The find command:

The find command is used to search and locate the list of files and directories based on conditions you specify for files that match the arguments.

find command can be used in a variety of conditions like you can find files by permissions, users, groups, file types, date, size, and other possible criteria.

IP = Internet Protocol

what is an IP?

Ans: An IP address is a unique 32-bits number assign dynamically by a DHCP SERVER or staticly by an Admin to a

     device on a network

$sudo find / -name "\*file.yaml" --> find from root any file with extension file.yaml

$sudo find / -name etechfile.yaml  -->search all directories in your OS

$sudo find . -name etechfile.yaml   -->Find all the files whose name is etechfile.yaml in a current working directory.

$sudo find /tmp -name etechfile.yaml  -->Find all the files under /tmp directory with the name etechfile.yaml.

$sudo find $(pwd) -mtime -2         -->find and delete files that are less than 2 days younger

$sudo find /opt/backup -name text -type f -mtime +30 -delete   -->find and delete files that are more than 30 days old

$sudo find /var/log -name "\*.log" -type f -mtime +30 -delete  -->find and delete files that ends with log and are less than 2 days old

$sudo find /var/log -type d -mtime +90   -->find and delete directories that are more than 90 days old

$sudo find /home -name etechfile.yaml   -->Find all the files whose name is tecmint.txt and contains both capital and small letters in /home directory.

$sudo find / -type d -name etechfile.yam  -->Find all directories whose name is etechfile.yaml in / directory.

Special linux commands:

$ date --> to check the date

$ cal --> to check the calendar

$uptime --> is used to check how long a system has been running

$ DO NOT RUN $ reboot

What are Linux Logs? :

Linux logs provide a timeline of events for the Linux operating system, applications and system and are a valuable troubleshooting tool when you encounter issues.

When issues arise, analyzing log files is the first thing an administrator needs to do.

Linux log files are stored in plain-text and can be found in the /var/log directory and subdirectory. There are Linux logs for everything:

system, kernel, package managers, boot processes, Xorg, Apache, MySQL, etc.

Log Files in Linux:

system log files:

        /var/log/kern.log --> stores Kernel logs and warning data. This log is valuable for troubleshooting custom kernels as well

         /var/log/auth.log. -->This is where you will find information about user authorization attempts; including the use of the sudo command.

sudo less /var/log/auth.log --> to inspect the content of the auth.log file.

grep memory /var/log/kern.log

sudo less /var/log/auth.log | grep user

sudo less /var/log/kern.log

sudo head /var/log/kern.log

Basic Linux Disk Management Commands :

Disk management:

/dev/sda1

Your operating system,applications, and data all need to be kept on some kind of permenent

storage so that when you turn off your computer and then ON again, your data is intack.

When you install the operating system, the disk is divided into one or more partions.

Disks: use for permenent storage

RAM(RandomAccessMemory): use for temporary storage

Swap: use for temporary storage

for example when you run a command, that command is copied from the hard disk into RAM so that

your computer processor(CPU) can access it quickly.

Linux disk management commands:

  $ df -h ---> use to check disk free space

  $ du -h ----> use to check for disk usage

  $ free -m --> use to check memory free space in megabytes

  $ free -g --->  use to check memory free space in gigabytes

  $ lscpu ---> use to check the cpu statistics

  $ ls -i ---> use to show the position of a file within the linux filesystem

Disks commands:

  $ parted -l /dev/sda   --->use to view partions

  $ fdisk -l /dev/sda     --->use to format a drive

  $ lsblk       ----->to see the different partitions block

  $  mount      ------>use to munt a drive

  $ unmount     ----->use to unmount a drive

  /mnt          ----->is the default mount directory in linux

  $ mkdir /mnt/test

  $ mount /dev/sdb1 /mnt/test

  $ df -h /mnt/sdb1   ----> h stands for human readable format

  fstab( File System Table)  ---->use to permenently mount a drive to the file system

  /dev/sdb1   /mnt/test  xfs  defaults  0 1    ---->is sample fstab entry

  xfs: is the filesystem

  defaults: means that the partition should be mounted at boot time

  number 0: tells the system not to backup files automatically from this filesystem

  number 1: tells the system to check the partition for errors after a certain number of mounts

  swap: Used for swap partitions.swap areas are used to hold data temporarily when RAM is used up.

        Data swapped to the swap area and then returned to RAM when it is needed again

  nfs: Network filesystem

  xfs: A high-performance filesystem originally developed by silicon graphics that works extremely well

       with large file.

 Network management:

 Linux Networking Commands

 Linux networking commands are used extensively to inspect, analyze, maintain, and troubleshoot the network/s connected to the system.

 Let us first know the list of the basic networking commands used in Linux followed by a detailed explanation of each.

1. ifconfig

2. ip

3. traceroute

5. ping

6. netstat

8. dig

9. nslookup

10. route

12. arp

13. iwconfig

14. hostname

15. curl or wget

16. mtr

17. whois

18. ifplugstatus

19. iftop

20. tcpdum

$ifconfig

Linux ifconfig stands for interface configurator. It is one of the most basic commands used in network inspection.

ifconfig is used to initialize an interface, configure it with an IP address, and enable or disable it.

