LINUX INTERVIEW QUESTIONS AND ANSWERS

What is Linux Kernel?

Ans: Linux kernel is the heart of the operating system. It acts as a bridge between software and hardware. If Software requests the hardware, then the kernel delivers the data between software and hardware.

For example, if you want to play a song you should launch your default player, it requests the kernel to play a song, now the kernel will contact the hardware to seek the permissions or to seek the hardware components like if you plugged in any headset to the device. Most Android phones use Linux kernels.

How do you monitor system performance and resource usage in Linux?

Linux offers several built-in and third-party tools to monitor system performance and resource usage. Some popular tools include:

1) **top**: Provides a real-time, dynamic view of processes and their resource usage.
2) **vmstat**: Displays virtual memory statistics, including system processes, memory, and CPU utilization.
3) **iostat**: Reports disk input/output (I/O) statistics and CPU usage.
4) **sar**: Collects, reports, and saves system activity information.
5) **free**: Displays memory usage, including free, used, and swap memory.
6) **netstat**: Shows network connections, routing tables, and network interface statistics.

How do you create and manage cron jobs in Linux?

Cron jobs are scheduled tasks that run automatically at specified intervals. To create and manage cron jobs in Linux:

1. Edit the crontab file using the command crontab -e.
2. Add a new line for each cron job, specifying the time schedule and command to run. The format is:* * * * * /path/to/command
   The five fields represent minutes (0-59), hours (0-23), days of the month (1-31), months (1-12), and weekdays (0-7, with both 0 and 7 representing Sunday).
3. Save and exit the file. The new cron jobs will be scheduled and executed automatically.

To manage existing cron jobs, use crontab -l to list them and crontab -r to remove them.

Explain the process of automating tasks using scripts in Linux.

Automating tasks using scripts in Linux involves creating executable files containing a series of commands that can be run automatically or on-demand. Shell scripts are a common method for

automating tasks in Linux. To create a shell script:

1. Open a new text file using a text editor (e.g., nano script_name.sh).
2. Add a shebang (#!) at the beginning of the file to specify the interpreter (e.g., #!/bin/bash for Bash scripts).
3. Write the commands to be executed, one per line. Include variables, loops, and conditional statements as needed.
4. Save and close the file.
5. Make the script executable using the chmod command (e.g., chmod +x script_name.sh).

How do you optimize the performance of a Linux server?

To optimize the performance of a Linux server:

1) Keep the server up to date with the latest software, security patches, and kernel updates.
2) Use performance monitoring tools (e.g., top, htop, vmstat, iostat) to identify bottlenecks and resource-intensive processes.
3) Optimize hardware settings, including BIOS configurations, power management, and processor settings.
4) Configure the server for its specific role, disabling unnecessary services and tuning kernel parameters.
5) Optimize storage performance using appropriate file systems, mount options, and storage technologies (e.g., LVM, RAID).
6) Regularly review and audit system configurations, logs, and performance metrics to detect and resolve potential issues.

How do you manage disk space in Red Hat Linux?

In Red Hat Linux, disk space can be managed using a variety of command line tools. The process of managing disk space in Red Hat Linux typically involves the following steps:

- **Check disk usage**: Use the command “df -h” to check the current disk usage, which will display the total size, used space, available space, and percentage of usage for each file system.
- **Check directory usage**: Use the command “du -sh directory” to check the space usage of a specific directory, where “directory” is the path to the directory you want to check.
- **Find large files**: Use the command “find / -type f -size +10M -exec ls -lh {} ;” to find files larger than 10 MB and list them with their sizes and permissions.
- **Clear log files**: Use the command “find /var/log -type f -name ‘*.log’ -mtime +30 -delete” to delete log files that haven’t been modified for more than 30 days.

- **Remove old packages**: Use the command “package-cleanup –oldkernels –count=2” to remove old kernels that haven’t been used for more than 2 days.
- **Remove unneeded dependencies**: Use the command “yum autoremove” to remove packages that were installed as dependencies but are no longer needed by any package.
- **Compress files**: Use the command “tar -czvf archive.tar.gz directory” to compress a directory and save it as an archive.
- **Extend disk space**: If your disk space is running low and you need more disk space, you can use the command “lvextend -L +SIZE /dev/mapper/vgname-lvname” to extend the size of a logical volume.
-

How do you troubleshoot common issues in Red Hat Linux?

