Module 16 Linux server - Operate running systems

1. **What is PID ?**
    - PID stands for "Process IDentifier." It is a unique numerical identifier assigned to each running process on a Linux system. The PID is used by the operating system to keep track of and manage processes.

2. **What is PPID?**
    - PPID stands for "Parent Process ID." It is a numerical identifier assigned to the parent process of a running process on Linux like operating systems. PPID indicates which process spawned or created the running process, establishing a parent-child relationship within the process hierarchy. Understanding PPIDs is essential for process management and tracking how processes are related to each other on Linux systems.

3. **What is the use of “ ps “ command ?**
    - The "ps" command in Linux provides essential process status information, listing running processes along with their unique Process IDs (PIDs), resource utilization, execution times, and more. It aids in process monitoring, troubleshooting, and management by helping users identify resource-heavy processes, track parent-child relationships, and diagnose system issues. With various options, it offers flexibility for customized process information retrieval, making it a crucial tool for system administrators, developers, and users to monitor and control processes efficiently.

4. **What is the use of “ ps aux “ command ?**
    - The "ps aux" command in Linux is used to list all running processes along with detailed information. It provides a comprehensive view of the system's processes, displaying their Process IDs (PIDs), user ownership, CPU and memory usage, and the command that initiated each process. This command is particularly useful for system administrators and users to gain an overview of all active processes, identify resource-intensive tasks, and investigate system performance or issues.

5. **What is the use of “ tops “ command ?**
    - The "top" command in Linux is a powerful real-time system monitoring tool that offers a comprehensive view of system resource usage and running processes. Its main uses are:
    - Real-Time Monitoring: "top" continuously updates and displays crucial system performance metrics, including CPU usage, memory consumption, swap space

utilisation, and more. This real-time insight allows administrators and users to detect resource bottlenecks and performance issues as they occur.

- Process List: "top" provides a detailed list of running processes, listing their Process IDs (PIDs), associated users, CPU and memory usage, and command names. This helps in identifying resource-intensive processes and understanding their impact on system performance.
- Interactive Control: Users can interact with "top" in real-time, enabling them to send signals to processes (e.g., to terminate them), change the sorting order of the process list, and dynamically adjust display settings to suit their needs. This interactivity makes "top" a versatile tool for system management and troubleshooting.
- System Information: Alongside process details, "top" offers system-level information such as system uptime, load averages, and the number of logged-in users. This summary helps assess the overall health of the system.
- Sorting and Filtering: Users can sort and filter the process list based on various criteria, such as CPU usage or process name, making it easier to focus on specific aspects of system performance.

6. **Which command is used to change priority value ?**
    - The "renice" command is used to change the priority value (niceness) of a running process in Linux. Niceness is a value that determines the priority of a process, affecting its CPU scheduling. A lower niceness value indicates higher priority, while a higher niceness value indicates lower priority.
    - Example:
    - renice priority_value -p process_id

7. **What is the use of “jobs” command ?**
    - The "jobs" command in Linux is used to display the list of background jobs that are currently running or suspended in the current shell session. It is particularly useful when you have multiple processes running in the background and you want to keep track of their status or bring them to the foreground for interaction.

8. **What is the use of grep command ?**
    - The grep command in Linux and Unix-like operating systems is used to search for text patterns within files and streams of text. Its primary purpose is to locate and display lines of text that match a specified pattern or regular expression.

Module 16 Linux server - Operate running systems

9. What is daemons?

- daemon is a background process that runs continuously without direct user interaction. Daemons perform various tasks and services essential for the proper functioning of the Linux operating system.

10.I want to check the service status for" sshd", which will help me?

- To check the service status for "sshd" (the SSH daemon) in Linux, you can use the systemctl command. systemctl is the standard service management utility in many modern Linux distributions. Here's how you can use it to check the status of the SSH daemon.
- Example:-
- systemctl status sshd

11.How to stop and start services in terminal?

- In the terminal on Linux systems, you can use the systemctl command to stop and start services. Here's how to do it:
- Systemctl start ssh
- Systemctl stop ssh

12.What is the use of openSSH ?

- OpenSSH (Open Secure Shell) is a widely used and open-source software suite that provides secure network communication, primarily for remote login and file transfer. It is a critical tool for system administrators, developers, and anyone who needs to access and manage remote servers or network devices securely.

13.Which command is used to generate key in linux ?

- In Linux, you can use the ssh-keygen command to generate SSH keys. SSH keys are commonly used for authentication and secure communication with remote servers. Here's how you can use the ssh-keygen command to generate an SSH key pair.

