Monitor System Resources:

top

- **Basic Usage:**
  - top: Opens an interactive real-time view of system resource usage.
- **Description:**
  - The top command provides a live, real-time view of your system's resource usage. It shows information on CPU usage, memory usage, running processes, and system uptime. You can sort and filter this information interactively.
- **Example:**
  - Press M within top to sort by memory usage, or P to sort by CPU usage.

2. htop

- **Basic Usage:**
  - htop: Launches an interactive, colorful view of system resources.
- **Description:**
  - htop is an enhanced, more user-friendly version of top. It offers a color-coded display, better visualizations, and easier navigation through processes. It shows CPU, memory, swap usage, and process details in a visually appealing manner.
- **Example:**
  - Use arrow keys to navigate through processes, and F9 to kill a selected process in htop.

3. vmstat

- **Basic Usage:**
  - vmstat 5: Reports system resource usage every 5 seconds.
- **Description:**
  - vmstat (Virtual Memory Statistics) reports information about processes, memory, paging, block I/O, traps, and CPU activity. It provides a snapshot of system performance and is useful for diagnosing performance issues.
- **Example:**
  - vmstat 1 10: Reports system statistics every second for 10 seconds.

4. iostat

- **Basic Usage:**
    - iostat: Displays CPU and I/O statistics.
- **Description:**
    - iostat (Input/Output Statistics) provides detailed information about CPU utilization and input/output (I/O) statistics for devices and partitions. It helps in understanding the performance of disk subsystems and identifying bottlenecks.
- **Example:**
    - iostat -x: Shows extended statistics, including the percentage of CPU time spent on I/O operations.

5. free

- **Basic Usage:**
    - free -h: Displays memory usage in a human-readable format.
- **Description:**
    - The free command provides information about the total amount of free and used physical and swap memory in the system, as well as the buffers and caches used by the kernel. It's a quick way to see how much memory is available.
- **Example:**
    - free -m: Displays memory usage in megabytes.

6. sar

- **Basic Usage:**
    - sar -u 1 3: Displays CPU usage every second for 3 seconds.
- **Description:**
    - sar (System Activity Reporter) is part of the sysstat package and collects, reports, or saves system activity information. It can report on CPU, memory, I/O, network, and other system resources over time.
- **Example:**
    - sar -r 5: Reports memory statistics every 5 seconds.

7. nmon

- **Basic Usage:**
    - nmon: Opens an interactive view of various system resources.

- **Description:**
    - nmon (Nigel's Performance Monitor) is a powerful tool that provides real-time monitoring of CPU, memory, disk I/O, network, file systems, NFS, and other system resources. It's especially useful for performance analysis and troubleshooting.
- **Example:**
    - After launching nmon, press c to view CPU usage, m for memory, d for disks, etc.

8. dstat

- **Basic Usage:**
    - dstat: Displays various system resource statistics in real-time.
- **Description:**
    - dstat is a versatile resource monitoring tool that provides real-time statistics for CPU, memory, disks, network, and more. It combines the functionality of tools like vmstat, iostat, netstat, and ifstat.
- **Example:**
    - dstat --cpu --mem --net: Displays CPU, memory, and network statistics in real-time.

Monitor Running Processes:

1. ps

- **Basic Usage:**
    - ps: Lists the currently running processes for the current user.
    - ps aux: Displays detailed information about all running processes.
    - ps -ef: Another way to show all running processes with full format listing.
- **Description:**
    - The ps command provides a snapshot of current processes. It's highly flexible, allowing you to view processes based on different criteria like user, CPU usage, memory usage, etc.
- **Example:**
    - ps aux | grep firefox: This will show all processes related to Firefox.

2. top

- **Basic Usage:**
    - top: Opens an interactive real-time view of running processes.
- **Description:**
    - The top command provides a dynamic view of system processes, updating in real time. It shows information like CPU usage, memory usage, and process IDs, and allows you to sort and filter the processes interactively.
- **Example:**
    - Within top, you can press M to sort by memory usage or P to sort by CPU usage.