1. **Check log files**: The first step in troubleshooting any issue is to check the log files. Common log files in Red Hat Linux include /var/log/messages, /var/log/secure, and /var/log/httpd/error_log. The commands “tail -f /var/log/messages” and “tail -f /var/log/secure” can be used to monitor the log files in real-time.
2. **Check system status**: Use the command “systemctl status servicename” to check the status of a specific service, where “servicename” is the name of the service you want to check. The command “systemctl list-units –all” can be used to list all the units and their status.
3. **Check network status**: Use the command “ipaddr show” to view the IP address and status of all network interfaces, and “ping hostname” or “ping IP address” to test network connectivity.
4. **Check process status**: Use the command “ps aux” to view all running processes and their status, and “top” to view the processes that are using the most resources.
5. **Check disk space**: Use the command “df -h” to check disk usage, and “du -sh directory” to check the space usage of a specific directory.
6. **Check for updates**: Use the command “yum check-update” to check for updates and “yum update” to update the system.
7. **Restart the service or reboot the system**: If the issue persists, try restarting the service with the command “systemctl restart servicename” or reboot the system with the command “reboot”
8. **Check the kernel**: If a service is not running or the system is not booting, it could be due to a kernel issue. You can use the command “uname -r” to check the kernel version that is running and compare it with the kernel version that is installed.

What is BASH?

Ans: Bash is a Unix shell and command processor written by Brian Fox for the GNU project. It is free software and acts as a replacement for Bourne Shell. It is an interpreted and not compiled process which can also be run in the terminal window.

What is Shell?

Ans: Shell is a computer program that acts as an interface between the user and the kernel. Users can communicate with the kernel by writing programs, commands, and scripts on the shell. It accepts human-readable commands and converts them into kernel-understandable language.

How many types of Shells are there in Linux?

Ans: They are five Shells in Linux:

- **C Shell (csh):** It is like C syntax and provides spelling checking and job control.
- **Korn Shell (ksh):** This is a high-level programming language shell.
- **Z Shell (Zsh):** It provides some unique nature like it observes login/logout watching, file name generating, startup files, and closing comments.
- **Bourne Again Shell (bash):** It is the default to Linux distributions.

What is a swap space?

Ans: Swap Space is used when the physical Ram memory is running out. It will move the Ram inactive pages to the swap space. It can consider in the form of a dedicated swap partition or swap files.

Explain File Permissions types in Linux?

Ans: Linux file permissions - Each file or directory has 3 permissions

They are

1. **Read:** It refers to only they can read the file.
2. **Write:** It refers that they can write the file or modify the file of a directory.
3. **Execute:** It affects the user's capability to execute the file or to view the file of a directory.

What are the symbolic links?

Ans: It will be redirected to another file using its path. Target files do not contain any data. Symbolic links redirect to another entry somewhere in the file system. If the target file is

deleted, the link to that file is removed, but not the file.

What are the hard links?

Ans: A hard link is another name for an existing file on Linux. We can create so many numbers of hard links, for any file. They can create links for other hard links.

Describe the root account?

Ans: The root is the user name, which default has access to all files and commands. The root user can do many things, but an ordinary user cannot do like installing software, changing file permissions, etc.

What are the different modes when using the vi editor?

Ans: There are three kinds of modes in vi editors. They are

- Command Mode/ Regular Mode
- Insertion Mode/Edit Mode.
- Ex Mode/ Replacement Mode

What are inode and process id?

Ans: The inode is a unique name given to each file and the process id is a unique name given to each process.

What are the Process states in Linux?

Ans: Five process states in Linux. They are

1. **New/ Ready:** A new process is created and ready to run.
2. **Running:** The process is being executed.
3. **Blocked/ Wait:** The process is waiting for input from the user.
4. **Terminated/ Completed:** The process completed the execution or terminated by the operating system.
5. **Zombie:** The process is deleted, but still the information regarding the process exists in the process table.

Explain File Permission groups in Linux?

Ans: There are three user-based permission groups for each file and directory.

They are:

1. **Owner:** Owners only will have to access the file or directory, they will not impact the

actions of other users.

2. **Group:** These permissions apply only to the group, that has been assigned to the file or directory. They will not impact the actions of other users.
3. **All Users:** These permissions are applied to all users on the system.

What Is a File system in Linux?

Ans: Linux file system stores and handles the data. Without a file system, it cannot know where the file starts from and where the file ends.

Explain different file system types in Linux?

Ans: In Linux, there are many file systems:

Ext, Ext2, Ext3, Ext4, JFS, XFS, btrfs, ufs, autofs, devpts, ntfs and swap.

