Lab 11 – System/Log monitoring commands and System Information/Maintenance Commands

top

- The top command has been around a long time and is very useful for viewing details of running processes and quickly identifying issues such as memory hogs. Its default view is shown below.

cbkpc@ubuntulinux~$ top

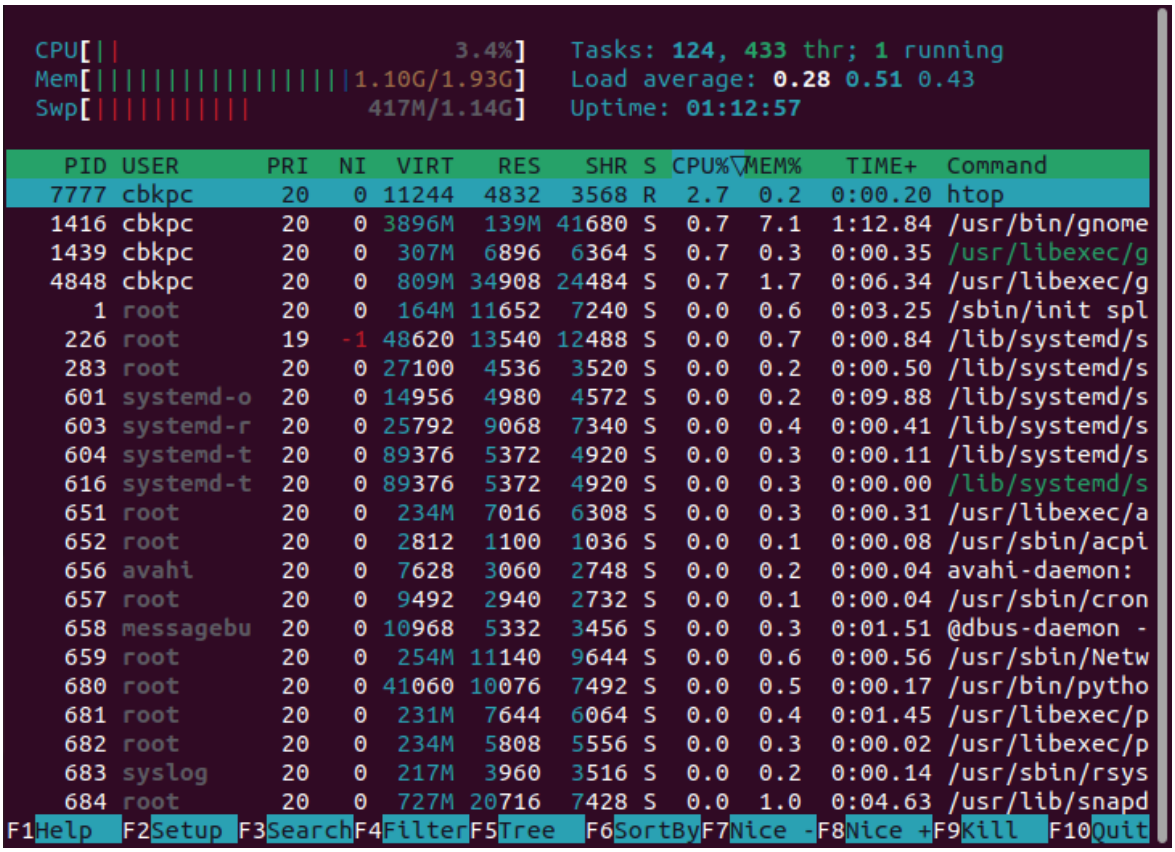
```
top - 11:56:28 up 1 day, 13:37,  1 user,  load average: 0.09, 0.04, 0.03
Tasks: 292 total,   3 running, 225 sleeping,  0 stopped,   0 zombie
%Cpu(s):  0.1 us,  0.2 sy,  0.0 ni, 99.7 id, 0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 16387132 total, 10854648 free, 1859036 used,  3673448 buff/cache
KiB Swap:        0 total,        0 free,        0 used. 14176540 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
17270 alan      20   0 3930764 247288  98992 R   0.7  1.5   5:58.22 gnome-shell
20496 alan      20   0  816144  45416  29844 S   0.5  0.3   0:22.16 gnome-terminal-
21110 alan      20   0   41940   3988   3188 R   0.1  0.0   0:00.17 top
    1 root      20   0  225564   9416   6768 S   0.0  0.1   0:10.72 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.01 kthreadd
    4 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/0:0H
    6 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 mm_percpu_wq
    7 root      20   0       0      0      0 S   0.0  0.0   0:00.08 ksoftirqd/0
```

