg_name/lv_name   # Format with an appropriate filesystem
```

f. Mount the Logical Volume:

```bash
sudo mkdir /mnt/mount_point
sudo mount /dev/vg_name/lv_name /mnt/mount_point
```

3) How do you add a new Physical Volume to an existing Volume Group?

To add a new Physical Volume (PV) to an existing Volume Group (VG):

```bash
sudo pvcreate /dev/sdY     # Replace /dev/sdY with the appropriate disk
sudo vgextend vg_name /dev/sdY    # Add the new PV to the existing VG
```

4) Can you explain the process of creating, extending, and removing Logical Volumes within a Volume Group?

Create Logical Volume:

```bash
sudo lvcreate -n new_lv -L sizeG vg_name   # Replace new_lv and sizeG accordingly
```

Extend Logical Volume:

```bash
sudo lvextend -L +sizeG /dev/vg_name/lv_name   # Extend by a specific size
```

Remove Logical Volume:

```bash
sudo lvremove /dev/vg_name/lv_name
```

5) In the event of metadata corruption or other failures, what steps can be taken to recover an LVM setup?

If metadata corruption or other failures occur, the following steps can be taken:

- Use the `vgcfgrestore` command to restore the Volume Group configuration.
- Check for and repair any inconsistencies with `vgscan` and `vgck`.
- If necessary, restore data from backups.

6) Discuss best practices for maintaining the integrity of an LVM configuration and preventing potential failures.

- Regularly back up critical data.
- Monitor the health of storage devices.
- Use redundant hardware (RAID) for physical volumes.
- Keep the system and LVM tools up to date.
- Document the LVM configuration for easier recovery.

7) Adding on Multiple Swap and how can we extend swap size?

Add a New Swap Partition:

```bash
sudo mkswap /dev/sdZ     # Replace /dev/sdZ with the appropriate disk
sudo swapon /dev/sdZ
```

Extend Existing Swap (Assuming it's an LVM Logical Volume):

```bash
sudo lvcreate -n swap2 -L sizeG vg_name
sudo mkswap /dev/vg_name/swap2
sudo swapon /dev/vg_name/swap2
```

8) How to reduce the size of LVM?

To reduce the size of an LVM Logical Volume:

```bash
sudo lvreduce -L -sizeG /dev/vg_name/lv_name   # Reduce by a specific size
```

Networking Questions:

1) Share the type of Network Bonding in Linux?

In Linux, Network Bonding refers to the process of combining multiple network interfaces into a single bonded interface for fault tolerance or increased bandwidth. The types of bonding modes include:

- Mode 0 (balance-rr): Round-robin load balancing.
- Mode 1 (active-backup): Active-passive failover.
- Mode 2 (balance-xor): XOR load balancing.
- Mode 3 (broadcast): All transmissions sent on all slaves.
- Mode 4 (802.3ad): Dynamic link aggregation (LACP).
- Mode 5 (balance-tlb): Adaptive transmit load balancing.

- Mode 6 (balance-alb): Adaptive load balancing.

2) Describe the role of IPTABLES and FIREWALLD?

- IPTABLES: It is a user-space utility program that allows configuring the IP packet filter rules of the Linux kernel firewall. It is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel.

Example commands:

```bash
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT   # Allowing SSH traffic
sudo iptables -A INPUT -j DROP                       # Dropping all other incoming traffic
```

- FIREWALLD: It is a dynamic daemon that manages the system's firewall rules. It provides a management interface using both a command-line tool (`firewall-cmd`) and a graphical user interface.

Example commands:

```bash
sudo firewall-cmd --zone=public --add-port=80/tcp --permanent   # Allowing HTTP traffic
sudo firewall-cmd --reload                                      # Applying changes
```

3) How do you configure ROUTE, and how can we check the same, share the command?

- Configure ROUTE:

```bash
sudo route add default gw 192.168.1.1     # Adding a default gateway
```

- Check ROUTE:

```bash
route -n                # Display routing table
```

4) How to configure IP by GUI method?

The GUI method depends on the desktop environment used. For example, on GNOME (used by Ubuntu), you can use the NetworkManager applet:

- Open "Settings" -> "Network."
- Click on the gear icon next to the network connection you want to configure.
- Enter the desired IP address, subnet mask, gateway, and DNS settings.

5) How to configure IP by command line?

- Using ifconfig (deprecated):

```bash
sudo ifconfig eth0 192.168.1.2 netmask 255.255.255.0
```

- Using ip command (recommended):

```bash
sudo ip addr add 192.168.1.2/24 dev eth0
```

- Set default gateway:

```bash
sudo ip route add default via 192.168.1.1
```

6) Difference between NFS and SAMBA?

- NFS (Network File System):

  - *Purpose:* Designed for sharing files and directories between UNIX-like systems.

  - *Protocol:* Uses the NFS protocol.

  - *Authentication:* Typically relies on the security mechanisms of the underlying network.

  - *Access Control:* Controlled by host-based permissions.

  - *Platform:* Native to UNIX/Linux.

- SAMBA:

  - *Purpose:* Facilitates file and print services for Windows clients in a UNIX environment.

  - *Protocol:* Uses the SMB/CIFS protocol.

  - *Authentication:* Can integrate with Windows authentication (Active Directory).

  - *Access Control:* Uses user-based permissions.

  - *Platform:* Cross-platform, runs on UNIX/Linux but serves Windows clients.

Example commands for NFS and SAMBA are specific to their configuration files and require setup beyond the scope of a single command. The configuration files for NFS are usually located in `/etc/exports`, while SAMBA's configuration is in `/etc/samba/smb.conf`.

Advanced Linux questions:

1. What is LDAP and how can we configure it?

   - LDAP (Lightweight Directory Access Protocol) is a protocol for accessing and maintaining distributed directory information services. Configuration involves setting up an LDAP server, defining its structure, and configuring client systems to connect to the LDAP server.

2. How many types of RUN LEVEL and explain in detail?

- There are typically seven run levels (0-6) in Linux, each serving a specific purpose. Run levels determine the state of the system, such as single-user mode, multi-user mode, or reboot. Detailed explanations include:

  - 0: Halt

  - 1: Single-user mode

  - 2-5: Multi-user modes

  - 6: Reboot

3. Explain the BOOT Process?

- The boot process involves several stages, including BIOS/UEFI, bootloader (e.g., GRUB), kernel loading, initialization of hardware and services, and finally, handing over control to the init process or system manager.

4. What are the fields in FSTAB?

- /etc/fstab fields include:

  - Device: The device or partition.

  - Mount point: The directory where the device is mounted.

  - Filesystem type: The type of filesystem.

  - Options: Mount options.

  - Dump: Backup frequency.

  - Pass: Filesystem check order.

5. Explain fields in /etc/password?

- Fields in /etc/passwd include:

  1. Username

  2. Password (encrypted or 'x' for shadow password)

  3. User ID (UID)

  4. Group ID (GID)

  5. User information (e.g., full name)

  6. Home directory

  7. Shell

6. How to configure LOCAL Repository?

- Create a directory, copy package files into it, and create a repository configuration file (e.g., /etc/yum.repos.d/local.repo) pointing to the local directory.

7. Share the details for System calls for Process Management?

- System calls for process management include fork(), exec(), wait(), exit(), getpid(), and others. These calls help manage processes in a Linux system.

8. Why is the finger service always kept disabled?

- The finger service is often disabled due to security concerns. It can be exploited to gather information about users on a system, posing a security risk.

9. What is KVM, and what is the use of the XEN command?

- KVM (Kernel-based Virtual Machine) is a virtualization solution for Linux. XEN is another hypervisor. Commands associated with them are used for managing virtual machines.

10. What are some techniques for Kernel Tuning?

- Techniques include adjusting kernel parameters using sysctl, enabling/disabling kernel modules, and modifying kernel configuration files to optimize performance.

11. How do you perform incident response and root cause analysis in LINUX?