Why LVM is required?

Ans: LVM stands for Large Volume Management, it is a storage management device. Users can create, resize, and delete LVM partitions. It increases abstraction, flexibility, and control. LVM is used to gather existing storage devices into the group and allocate logical units.

What is umask?

Ans: unmask stands for user file creation mode. When the user creates any file, it has default file permissions. So unmask will specify few restrictions to the newly created file (it controls the file permissions).

```
umask [-S] [mask]
```

How to set the mask permanently for a user?

Ans: If the unmask command invoked without any arguments, it means it will display the current mask.

To set the unmask permanently, we have two types.

They are:

- Ocotal representation.
- Symbolic representation.

What is network bonding in Linux?

Ans: Network Bonding is a process of combining more than two network interfaces to form a single network interface. It offers performance improvement and redundancy by increasing

network throughput and bandwidth.

No need to worry if one interface is down or unplugged because the other will work. The behaviour of the bonded interface depends on the bonding method.

How to check which ports are listening in my Linux Server?

Ans: We have two commands to check which ports are in listening in Linux Server. Following are the two commands

```
# netstat --listen
# netstat -l
```

How to share a directory using NFS?

Ans: To share a directory using NFS, first edit the configuration file and '/etc/exports' and add an entry like directory name '*/<directory-name>*'. Now restart the NFS service.

What are the default ports used for SMTP, DNS, FTP, DHCP, SSH, and squid?

Ans: Details mentioned below

How to lock a user account in Linux?

Ans: Locking user account is done for the security purpose so that unauthorized users cannot log in. So, we have a few ways to lock the user account. Some of them are below.

1. Lock or disable the password using passwd command.
2. Expire the user account using usermod command or chage command.
3. Changing the shell using nologin command (/sbin/nologin).

What is the tail command in Linux?

Ans: The Tail command print the last N number of lines of the given data, it prints 10 lines by default.

Syntax:

```
tail [OPTION]... [FILE]
```

What is grep command in Linux?

Ans: grep command is a filter that is used to the global search for regular expressions.

Syntax:

```
grep [options] pattern [files]
```

What is ps command in Linux?

Ans: The ps command displays the current process status of the system. And it displays the processes id's with some other related data also.

Syntax:

Ps [options]

What is lsof command in Linux?

Ans: lsof means List of files, we can know which file is opened by which process.

```
#lsof
```

What is a du command in Linux?

Ans: du command in Linux is used to retrieve more detailed information about which files use the disk space in a directory.

How do you list the contents of tar.gz and extract only one file?

Ans: Use these commands:

- tar tf file.tgz
- tar xf file.tgz filename

How do you change permissions under Linux?

Assuming you are the system administrator or the owner of a file or directory, you can grant permission using the chmod command. Use + symbol to add permission or – symbol to deny permission, along with any of the following letters: u (user), g (group), o (others), a (all), r (read), w (write) and x (execute). For example, the command chmod go+rw FILE1.TXT grants read and write access to the file FILE1.TXT, which is assigned to groups and others.

How do you terminate an ongoing process?

Every process in the system is identified by a unique process id or pid. Use the kill command followed by the pid to terminate that process. To terminate all process at once, use kill 0.

What is RAID in Linux?

The full form of RAID is the **Redundant Array of Independent Disk** that allows the system to combine the different physical disk drives into a logical unit. RAID is used to improve the system's disk performance and data integrity. There are **different RAID levels** you can

configure according to the requirements.

How do you secure a Linux server?

There are multiple methods to secure the Linux server and protect it from data breaches, security threats, and unauthorized access. Here are some of these methods:

1. Create a strong password
2. Update the server and apply security patches.
3. Use secured protocols like SSH and configure it to use key-based authentication for higher security.
4. Use the intrusion detection system (IDS) to monitor network traffic and prevent malicious activities.
5. Configure the firewall to limit the inbound and outbound traffic on the server.
6. Disable all unused network services.
7. Create regular backups.
8. Review logs and perform regular security audits.
9. Encrypt network traffic and enable monitoring.

How do you troubleshoot a Linux OS that fails to boot?

In case of the system boot failure, you can follow various approaches such as:

1. Check the warning and error messages you get during the boot process because it can help you diagnose the issues.
2. Check the boot logs to find the exact reason behind the boot error.
3. Open the GRUB bootloader and check the boot options to solve the booting problems.
4. Check the hardware connections like cables, RAM, cooling fan, etc.
5. If the system shows an error message related to the Kernel, try to boot it with the older Kernel version from GRUB.
6. Identify the last changes you made in the system before the boot.