cbkpc@ubuntulinux~$ top-p20881 -p20882 -p20895

```
Tasks:   4 total,   0 running,  4 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.8 us,  1.3 sy,  0.0 ni, 95.9 id, 0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 16387132 total, 10856008 free, 1857648 used,  3673476 buff/cache
KiB Swap:        0 total,        0 free,        0 used. 14177928 avail Mem
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
20881 alan      20   0   12016    348      0 S   0.0  0.0   0:00.00 nginx
20882 alan      20   0   12460   1644    932 S   0.0  0.0   0:00.00 nginx
20895 alan      20   0   12016    352      0 S   0.0  0.0   0:00.00 nginx
```

htop

cbkpc@ubuntu:~$ htop



df

- The **df** command (short for disk free), is used to display information related to file systems about total space and available space.
- **Syntax :** df [OPTION]... [FILE]...
- If no file name is given, it displays the space available on all currently mounted file systems.

Example 1: **cbkpc@ubuntulinux~$ df**

Portion of output:

```
Filesystem     1K-blocks     Used Available Use% Mounted on
udev           3996816       0  3996816 0% /dev
tmpfs           804624    10020    794604  2% /run
/dev/sda9      68117056 18036160  46597712  28% /
```

Example 2: specify particular file, then it will show mount information of that particular file.

For example: cbkpc@ubuntulinux~$ df /home/cbkpc/test/test.cpp

Output:

```
Filesystem     1K-blocks     Used Available Use% Mounted on
/dev/sda10     78873504 67528220  7315640  91% /home
```

iostat

- The **iostat** command in Linux is used for monitoring system input/output statistics for devices and partitions.
- **Note**: iostat is being included in sysstat package. If user doesn't have it, user need to install first. (apt-get install sysstat)
- **Syntax: iostat**
- **Options used:**
  - **-x:** This command shows more details statistics information.
  - **-c:** This command show only the CPU statistic.
  - **-d:** This command displays only the device report
- Example: **cbkpc@ubuntulinux~$ iostat –x**

```
Linux 5.19.0-43-generic (ubuntu)  05/06/23        _x86_64_        (1 CPU)
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           5.87    0.43    1.94   13.39    0.00   78.37
Device            tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
loop0            0.00         0.00         0.00         0.00         17          0          0
loop1            0.01         0.08         0.00         0.00        349          0          0
loop10           0.01         0.08         0.00         0.00        350          0          0
loop11           0.08         1.47         0.00         0.00       6764          0          0
```

free

- **free** command is used to view memory consumption
- **cbkpc@ubuntulinux~$ free -m**

```
                total        used        free      shared  buffers     cached
Mem:          7976        6459        1517           0         865        2248
-/+ buffers/cache:        3344        4631

Swap:         1951           0        1951
```

- The m option displays all data in MBs.

cat /proc/cpuinfo

- The file **/proc/cpuinfo** displays what type of processor the user system is running including the number of CPUs present.
- **cbkpc@ubuntulinux~$ cat /proc/cpuinfo**

```
processor       0
vendor_id       : GenuineIntel
cpu family      6
model           45
model name      : Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
stepping        6
```

microcode 1561
cpu MHz : 600.000
cache size : 20480 KB

cat /proc/meminfo

- On Linux, user can use the command cat /proc/meminfo to **determine how much memory the computer has**.

- **cbkpc@ubuntulinux~$ cat /proc/meminfo**

MemTotal: 8167848 kB
MemFree: 1409696 kB
Buffers: 961452 kB
Cached: 2347236 kB
SwapCached: 0 kB
SwapTotal: 1998844 kB
SwapFree: 1998844 kB
...

Work on log directory:

/var/log

- It is essential that user know where the log files are located, and what is contained in them. Such files are usually in **/var/log**. Logging is controlled by the associated .**conf** file.

cbkpc@ubuntu:~$ ls /var/log

alternatives.log cups kern.log.1
alternatives.log.1 dist-upgrade kern.log.2.gz
apport.log dmesg lastlog
apport.log.1 dmesg.0 openvpn
apport.log.2.gz dmesg.1.gz private
apt dmesg.2.gz speech-dispatcher
auth.log dmesg.3.gz syslog
auth.log.1 dmesg.4.gz syslog.1
auth.log.2.gz dpkg.log syslog.2.gz

Few log files:

- **/var/log/messages** – Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.
- **/var/log/auth.log** – Contains system authorization information, including user logins and authentication machinsm that were used.
- **/var/log/boot.log** – Contains information that are logged when the system boots
- **/var/log/lastlog** – Displays the recent login information for all the users. This is not an

ascii file. User should use lastlog command to view the content of this file.

