## Part 2 Monitoring Own System:

First I will install htop to run basic commands to get information on basics system performances etc.

- I run sudo apt install htop
- Then i just run <u>htop</u>

```
root@LinuxServer: /
 0[||||
                                  11.5%]
12.7%]
                                           Load average: 0.07 0.11 0.03
                                           Uptime: 16:20:14
          PID USER
                               RES
                                           CPU%-MEM%
                                                      1h10:14 /usr/bin/gnome-shell
6304 vboxuser
                       4799N
                                    178M S
                                           6.0 15.1 30:28.83 /snap/firefox/3836/usr/lib/
9949 vboxuser
                20
                     0 12.8G
6315 vboxuser
                                           3.3 8.9 15:59.20 /usr/bin/gnome-shell
                20
                     0 4799M
19982 vboxuser
                20
                     0 2474M
                              126M 91308 S
                                           3.3
                                                3.2
                                                    1:09.98
                                                             /snap/firefox/3836/usr/lib/
68856 root
                20
                     0 20968
                              5376
                                    3456
                                            3.3
                                                 0.1
                                                     0:01.36 htop
                                           2.7
6313 vboxuser
                     0 4799M
                                    153M S
                                                8.9 16:15.19 /usr/bin/gnome-shell
                20
                                  153M S 2.7
6314 vboxuser
                     0 4799M
                                                8.9 15:50.13 /usr/bin/gnome-shell
                20
6894 vboxuser
                20
                    0 554M 52744 38368 S 2.0 1.3 3:23.50 /usr/libexec/gnome-terminal
19820 vboxuser
                20
                     0 2761M
                                   100M S
                                           2.0
                                                5.9 11:04.30 /snap/firefox/3836/usr/lib/
                     0 2165M 20844 18028 S
1466 vboxuser
                                           1.3 0.5
                                                     8:07.06 /usr/bin/pulseaudio --daemo
19829 vboxuser
                                    100M S
                                                     3:16.95 /snap/firefox/3836/usr/lib/
               20
                     0 2761M 231M
                                           1.3
                                               5.9
 421 systemd-o 20
                     0 14832
                             5888
                                    5760 S
                                           0.7
                                                0.1
                                                     2:33.36 /lib/systemd/systemd-oomd
1400 vboxuser
                9
                       2165M 20844 18028 S 0.7 0.5
                                                     8:28.87 /usr/bin/pulseaudio --daemo
                     0 4799M
                                    153M S
                                           0.7
6320 vboxuser
                20
                                                8.9
                                                     0:40.16 /usr/bin/gnome-shell
                                    178M S
10030 vboxuser
                20
                     0
                                           0.7 15.1
                                                     1:46.15
    F2Setup F3SearchF4FilterF5Tree F6SortByF7Nice -F8Nice +F9Kill F10Ouit
```

Now that I know it is running I can just type c to show current processes:

```
root@LinuxServer: /
 0[|||||
1[||||||
2[||||||
                                  18.3%
                                           Load average: 0.20 0.16 0.06
                                  16.7%]
Swp
                             701M/2.62G]
                               RES
                                     SHR S CPU%-MEM%
                                                       TIME+ Command
 PID USER
               PRI NI VIRT
                                    153M S 25.9 8.9
 6304 vboxuser
                     0 4799M
                                                      1h10:18 /usr/bin/qnome-shell
9949 vboxuser
                20
                     0 12.8G
                                    178M S
                                            8.6 15.1 30:30.23 /snap/firefox/3836/usr/lib/
                     0 4799M
                                    153M S 7.3 8.9 16:15.93 /usr/bin/gnome-shell
6313 vboxuser
                20
6315 vboxuser
                20
                     0 4799M
                                    153M S
                                            6.7
                                                 8.9 15:59.94
                                                8.9 15:50.84
                     0 4799M
                                    153M S
6314 vboxuser
                20
                                            6.0
19982 vboxuser
                     0 2474M
                              126M 91308 S
                                           4.0
                                                3.2 1:10.43 /snap/firefox/3836/usr/lib/
                20
68856 root
                     0 20968
                                    3456 R
                                           2.0 15.1 4:30.26
10092 vboxuser
                     0 12.8G
                                    178M S
                20
                                    100M S
19820 vboxuser
                20
                     0 2761M
                                            2.0
                                                5.9 11:07.00 /snap/firefox/3836/usr/lib/
                                                     8:29.77 /usr/bin/pulseaudio --daemo
1400 vboxuser
                9
                    11 2165M 20844 18028 S
                                            1.3
                                                0.5
                     0 12.8G
10138 vboxuser
                20
                                    178M S
                                            1.3 15.1
                                                      0:45.09 /snap/firefox/3836/usr/lib/
                                    178M S 1.3 15.1
                                                      0:50.03 /snap/firefox/3836/usr/lib/
10139 vboxuser
                20
                     0 12.8G
19829 vboxuser
                                    100M S 1.3 5.9
                                                      3:18.00 /snap/firefox/3836/usr/lib
                20
                     0 2761M
                20
                     0 14832
                                    5760 S
                                                0.1
                                                      2:33.64 /lib/systemd/systemd-oomd
 421 systemd-o
                              5888
                                            0.7
                       2165M 20844 18028 S
 1466 vboxuser
                -6
                     0
                                            0.7
                                                 0.5
                                                     8:07.91 /usr/bin/pulseaudio --daem
     F2Setup F3SearchF4FilterF5Tree
```