What is the difference between UDP and TCP?

The following table shows the difference between UDP and TCP:

Factors	UDP	TCP
Connection-oriented	UDP does not establish a proper connection.	TCP is connection-oriented because it establishes a connection between the sender and receiver.
Reliability	UDP does not provide a reliability mechanism.	It guarantees reliable data delivery by retransmitting corrupt packets or lost packets.

Factors	UDP	TCP
Usage	It is used in low overhead, speed, and real-time communication applications.	It is used where ordered data is delivered, and reliable data must be delivered.
Applications	Video/voice conferencing, DNS, online gaming, streaming media, etc.	File transfers, email, web browsing, database transactions,

What is /etc/resolv.conf file

The /etc/resolv.conf is the config file used for the DNS server resolution process. This config file is used to specify the DNS server, set up the search directive for domains, and configure the resolver options.

What is the difference between /etc/passwd and /etc/shadow files?

The /etc/passwd file stores essential user information like usernames, user IDs, home directories, and default shells. Each line in the file represents a user account.

The /etc/shadow file contains encrypted passwords and other security-related information. It is only accessible by the root user or privileged processes

What is the sed command used for in Linux?

The sed command is used to perform text transformations on files. It can search for specific patterns and replace them with desired text.

For Example:

sed `s/foo/bar/g` file.txt

What is umask?

It is used for user file creation mode. When a user creates any file, then it has default file permission. Umask specifies restrictions for these permissions on the file, i.e., controls the permissions.

What is the purpose of the crontab file in Linux, and how do you schedule recurring tasks using cron jobs?

The crontab file in Linux is used to schedule recurring tasks or cron jobs. It contains a list of commands or scripts that are executed at specified time intervals. To edit the crontab file, you can use the crontab -e command.

For example: If we want to run a script name `jayesh.sh` every day at 5 AM, we can use the following procedure.

First, we need to open the crontab in editorial format.

crontab -e

Secondly, add the entries in the crontab file.

0 5 * * * /path/to/jayesh.sh

What is the purpose of the sudoers file in Linux, and how do you configure sudo access for

users?

The sudoers file in Linux controls the sudo access permissions for users. It determines which users are allowed to run commands with superuser (root) privileges. To configure sudo access, you can edit the sudoers file using the visudo command.

For example:

sudo visudo

What is the purpose of the netstat command in Linux, and how do you view network connections and listening ports?

The netstat command in Linux is used to display active network connections, routing tables, and listening ports. To view network connections and listening ports, use the netstat command with appropriate options.

For example: If we want to display all listening TCP ports, we can use the following command.

netstat -tuln

How do you set up a static IP address in Linux using the command-line interface?

To set up a static IP address in Linux using the command-line interface, you need to modify the network configuration file. The location and name of the file may vary depending on the Linux distribution, but commonly it is /etc/network/interfaces. Open the file with a text editor and modify the configuration to set a static IP address, subnet mask, gateway, and DNS servers.

For example:

iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8 8.8.4.4

How to check memory stats and CPU stats as a Linux Admin?

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

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

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

- Unmount the file system using the **unmount** command

- Use the **resize2fs** command as follows:

```
resize2fs /dev/mapper/myvg-mylv 10G
```

- Then, use the **lvreduce** command as follows:

```
lvreduce -L 10G /dev/mapper/myvg-mylv
```

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

We cannot restore the entire operating system from the tape backup device. Therefore, we should reinstall the core operating system and then restore the system configuration files and user data from the tape backup device.

What is YUM?

YUM stands for Yellowdog Updater Modified because it is based on YUP, the Yellowdog Updater. Yellowdog 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.

5. **Name default ports used for DNS, SMTP, FTP, SSH, DHCP and squid.**

Here are the default ports used for some common network services:

1. **DNS (Domain Name System):** Port 53 (both TCP and UDP) is used for DNS queries and responses.
2. **SMTP (Simple Mail Transfer Protocol):** Port 25 is the default port for SMTP, used for sending outgoing email.
3. **FTP (File Transfer Protocol):** Port 21 is used for the FTP control connection. Data transfers may use other ports, depending on the FTP mode (active or passive).
4. **SSH (Secure Shell):** Port 22 is the default port for SSH, used for secure remote access to a system.
5. **DHCP (Dynamic Host Configuration Protocol):** Port 67 (DHCP server) and Port 68 (DHCP client) are used for DHCP messages, allowing automatic IP address assignment to devices on a network.