- **/var/log/user.log** – Contains information about all user level logs
- **/var/log/btmp** – This file contains information about failed login attemps. Use the last command to view the btmp file. For example, "last -f /var/log/btmp | more"
- **/var/log/yum.log** – Contains information that are logged when a package is installed using yum
- **/var/log/cron** – Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file

Example: sudo cat /var/log/auth.lo

cbkpc@ubuntu:~$ sudo tail -5 /var/log/auth.log

Jun 5 12:42:01 ubuntu CRON[8049]: pam_unix(cron:session): session closed for user cbkpc

Jun 5 12:43:01 ubuntu CRON[8066]: pam_unix(cron:session): session opened for user cbkpc(uid=1000) by (uid=0)

Jun 5 12:43:01 ubuntu CRON[8066]: pam_unix(cron:session): session closed for user cbkpc

Jun 5 12:43:40 ubuntu sudo: cbkpc : TTY=pts/0 ; PWD=/home/cbkpc ; USER=root ; COMMAND=/usr/bin/tail -10 /var/log/auth.log

Jun 5 12:43:40 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)

cbkpc@ubuntu:~$ sudo tail -5 /var/log/boot.log

[OK] Started Authorization Manager.

Starting Modem Manager...

[OK] Started Power Profiles daemon.

System maintenance commands:

Shutdown

- "**Shutdown**" refers to the process of stopping and shutting down a computer or server.
- **Standard command for shutting down Linux**
  - **shutdown –h**
    - Linux will shut down in under a minute. The "-h" option explicitly stands for the shutting down or powering off of a system.
  - **shutdown**
    - User can usually produce the same results by just entering the shutdown command on its own.
- **Standard command for restarting Linux**
  - **shutdown -r**
    - Linux will be restarted in under a minute.
    - The "-r" option stands for reboot or restart.
- **Command for shutting down Linux immediately**
  - **shutdown -h 0 // time Specification 0**
  - **shutdown now**
    - Another common command for shutting down Linux immediately:
- **Command for restarting Linux immediately**
  - **shutdown -r 0 // time Specification 0**
  - **shutdown -r now**
- **Command for Shutting Down/Restart Linux after 20 minutes**
  - shutdown -h 20
  - shutdown +20
  - shutdown -r 20
  - shutdown –r +20
  - shutdown -h 17:30 // Shutting down at 5.30pm
  - shutdown -r 17:30 // Restarting at 5.30pm

Rebooting

- Booting is **starting a computer's operating system**, so rebooting is to start it for a second or third time.
- **sudo reboot**
- **sudo systemctl reboot**
- **sudo shutdown -r**

halt

- This command in Linux is **used to instruct the hardware to stop all the CPU functions**.
- Basically, it reboots or stops the system.
- **halt [OPTION]**
- **Options used:**
  - -f, –force It does not invoke shutdown
  - -w, –wtmp-only It will not call shutdown or the reboot system call but writes the shutdown record to /var/log/wtmp file.
  - -p, –poweroff To behave as poweroff

init

- **init** is parent of all Linux processes with PID or process ID of 1.
- It is the first process to start when a computer boots up and runs until the system shuts down.
- init stands for initialization.The role of init is to create processes from script stored in the file /etc/inittab which is aconfiguration file which is to be used by initialization system.
- Run Levels is the state of init where a group of processes are defined to start at the startupof OS.Each runlevel has a certain number of services stopped or started. Conventionally sevenrunlevel exist numbers from zero to six.

Run Level	Mode	Action
0	Halt	Shuts down system
1	Single-User Mode	Does not configure network interfaces, start daemons, or allow non-root logins
2	Multi-User Mode	Does not configure network interfaces or start daemons.
3	Multi-User Mode with Networking	Starts the system normally.
4	Undefined	Not used/User-definable
5	X11	As runlevel 3 + display manager(X)
6	Reboot	Reboots the system

System update & repositories

Update the Repositories

- **sudo apt-get update**
- This command refreshes local list of software, making a note of any newer revisions andupdates.

Run the upgrade

- **sudo apt-get dist-upgrade**
- The "dist-upgrade" switch asks Ubuntu to handle any **dependencies** intelligently.

Packaging Manager

- Packaging manager is the software used for managing, installing, updating, upgrading

  etc. of the packages of a system.
- Linux based systems or Linux systems have a lot of such packaging managers in whichtwo are: **yum** and **rpm**.

yum

- Yum and RPM are both package managers for Linux systems.
- Yum stands for Yellowdog Updater Modified. They are packaging managers for RPM-based Linux systems.
- Yum can only install the packages available in its repository.
- Yum can also scan and upgrade the packages to the latest versions. It also entirely relieson online repositories.

rpm

- RPM stands for Redhat Packaging Manager.
- It can be considered one of the oldest packaging managers that do basic functions likeuninstalling, updating, archiving the packages received by the Linux systems.
- It can install multiple packages with the condition that we give the correct file name withthe .rpm extension.