LINUX

PROCESS MANAGEMENT AND NETWORK MANAGEMENT

LORDSON DAVID R
LORDSONDAVID.WORK@GMAIL.COM

Linux

Process Management

Introduction

Process management in Linux is about observing and controlling the execution of programs (processes). Linux provides various commands to monitor CPU/memory usage, manage running processes, and terminate them if needed.

Let’s Get Dive into Commands

ps – View Running Processes

1. Purpose

The ps (process status) command is used to display information about active processes on a Linux system. It provides a snapshot of the current processes, unlike top, which updates dynamically.

2. Syntax

```
ps [options]
```

3. Common Options

Command	Meaning
aux	List all running processes from all users, showing user, PID, CPU, memory usage, and command.
-ef	Show full format listing with detailed information.
-u username	Display processes belonging to a specific user.
-eo pid,cmd	Show only the Process ID (PID) and the command name.

3. Examples

Command	Meaning
ps	Show current shell processes
ps aux	List all running processes
ps -ef	Display full-format list of processes
ps -u username	Show processes for a specific user
ps -eo pid,cmd	Display only PID and command columns

top – Real-Time Process Monitor

1. Purpose

The top command is used to monitor real-time system performance, including CPU usage, memory usage, and details of currently running processes. It provides a dynamic view of the system's resource usage, which updates every few seconds.

2. Syntax

```
top [options]
```

3. Examples

Command	Meaning
top	Show dynamic real-time process list with CPU and memory usage.
top -u username	Show processes belonging to a specific user dynamically.

free – Check Memory Usages

1. Purpose

The free command displays information about the system's memory usage, including:

- **Total memory** (RAM),
- **Used memory**,
- **Free memory**,
- **Shared memory**,
- **Buffers/cache**,
- **Swap space** (used and free).

It provides a quick snapshot of how much physical memory and swap space your system is currently using or has available, helping you

monitor system performance and troubleshoot memory-related issues.

2. Syntax

```
free [options]
```

3. Examples

Command	Meaning
free	Show memory and swap usage.
free -h	Show memory in human-readable format
free -m	Display memory in

	megabyte.
free -g	Display memory in gigabytes

kill – Terminate a Process by PID

1. Purpose

The kill command is used to send signals to running processes, most commonly to terminate (stop) a process by specifying its Process ID (PID). While its primary use is to end processes, it can send other signals for different actions.

2. Syntax

```
kill [signal] PID
```

3. Examples

Command	Meaning
kill 1234	Terminate the process with PID 1234
kill -9 1234	Forcefully kill process with PID 1234
kill -15 1234	Gracefully stop process with PID 1234

pkill – Kill by Process Name

1. Purpose

The pkill command is used to send signals to processes by matching their names or other attributes rather than specifying the process ID (PID). It is commonly used to kill all processes whose names match a given pattern.

2. Syntax

```
pkill [options] process_name
```

3. Examples

Command	Meaning
pkill firefox	Kill all processes named firefox
pkill -u root	Kill all processes belonging to user root
pkill -f server.py	Kill processes by full command match

swapon/swapoff – Manage Swap Space

1. Purpose

The swapon and swapoff commands are used to enable or disable swap areas (partitions or files) on a Linux system. Swap space acts as an overflow area on disk when physical RAM is fully used, helping maintain system stability.

2. Syntax

```
swapon [options] [file/device]

swapoff [options] [file/device]
```

3. Examples

Command	Meaning
swapon -s	Show active swap areas
swapon /swapfile	Enable a swap file
swapoff /swapfile	Disable a swap file

nice & renice – Change Process Priority

Purpose

- `nice` is used to **start a new process with a specified priority** (also called niceness), influencing how the Linux scheduler allocates CPU time.