3. htop

- **Basic Usage:**
    - htop: Launches an interactive, colorful view of system processes.
- **Description:**
    - htop is an enhanced version of top, providing a more user-friendly, visually appealing interface. It allows for easier navigation, filtering, and killing of processes.
- **Example:**
    - Use arrow keys to navigate and F9 to kill a selected process in htop.

4. pgrep

- **Basic Usage:**
    - pgrep firefox: Finds process IDs of processes with names matching "firefox".
- **Description:**
    - The pgrep command is used to search for processes based on their name or other attributes. It's useful for quickly finding and managing specific processes.
- **Example:**
    - pgrep -l ssh: Lists the process IDs and names of all processes containing "ssh".

5. pstree

- **Basic Usage:**
    - pstree: Displays processes in a tree format.
- **Description:**
    - pstree shows running processes as a tree, which makes it easier to see the relationship between parent and child processes.

- **Example:**
    - pstree -p: Shows the tree with process IDs.

6. kill

- **Basic Usage:**
    - kill PID: Sends a signal to terminate a process with the given Process ID (PID).
- **Description:**
    - The kill command is used to send signals to processes, often to terminate them. By default, it sends a SIGTERM signal, but it can be used to send other signals as well.
- **Example:**
    - kill -9 1234: Forcefully kills the process with PID 1234.

7. nice and renice

- **Basic Usage:**
    - nice -n 10 command: Runs a command with a lower priority.
    - renice 10 -p 1234: Changes the priority of an already running process with PID 1234.
- **Description:**
    - nice and renice commands are used to start a process or change the priority of running processes. Lower priority means the process will get less CPU time.
- **Example:**
    - nice -n -5 make: Runs the make command with a higher priority.

Example: Using ps to Monitor Processes

ps aux | grep httpd

This command lists all processes related to the Apache HTTP server.

<u>Monitor Network Connections:</u>

1. netstat

- **Basic Usage:**

- netstat -tuln: Lists all listening ports with TCP/UDP protocols.
- netstat -an: Shows all active connections and listening ports.
- netstat -at: Displays only TCP connections.
- netstat -au: Displays only UDP connections.

- **Description:**
  - netstat is a command-line tool that provides various network statistics, including current active connections, listening ports, routing tables, and more. It's widely used for troubleshooting network issues.

2. ss (Socket Statistics)

- **Basic Usage:**
  - ss -tuln: Shows listening TCP and UDP ports.
  - ss -s: Provides summary statistics.
  - ss -at: Lists all TCP connections.
- **Description:**
  - ss is a modern alternative to netstat with similar functionality. It's faster and provides more detailed information about network connections, making it a preferred choice for many users.

3. lsof

- **Basic Usage:**
  - lsof -i: Displays all network connections.
  - lsof -iTCP -sTCP:LISTEN: Shows only listening TCP ports.
  - lsof -i :80: Lists processes using port 80.
- **Description:**
  - lsof (List Open Files) is a versatile command that can be used to list all open files and network connections on the system. It's particularly useful for identifying which processes are using specific ports.

4. iftop

- **Basic Usage:**
  - sudo iftop: Displays a real-time view of network traffic.
- **Description:**

- iftop is a real-time console-based network bandwidth monitoring tool. It shows a list of network connections with their data transfer rates, which is useful for monitoring bandwidth usage.

5. tcpdump

- **Basic Usage:**
  - sudo tcpdump -i eth0: Captures packets on the eth0 interface.
  - sudo tcpdump -n -v: Provides a verbose output with IP addresses instead of hostnames.
- **Description:**
  - tcpdump is a packet analyzer that captures and displays packet data from a network interface. It's powerful for diagnosing network issues at a packet level.

6. ip (iproute2)

- **Basic Usage:**
  - ip a: Displays all IP addresses on the system.
  - ip route: Shows the routing table.
  - ip -s link: Displays statistics for network interfaces.
- **Description:**
  - The ip command, part of the iproute2 package, is a versatile tool for network configuration and monitoring. It can replace older tools like ifconfig, route, and netstat for many tasks.