6. **Squid (Web Proxy Cache):** Port 3128 is often used as the default HTTP port for Squid, a popular web proxy cache server.

It's important to note that while these are the default port numbers, some services and applications may be configured to use different ports based on administrator preferences or specific network configurations. Additionally, for services running over SSL/TLS, different port numbers may be used for the secure versions (e.g., SMTPS over port 465, HTTPS over port 443)

Elaborate about sgid and suid terms?

Answer: Talking about suid, it offers the same level of ownership permissions while a user executes a file. Coming to the sgid, it comes with a group of privileges of a completed file. It inherits the ownerships while developing the directory.

How will you create a partition of 100MB and mount it?

Answer:

1. Use the command "partprobe" and then mkfs -t ext3 /dev/hda?
2. First, to create a new partition, the users need to use fdisk /dev/had.
3. Now, for the new partition, type "n."
4. Then, the users need to select between primary or logical partition. There, press "1" to go for a logical partition.
5. It will then ask to choose the starting cylinder type. Keep it default by pressing "Enter."
6. Now, the users need to put the size. Put +100M then press "P" for verification of the partition list and name.
7. To write the partition on the partitions table, press "W."

What are the basic networking concepts a Linux admin should be familiar with?

A7. A Linux admin should be familiar with the following basic networking concepts:

1) IP addressing and subnets
2) Network interfaces and configuration files
3) Routing and gateways
4) Domain Name System (DNS)
5) Network File System (NFS)
6) DHCP server configuration
7) Network troubleshooting tools, such as ping, traceroute, netstat, nslookup, tcpdump, and ifconfig

How do you install and update packages using a package manager in Linux?

Ans:Package managers are used to manage software packages in Linux. The most common package managers are apt for Debian-based distributions and yum or dnf for Red Hat-based distributions. Here are examples for each:

sudo apt update # Update package list sudo apt upgrade # Upgrade installed packages sudo apt install package-name # Install a package sudo apt remove package-name # Remove a package

- Using yum or dnf:

sudo yum update # Update package list and upgrade installed packages sudo yum install package-name # Install a package sudo yum remove package-name # Remove a package.

How do you set up a database server in Red Hat Linux?

Setting up a database server in Red Hat Linux involves several steps, such as the follows:

1. **Install the necessary software**: Install the database server software of your choice. For example, to install MySQL you can use the command “yum install mysql-server”
2. **Start the database service**: Use the command “systemctl start mysqld” to start the MySQL service and “systemctl enable mysqld” to start the MySQL service automatically at boot time.
3. **Secure the database**: Run the command “mysql_secure_installation” to set a root password and remove any test databases and users.
4. **Create a new database**: Connect to the MySQL server using the command “mysql -u root -p” and then use the SQL command “CREATE DATABASE database_name;” to create a new database.
5. **Create a new user**: Use the SQL command “CREATE USER ‘username’@’hostname’ IDENTIFIED BY ‘password’;” to create a new user.
6. **Grant permissions to the user**: Use the SQL command “GRANT ALL PRIVILEGES ON database_name.* TO ‘username’@’hostname’;” to grant all privileges to the new user for the newly created database.
7. **Reload the privileges**: use the SQL command “FLUSH PRIVILEGES;”

How do you configure a DNS server in Red Hat Linux?

Configuring a DNS server in Red Hat Linux involves several steps, such as below:

1. Install the necessary software
2. Configure the DNS server
3. Create zones and records
4. Start the DNS service
5. Testing the server

List the fields in /etc/passwd file.

ANS : UserName | Password | UserID | GroupID | Comments | HomeDir | LoginShell

How to lock an user account?

ANS: This can be done by using either “usermod -L <UserName>” or “passwd -l <UserName>” commands.

Example:-

#usermod -L mango

Once an account gets locked, there would be an exclamation mark before the encrypted password files in “/etc/shadow” as shown below:

mango:!1O5zV5Rj/$XhuRe8Og.AiXMXDGSIsae/:16266:0:99999:7:::

To un-lock an account:-

#usermod -U mango

Whenever an user tries to login via terminal, system would throw up the error “The account is currently not available”, otherwise, via GUI when user enters password, it looks to be logging in, however, comes back to the login prompt. How could this issue be fixed?

ANS: This is because of the shell field set as “/sbin/nologin” in “/etc/passwd” file, so change this back to “/bin/bash” and user should be allowed to login.