- `renice` is used to **change the priority (niceness) of an already running process.**

Syntax

```
nice [options] command

renice [priority] -p PID
```

3. Examples

Command	Meaning
nice -n 10 command	Run command with lower priority
renice +5 1234	Lower the priority of process 1234

Linux

Network Management

Introduction

In Linux, network management tools are essential for monitoring, configuring, and troubleshooting network-related components. These tools help administrators understand the state of the system's network interfaces, bandwidth usage, open ports, and traffic flow. This section covers practical commands such as netstat, iostat, ifconfig, and more.

1. Viewing Network Connections

netstat - (Network Statistics)

1. Purpose

The netstat command displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

2. Use Case

- Check open ports and listening services.
- Monitor incoming and outgoing connections.
- View routing information.

3. Common Options

Command	Meaning
-t	Show TCP connections.
-u	Show UDP connections.
-l	Show only listening sockets.
-n	Show numerical

	addresses.
-p	Show the PID and name of the program.

4. Examples

Command	Meaning
netstat -tun	Displays all active TCP and UDP connections with numerical IPs and ports.
netstat -tuln	Lists all TCP/UDP ports the system is currently listening on (useful for server diagnostics).
sudo netstat -tulpn | grep :80	Find which process is using port 80 (HTTP).
netstat -i	Displays statistics

	about each network interface (like packets sent/received).
netstat -r	Displays the kernel IP routing table (similar to route -n).
netstat -g	Useful for analyzing multicast traffic and group memberships.
netstat -a	Lists all active sockets, including UNIX domain sockets (e.g., inter-process communication).
netstat -at netstat -au	-at: Show only TCP connections -au: Show only UDP connections

2. Monitoring Disk and I/O Stats

iostat - (Input/Output Statistics)

1. Purpose

The iostat command provides CPU statistics and I/O statistics for devices and partitions. It helps to monitor system performance, especially in diagnosing disk I/O bottlenecks.

2. Use Case

- Monitor disk read/write throughput
- Identify high disk usage devices
- Check CPU wait time caused by I/O delays
- Understand the load distribution between CPU and I/O operations

3. Syntax

```
iostat [options] [interval] [count]
```

4. Common Options

Command	Meaning
-x	Show extended statistics, including utilization, IOPS, and

	latency
-d	Display only device statistics
-c	Display only CPU statistics
-p	Show stats for all partitions
-k / -m	Show Values in kB or MB
Interval count	Report stats at specified intervals and repetitions

5. Examples

Command	Meaning
iostat -xd 2 5	Monitor extended I/O stats (e.g., %util,

	await, r/s, w/s) for each disk every 2 seconds, five times.
iostat -c	View how much time the CPU spends in user, system, idle, and I/O wait modes.
iostat -d	View read/write rates for devices without CPU stats.
iostat -m -p	View I/O statistics in megabytes per second, including for all partitions (like /dev/sda1, /dev/sda2).
iostat -xd 1	Live monitoring of extended disk I/O stats every second (press Ctrl+C to stop).

3. Configuring Network Interfaces

ip - (IP Routing & Network Device Configuration)

1. Purpose

The ip command is used to **display**, **configure**, **and manage** network interfaces, IP addresses, and routing rules. It replaces the older ifconfig, route, and related tools.

2. Use Case

- Display IP address and MAC address for interfaces
- Assign or delete IP addresses
- Enable or disable network interfaces
- View or modify routing tables
- Inspect link status and statistics

3. Syntax

```
ip [OBJECT] [COMMAND] [OPTIONS]
```

4. Common Objects

Command	Meaning
addr	Manage IP addresses

link	Manage network interfaces
route	Manage routing tables

5. Examples

Command	Meaning
ip addr show # or simply ip a	Displays IPv4/IPv6 addresses, MAC addresses, interface names and states.
ip addr show dev eth0	Shows IP configuration of the eth0 interface only.
sudo ip addr add 192.168.1.100/24 dev eth0	Assigns an IP to eth0 (will not persist after reboot unless added

	to config files).
sudo ip addr del 192.168.1.100/24 dev eth0	Removes the assigned IP from the interface.
sudo ip link set eth0 up	Enables the interface (equivalent to ifconfig eth0 up).
sudo ip link set eth0 down	Disables the interface.
ip link show	Shows MAC address, MTU, and operational status of all interfaces.
sudo ip link set dev eth0 address 00:11:22:33:44:55	Temporarily change the MAC address of the interface.
ip route	Lists current routes configured on the system.