It is also used to display the route and the network interface.

Basic information displayed upon using ifconfig are:

IP address

MAC address

MTU(Maximum Transmission Unit)

$ip

This is the latest and updated version of ifconfig command.

Syntax:

$ip a

$ip addr

This command gives the details of all networks like ifconfig.

This command can also be used to get the details of a specific interface.

Commands to get details are:

Syntax:

$ip a show eth0

$ip a show lo

$ip a show wlan0

traceroute:

Linux traceroute is one of the most useful commands in networking. It is used to troubleshoot the network. It detects the delay and determines the pathway to your target. It basically helps in the following ways:

It provides the names and identifies every device on the path.

It follows the route to the destination

It determines where the network latency comes from and reports it.

traceroute <destination>

example:

traceroute google.com

The output provides the following information:

The specified hostname

Size of the packets

The maximum number of hops required.

The IP address.

4.tracepath :

Linux tracepath is similar to traceroute command. It is used to detect network delays. However, it doesn't require root privileges.

It traces the route to the specified destination and identifies each hop in it. If your network is weak, it recognizes the point where the network is weak.

Example:

tracepath google.com

tracepath etechconsultingllc.com

tracepath facebook.com

5.ping

Linux ping is one of the most used network troubleshooting commands. It basically checks for the network connectivity between two nodes.

ping stands for Packet INternet Groper.

The ping command sends the ICMP echo request to check the network connectivity.

It keeps executing until it is interrupted.

Use Ctrl+C Key to interrupt the execution.

Syntax:

ping <destination>

ping googlr.com

ping -c <number> <destination>

Functions:

The command is used to measure the average response. If there is no response for the ping command, you can assume one of the following issues with the network:

There is a physical issue causing network loss.

The destination address might be dysfunctional or incorrect.

The ping request is blocked due to a target.

There might be a problem with the routing table.

6.netstat

Linux netstat command refers to the network statistics.

It provides statistical figures about different interfaces which include open sockets, routing tables, and connection information.

Syntax:

netstat

Output:

Observe the output displaying all the open sockets.

Variations in netstat command

Below are few variations of the netstat command used.

a) To display the programs

Syntax:

netstat -p

This displays the programs associated with the open socket.

b) To get the details of the ports

Syntax:

netstat -s

This gives detailed statistics of all the ports.

c) To get the information of the routing table

Syntax:

netstat -r

This gives information related to the routing table.

7. dig

Linux dig command stands for Domain Information Groper. This command is used in DNS lookup to query the DNS name server. It is also used to troubleshoot DNS related issues.

8.hostname :

Linux hostname is the simple command used to view and set the hostname of a system.

9.curl & wget:

Linux curl and wget commands are used in downloading files from the internet through CLI

$curl -O <fileLink>

$ wget <fileLink>

Process Management Commands:

Tasks run as processes

ps command is short for ‘Process Status’. It displays the currently-running processes. However, unlike the top command,

the output generated is not in realtime.

$ps

The terminology is as follows :

 PID = process ID

 TTY = terminal type

 TIME = total time the process has been running

 CMD = name of the command that launches the process

 To get more information using ps command use:

 $ ps -u

 %CPU represents the amount of computing power the process is taking.

 %MEM represents the amount of memory the process is taking up.

 STAT represents process state.

 While ps command only displays the processes that are currently running, you can also use it to list all the processes.

 $ ps -A

  ps -ef

  ps -ef | grep java

  ps -ef | grep http

  ps -ef | grep ssh

How to Find and Kill a Zombie Process:

kill : Kill the process

$ ps aux | egrep "Z|defunct"

$ ps -o ppid= <Child PID>

$ kill -s SIGCHLD <Parent PID>

$ kill -9 <Parent PID>

top :

Top command displays a list of processes that are running in real-time along with their memory and CPU usage.

$top

PID: Unique Process ID given to each process.

User: Username of the process owner.

PR: Priority given to a process while scheduling.

NI: ‘nice’ value of a process.

VIRT: Amount of virtual memory used by a process.

RES: Amount of physical memory used by a process.

SHR: Amount of memory shared with other processes.

S: state of the process

‘D’ = uninterruptible sleep

‘R’ = running

‘S’ = sleeping

‘T’ = traced or stopped

‘Z’ = zombie

%CPU: Percentage of CPU used by the process.

%MEM; Percentage of RAM used by the process.

TIME+: Total CPU time consumed by the process.

Command: Command used to activate the process.

==========================================================================================================

1. touch --> create a file

2. mkdir --> to create a directory

3. rmdir --> remove an empty directory

4. rm -rf --> to forcely removed a directory

5. ls --> to disply the content of a directory(lists)

6. cat --> to see the content of a file

7. cp --> to copy files locally

8. pwd --> to print working directory

9. cd --> to change directory

10. history --> to previous run commands