14.Which command is used to copy ssh key?

- **ssh-copy-id user@hostname**

Module 16 Linux server - Operate running systems

15.How do we prohibit the root user from logging in using ssh?

- To prohibit root user SSH login:
- 1. **Connect to server:** Log in as a user with sudo privileges.
-
- 2. **Edit SSH config:** Open the SSH server configuration file, usually located at `/etc/ssh/sshd_config`.
- 3. **Find PermitRootLogin:** Locate the line that says `PermitRootLogin yes`. Change it to `PermitRootLogin no`.
- 4. **Restart SSH:** Save the changes and restart the SSH service with `sudo service ssh restart` or `sudo systemctl restart sshd`.
- Now, the root user will be prohibited from logging in via SSH for enhanced security.

16.How do we prohibit password authentication using ssh?

- To prohibit password authentication and enforce the use of SSH keys for authentication in SSH, follow these steps. This enhances security by eliminating the possibility of brute-force password attacks.
- Connect to server: Log in as a user with sudo privileges.
- Edit SSH config: Open the SSH server configuration file, usually at /etc/ssh/sshd_config.
- Disable PasswordAuthentication: Set PasswordAuthentication no.
- Restart SSH: Save changes and restart SSH with sudo service ssh restart or sudo systemctl restart sshd.
- Now, SSH password authentication is disabled, and users must use SSH keys for authentication.

17.Where we find general logs ?

- General system logs in a Linux system are typically located in the /var/log directory. These logs provide information about various aspects of the system's operation, including system messages, hardware events, login attempts, and more.

18.Where we find secure logs ?

- Secure logs are often stored in /var/log/secure.

Module 16 Linux server - Operate running systems

19. Where we find mail log ?

- Mail logs on Linux systems are often located in the /var/log directory, and the specific log file can vary depending on the mail server software you are using.

20. Where we find scheduling logs?

- System-wide cron logs are often found in /var/log/cron
- The at command, which schedules one-time tasks, typically logs its activities in /var/log/atd.log.

21. Where we find booting logs?

- boot logs may be found in /var/log/boot.log.

22. What is the use of “lastb” command ?

- The lastb command in Linux is used to display the list of failed login attempts on the system. It reads the /var/log/btmp file, which records unsuccessful login attempts, and presents this information in a readable format. Each entry typically includes the username, terminal or IP address, date, and other relevant details about the failed login attempt.

23.Remote host is “NADIAD”, Remote user is “KAMAL, how to access remote user via ssh?

- ssh KAMAL@NADIAD

24.What is the use of “w -f “command ?

- The w command in Linux is used to display information about currently logged-in users and their activities. When used without any options, it provides a list of logged-in users, their terminal sessions, login times, idle times, and the commands they are currently running.
- The -f option in the w command allows you to display additional information about the command associated with each terminal session. It shows the command name and its arguments, providing more context about what each user is doing. This can be helpful when you want to see not only who is logged in but also what specific processes or commands are running.

Module 16 Linux server - Operate running systems

25. What is “SSHS host keys “?

- SSH host keys, often referred to as SSH host key pairs, are a critical component of the SSH (Secure Shell) protocol. They play a fundamental role in securing the communication between SSH clients and servers. SSH host keys are used to verify the authenticity of the remote server and establish secure encrypted connections.

26. What is the default location for server’s public key in client side?

- ~/.ssh/known_hosts

27. I want to fire “ls -l /etc” command on remote host “desktop” .

- ssh desktop "ls -l /etc"

28.What is the use of this command “ #journalctl --since today “.

- The command journalctl --since today is used to display journal entries (logs) from the systemd journal that have been recorded since the beginning of the current day. The systemd journal is the logging system used by systemd-based Linux distributions to manage system and service logs.

29. What is “ chronyd “?

- chronyd is a computer program for maintaining the accuracy of the system clock (system time) in Unix-like operating systems. It is commonly used on Linux systems as a replacement for the older ntpd (Network Time Protocol daemon) for time synchronisation.

30. Full form of NTP.

- The full form of NTP is "Network Time Protocol."

31. Port number for NTP is…

- The default port number for NTP (Network Time Protocol) is UDP port 123.

32. I want to check timzone, which command will help me ?

- To check the timezone of your system on a Linux or Unix-based system, you can use the timedatectl command.

33.How to set timezone? Give a comman….

- timedatectl set-timezone your_timezone

Module 16 Linux server - Operate running systems