4. Resolving Hostnames and Testing Connectivity

ping

1. Purpose

The ping command is used to test the reachability of a remote host over a network. It also helps measure packet loss and network latency (round-trip time).

2. Use Case

- Check if a host is online or reachable
- Diagnose DNS resolution issues
- Measure round-trip time and latency

- Detect packet loss or high network delay

3. Syntax

```
ping [options] <hostname or IP>
```

4. Common Options

Command	Meaning
-c	Number of packets to send
-i	Interval between packets
-s	Packet size in bytes
-D	Print timestamps
-f	Flood ping (root only)

-q	Quiet mode, only summary output

5. Examples

Command	Meaning
ping google.com	Tests internet connectivity and DNS resolution. You'll see responses with latency in milliseconds.
ping 8.8.8.8	Verifies network connectivity without relying on DNS.
ping -c 4 google.com	Sends exactly 4 echo requests and stops automatically (useful in scripts).

ping -s 128 google.com	Sends packets of 128 bytes instead of the default 56 (to test MTU or bandwidth stability).
sudo ping -f google.com	Sends packets as fast as possible (use carefully, only for internal testing).
ping -D google.com	Each line will be prefixed with a timestamp — useful for logging and analyzing patterns.

traceroute

1. Purpose

traceroute maps the path that packets take from your system to a remote host. It shows each hop (router or gateway) along the way and measures the delay (latency) at each step.

2. Use Case

- Identify where network delay or failure occurs
- Trace routing problems (e.g., wrong path, unreachable node)
- Detect long hops or ISP issues

- Understand how data travels across the internet or within your LAN

3. Syntax

```
traceroute [options] <hostname or IP>
```

4. Common Options

Command	Meaning
-n	Show only IP addresses (no DNS lookup) - Faster
-m	Set maximum hop count (default: 30)
-w	Set wait time (in seconds) for each

	reply
-I	Use ICMP ECHO instead of UDP
-T	Use TCP SYN packets instead of UDP (useful for firewalled targets)

5. Examples

Command	Meaning
traceroute google.com	This shows each router your request passes through on its way to Google.
traceroute 8.8.8.8	Helpful if DNS resolution is down or you're testing a raw IP connection.

traceroute -n google.com	Faster output with raw IPs only.
sudo traceroute -I google.com	This behaves more like ping and works better on some networks.
sudo traceroute -T -p 80 google.com	This sends TCP SYN packets to port 80, useful if ICMP/UDP is blocked.

nslookup

1. Purpose

nslookup (Name Server Lookup) is a network utility used to query DNS servers to get:

- IP addresses from domain names (forward lookup)

- Domain names from IP addresses (reverse lookup)
- DNS record details (like A, MX, NS, etc.)

2. Use Case

- Check if a domain resolves correctly
- Diagnose DNS resolution issues
- Identify mail servers (MX records) or name servers (NS records)
- Perform reverse lookups to verify hostnames from IPs

3. Syntax

```
nslookup [hostname or IP]
```

4. Common Options

Record Type	Meaning
A	IPv4 address record
AAAA	IPV6 address record
MX	Mail exchange record
NS	Name Server
CNAME	Canonical name(alias)
PTR	Pointer for reverse DNS

5. Examples

Command	Meaning
nslookup example.com	This command queries your DNS server to

	find the **IP address** associated with example.com.
nslookup 8.8.8.8	Gets the domain name mapped to the IP (if available).
nslookup example.com 1.1.1.1	Queries Cloudflare's DNS instead of your system default.
nslookup Then, at the prompt: > set type=MX > gmail.com	Look up Mail Exchange (MX) records for a domain.