- Incident response involves identifying, containing, eradicating, recovering, and analyzing incidents. Root cause analysis investigates the fundamental cause of problems.

12. Advantage of using Reverse Proxy?

- A reverse proxy enhances security, load balances, and improves performance by serving as an intermediary between clients and servers, handling requests on behalf of the servers.

13. Explain the process to reset ROOT password in Single User Mode?

- Boot into single-user mode, mount the root filesystem with write permissions, and use the "passwd" command to reset the root password.

14. How do you increase Linux OS performance?

- Performance tuning involves optimizing kernel parameters, disk I/O, network settings, and application-specific configurations.

15. What is Linux Virtual Memory?

- Linux Virtual Memory is a memory management technique that provides an "idealized abstraction of the storage resources that are actually available on a given machine."

16. What is drop cache in Linux?

- The "drop_cache" in Linux allows the system to drop clean caches, dentries, and inodes, freeing up memory.

17. What are some common reasons for Linux systems not booting up?

- Reasons include corrupted bootloader, misconfigured kernel parameters, hardware issues, and file system errors.

18. How do you troubleshoot Kernel-based issues in Linux?

- Review kernel logs (dmesg), analyze system logs, and use debugging tools like gdb for kernel-related issues.

19. To exclude a package permanently, which file would you edit?

- Edit the "/etc/yum.conf" or create a configuration file in "/etc/yum.repos.d/" to exclude a package from updates.

20. What are the different ways in which we can secure the website?

- Techniques include using HTTPS, strong authentication, web application firewalls, regular security audits, and keeping software up-to-date.

DNS-related questions:

1. What is the Domain Name System (DNS) and its role in networking?

- DNS is a distributed system that translates human-readable domain names into IP addresses, facilitating communication on the internet.

2. Explain the difference between a forward lookup and a reverse lookup in DNS.

- Forward lookup translates domain names to IP addresses, while reverse lookup does the opposite, resolving IP addresses to domain names.

3. How do you configure DNS settings on a Linux system using /etc/resolv.conf? Which parameters are commonly used in this file?

- Edit `/etc/resolv.conf` with parameters like `nameserver` (DNS server IP), `search` (domain search list), and `domain` (default domain).

4. Explain the concept of DNS zones. What is the difference between a forward lookup zone and a reverse lookup zone?

- DNS zones are administrative units for domain delegation. Forward lookup zones map domain names to IP addresses, while reverse lookup zones map IP addresses to domain names.

5. Explain various DNS record types?

- Common DNS record types include:
  - A (Address)
  - CNAME (Canonical Name)
  - MX (Mail Exchange)
  - PTR (Pointer)
  - NS (Name Server)
  - SOA (Start of Authority)

6. What is the purpose of DNS forwarders and resolvers? How do they differ, and how are they configured on a Linux DNS server?

- DNS forwarders are servers that handle DNS queries on behalf of another server, while resolvers perform queries directly. Configuration involves specifying forwarders in the server's DNS settings.

7. What is Master and Slave concept in DNS?

- In DNS, the Master (Primary) server holds the original read-write copies of zone records, while the Slave (Secondary) server replicates these records for redundancy but is read-only.

8. What is TTL in DNS?

- TTL (Time to Live) in DNS is a value that determines how long a DNS record can be cached by resolver systems or intermediary servers. It is measured in seconds.

9. Define DNS cache poisoning. How can DNS cache poisoning attacks be mitigated or prevented?

- DNS cache poisoning involves introducing false DNS information into the cache. Mitigation involves using DNSSEC (Domain Name System Security Extensions) and regularly updating DNS software.

10. Discuss the role of root DNS servers in the DNS hierarchy. How do they function and contribute to the DNS resolution process?

- Root DNS servers are the first step in the DNS resolution process. They provide information about Top-Level Domains (TLDs) and direct queries to authoritative DNS servers responsible for specific domains.