If the shell field is set as “/bin/false” then whenever an user tries to login there would not be any error or messages, it just comes back to the login prompt and same happens in GUI mode.

Create users home directory in /home1 directory instead of default /home directory. This gets applicable to any new users who gets created i.e the home directory of that user should

be /home1/<UserName>/

ANS: – Edit /etc/default/useradd

– Change the line : HOME=/home1

– Save the changes and exit. After this any new users home directory would be under /home1

– You could check the useradd defaults using the command :#useradd -D

How do you make/grant complete access (rwx) on files created for a user and deny any level of access to others including group?

ANS : – Need to define the umask value for the required user.
– This can be done by editing .bash_profile file.

For example, if we need to define this for a user "mmurthy" then we need to edit this file "/home/mmurthy/.bash_profile" and define umask as given below (assuming that the default home directory location is not changed):

umask 0077

– Save and exit the file.
– Next time this user logs in, files/directories would get exclusive permissions only for this user as masked by umask parameter.
– For root user the umask is defined in "/etc/init.d/functions" file. Otherwise, in /etc/profile (login shell) or /etc/bashrc (non-login shell) file.

By default log files are set to get rotated on weekly **basis, how to make this gets rotated on** monthly **basis?**

ANS: Edit /etc/logrotate.conf and change below lines

rotate log files monthly
monthly

Save changes and if you want to rotate the log files immediately then run the command:

#logrotate -f /etc/logrotate.conf

How do you check the boot messages (kernel ring buffer)?

ANS:- Using “dmesg” or #cat /var/log/dmesg

How to increase size of ‘kernel ring buffer’ file (dmesg)?

ANS:- By default the kernel ring buffer size is 512 bytes. So, to increase this space add “log_buf_len=4M” to the kernel stanza in grub.conf file.

Where is grub.conf/grub.cfg file stored in RHEL systems?

ANS : In /boot/grub/ OR /etc/grub2 (in case of RHEL7.x) directory.

How can you permanently set the umask for a user?

Answer. In order to permanently set the umask for a user, we need to put in the right profile file that highly depends on the default shell of a particular user.

What are suid and sgid terms?

Answer:

suid provides the same permissions as the owner of a file is having when the file is executed by the user.

Sgid inherits the group privileges of the file on execution. It inherits the group ownership of directories when a file is created within the directory.

Which file is used to automatically mount file systems?

Ans. Fstab file will automatically mount file systems

What is the difference between the home directory and the working directory?

Ans. The home directory is the default working directory when a user logs in.

The working directory is the user's current directory.

Why do we use /etc/resolv.conf and /etc/hosts files?

Ans. /etc/resolv.conf files contain the nameserver details and are used for configuring the DNS name servers. /etc/hosts files translate and map hostnames/domain names to the relevant IP address.

What is the procedure to convert the default run level in Linux?

Ans: We can use the init command to convert the default run level in Linux.

Mention some Linux file content commands.

Ans: Following are some file content commands:

1) **head:** Display the top lines of the file.
2) **tail:** Display the last lines of the file.
3) **cat:** Concatenate more than two files.
4) **more**: Display the content in pager form to view in the terminal.

Explain what PIPE in Linux is?

Ans: A pipe is a form of redirection in Linux, it is mainly used to combine two or more two commands, and the output of one command can take as input to the next command.

Explain lsof command in Linux?

Ans: lsof command lists the open files assigned to the application. It also lists the processes that opened them.

What is Secure Shell (SSH)? How can we connect to a remote server through Secure Shell?

Ans. Secure Shell (SSH) is a protocol for securely connecting to remote servers and enabling

communication between two systems. It is one of the most common methods to access remote Linux servers. It transmits data over encrypted channels leading to high-level security. You will require a domain name and IP address to connect to a remote server through a secure shell (SSH).

What is an inode?

Ans. Inode is the short form of index node. It can be defined as a record in a disk table. In terms of Linux, inodes manage the metadata of the file. Every Linux directory has a file name and an inode number.

The inode number has these attributes.

1) Size of the file
2) Owner of the file
3) Disk Location
4) Types of files
5) No. of links
6) Date and time
7) File metadata

How To check the default gatway ?

Ans: Using 'route -n' command we can determine the default gateway in linux.

Which Command is used to check the kernel Version ?

Ans: 'uname -r'

How to check the current runlevel of a linux box ?

Ans : 'who -r' and 'runlevel' , both of these command are used to find current run level

What is the procedure to convert the default run level in Linux?

Ans: We can use the init command to convert the default run level in Linux.