These answers provide a brief overview of each topic. For in-depth understanding and implementation details, refer to official documentation and resources on DNS.

RAID-related questions:

1. What is RAID?

- RAID (Redundant Array of Independent Disks) is a data storage technology that combines multiple physical drives into a single logical unit to improve performance, fault tolerance, or both.

2. What are different types of RAID?

- Common RAID levels include:
  - RAID 0 (Striping)
  - RAID 1 (Mirroring)
  - RAID 5 (Striping with Parity)
  - RAID 6 (Striping with Dual Parity)

- RAID 10 (Striping and Mirroring)

3. How many drives require for RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10?

- - RAID 0: Minimum 2 drives

- RAID 1: Minimum 2 drives

- RAID 5: Minimum 3 drives

- RAID 6: Minimum 4 drives

- RAID 10: Minimum 4 drives

4. How do you handle disk failure in RAID?

- Disk failure in RAID is handled by redundancy mechanisms in different RAID levels. The RAID controller rebuilds data from the remaining drives.

5. Describe how parity and striping work in RAID configurations. What are their roles in different RAID levels?

- - Parity: Used for error checking and data recovery. RAID 5 and RAID 6 use parity.

- Striping: Distributes data across multiple drives to improve performance. RAID 0, RAID 5, and RAID 6 use striping.

6. What is a hot spare in RAID configurations? How does it contribute to fault tolerance, and how is it managed within RAID setups?

- A hot spare is a designated drive that automatically replaces a failed drive in the array. It contributes to fault tolerance by reducing the time a RAID array operates in a degraded state. RAID controllers manage hot spares.

7. Explain the role of RAID controllers?

- RAID controllers manage the storage array, handling tasks such as data distribution, parity calculation, and error recovery. Hardware RAID controllers operate independently of the host system.

8. Discuss the data recovery process in RAID 10 configurations. What steps are involved in recovering data after a disk failure?

- In RAID 10, if a drive fails, data is reconstructed from the mirrored copy on the surviving drive. The RAID controller automatically rebuilds the data onto a replacement drive.

9. Explain how mirroring works in RAID 1. What advantages and limitations does RAID 1 mirroring have?

- RAID 1 mirrors data onto multiple drives, providing redundancy. Advantages include data integrity and quick recovery from drive failures. Limitations involve higher cost due to mirroring.

10. Describe the RAID rebuild process after a disk failure. How long does it typically take?

- The RAID rebuild process involves copying data from surviving drives to a replacement drive. Rebuild time varies based on drive size, RAID level, and system load.

11. How do you monitor RAID health and status? What tools or methods can be used for proactive monitoring and alerting?

- RAID health is monitored using tools like `mdadm` for software RAID or proprietary management software for hardware RAID. Regularly check logs and use monitoring tools for alerts.

12. How does RAID work with SSDs? Are there any specific considerations or optimizations when using SSDs in a RAID setup?

- RAID with SSDs enhances performance significantly. Specific considerations include wear leveling and ensuring the RAID controller supports SSDs. Optimizations involve aligning partitions to erase block boundaries.

13. How does RAID ensure data integrity? What mechanisms or checks are in place to prevent data corruption within RAID arrays?

- RAID ensures data integrity through parity checks, checksums, and error correction mechanisms. These methods help detect and correct errors that could lead to data corruption.

14. Explain the concept of snapshotting and cloning in RAID setups?

- - Snapshotting: Creating a point-in-time copy of the RAID array. Useful for backups or system state recovery.

- Cloning: Duplicating the entire RAID array onto another set of drives for redundancy or migration.

15. Describe the role of cache in RAID configurations?

- Cache in RAID controllers stores frequently accessed data temporarily, improving performance. It helps smooth out the differences in read and write speeds between the drives.