Here we can see several things about our host metric:

- First we can see the percentage used from each of our three cores (0 is 12%, 1 is 18.3%, 2 is 16.7%).
- We have 2.11 G of memory being used
- We see pour uptime being 16:21:55
- Here our load average is 0.20 for a minute, 0.16 for five, 0.06 for fifteen.
- Our swap space being used is 701 M.
- Here I can see several things, I can view the Uptime on my machine, the load averages (the first is a minute, the second is 5 minutes, the third is 15 min) and the % of CPU time a process is using (0% means it is not using the CPU at all, 100% means using a full CPU, 200% using two full CPUs and so on until 400% as our maximum CPUs are 4).

Next we will monitor user activity using ACCT:

- First we need to install it running sudo apt install acct install.
- Then we enable it running sudo systematl enable acct.
- And start it <u>sudo systemctl start acct.</u>
- Then we can run <u>sudo systemctl status acct</u> to check that acct is active, we should have something like this:

```
Created symlink /etc/systemd/system/multi-user.target.wants/acct.service -> /lib/systemd/sys
tem/acct.service.
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
root@LinuxServer:/# sudo systemctl enable psacct
Failed to enable unit: Unit file psacct.service does not exist.
root@LinuxServer:/# sudo systemctl enable acct
Synchronizing state of acct.service with SysV service script with /lib/systemd/systemd-sysv-
install.
Executing: /lib/systemd/systemd-sysv-install enable acct
root@LinuxServer:/# sudo systemctl start acct
root@LinuxServer:/# sudo systemctl status acct
  acct.service - Kernel process accounting
     Loaded: loaded (/lib/systemd/system/acct.service; enabled; vendor preset: enabled)
     Active: active (exited) since Tue 2024-04-09 10:44:59 CEST; 3min 40s ago
       Docs: man:accton(8)
   Main PID: 69957 (code=exited, status=0/SUCCESS)
        CPU: 2ms
apr 09 10:44:59 LinuxServer systemd[1]: Starting Kernel process accounting...
apr 09 10:44:59 LinuxServer accton[69957]: Turning on process accounting, file set to '/var>apr 09 10:44:59 LinuxServer systemd[1]: Finished Kernel process accounting.
```

Here we see that our process is active!

Then we can use the lastcomm command to view the logs and get a general view of the logs showing user activity mine will mostly show root:

sh		root	pts/4	0.00 secs	Tue Apr	9 10:44
gzip		root	pts/4	0.00 secs		9 10:44
install-info		root	pts/4	0.00 secs		9 10:44
sh		root	pts/4	0.00 secs		9 10:44
gzip		root	pts/4	0.00 secs		9 10:44
install-info		root		0.00 secs		9 10:44
			pts/4	0.00 secs		
sh 		root	pts/4			9 10:44
gzip		root	pts/4	0.00 secs		9 10:44
install-info		root	pts/4	0.00 secs		9 10:44
sh		root	pts/4	0.00 secs		9 10:44
gzip		root	pts/4	0.00 secs		9 10:44
install-info		root	pts/4	0.00 secs	Tue Apr	9 10:44
sh		root	pts/4	0.00 secs	Tue Apr	9 10:44
gzip		root	pts/4	0.00 secs	Tue Apr	9 10:44
find		root	pts/4	0.00 secs	Tue Apr	9 10:44
ГM		root	pts/4	0.00 secs		9 10:44
ср		root	pts/4	0.00 secs		9 10:44
LW -L		root	pts/4	0.00 secs		9 10:44
acct.postinst		root	pts/4	0.00 secs		9 10:44
deb-systemd-in	v	root	pts/4	0.02 secs		9 10:44
systemctl						
		root.	DTC / /	0 00 5055	Tue Are	0 10 • 11
Systemett	S	root	pts/4	0.00 secs	Tue Apr	9 10:44
systemd-udevd	SF	root	•	0.00 secs secs Tue Apr	Tue Apr 9 10:47	9 10:44
			0.00			9 10:44
systemd-udevd	SF	root	0.00	o secs Tue Apr	9 10:47	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo	SF SF SF S	root root	0.00 0.00 0.00 pts/2 0.00	9 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo	SF SF SF S	root root root root	0.00 0.00 0.00 pts/2 0.00 pts/3 0.00	9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl	SF SF SF S	root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00	9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask	SF SF SF S F S	root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 pts/3 0.00	9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd	SF SF SF S F S	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 pts/3 0.00	9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd	SF SF SF S F S	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 pts/3 0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker	SF SF SF S F S SF	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 pts/3 0.00 0.00 1.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker systemd-udevd	SF SF SF S S SF SF	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.00 1.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker systemd-udevd systemd-udevd	SF SF SF S F S SF	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.00 1.00 0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker systemd-udevd systemd-udevd systemd-udevd systemd-udevd	SF SF SF S S SF SF	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.00 0.00 0.00 0.00 0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker systemd-udevd systemd-udevd systemd-udevd lsb_release lsb_release	SF SF SF S S SF SF	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker systemd-udevd systemd-udevd systemd-udevd systemd-udevd	SF SF SF S S SF SF	root root root root root root root root	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd systemd-udevd dconf worker systemd-udevd systemd-udevd systemd-udevd lsb_release lsb_release	SF SF SF S S SF SF	root root root root root root root X vboxuser root vboxuser vboxuser vboxuser	0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd dconf worker systemd-udevd dconf worker systemd-udevd systemd-udevd lsb_release lsb_release lsb_release	SF SF S S SF SF SF SF	root root root root root root root xoot root xoot x	0.00 0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd dconf worker systemd-udevd systemctl	SF SF S S SF SF SF SF	root root root root root root root root	0.00 0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 2 secs Tue Apr 2 secs Tue Apr 3 secs Tue Apr 4 secs Tue Apr 5 secs Tue Apr 6 secs Tue Apr 7 secs Tue Apr 7 secs Tue Apr 8 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd dconf worker systemd-udevd systemd-udevd lsb_release lsb_release lsb_release sudo sudo systemctl dpkg	SF SF S S SF SF SF SF	root root root root root root root root	0.00 0.00 0.00 pts/2 0.00 pts/3 0.00 pts/3 0.00 0.	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 2 secs Tue Apr 2 secs Tue Apr 3 secs Tue Apr 4 secs Tue Apr 5 secs Tue Apr 6 secs Tue Apr 7 secs Tue Apr 8 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd dconf worker systemd-udevd systemd-udevd lsb_release lsb_release lsb_release sudo sudo systemctl dpkg dpkg	SF SF S S SF SF SF SF SF	root root root root root root root root	0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 2 secs Tue Apr 2 secs Tue Apr 3 secs Tue Apr 4 secs Tue Apr 5 secs Tue Apr 6 secs Tue Apr 7 secs Tue Apr 8 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd dconf worker systemd-udevd lsb_release lsb_release lsb_release sudo sudo systemctl dpkg dpkg (sd-executor)	SF SF S S SF SF SF SF	root root root root root root root root	0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 2 secs Tue Apr 2 secs Tue Apr 3 secs Tue Apr 4 secs Tue Apr 5 secs Tue Apr 6 secs Tue Apr 7 secs Tue Apr 8 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46	9 10:44
systemd-udevd systemd-udevd systemd-udevd sudo sudo systemctl systemd-tty-ask systemd-udevd dconf worker systemd-udevd systemd-udevd lsb_release lsb_release lsb_release sudo sudo systemctl dpkg dpkg	SF SF S S SF SF SF SF SF	root root root root root root root root	0.00 0.00	9 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 9 secs Tue Apr 1 secs Tue Apr 1 secs Tue Apr 2 secs Tue Apr 2 secs Tue Apr 3 secs Tue Apr 4 secs Tue Apr 5 secs Tue Apr 6 secs Tue Apr 7 secs Tue Apr 8 secs Tue Apr 9 secs Tue Apr	9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:47 9 10:46 9 10:46	9 10:44

Here we can see two users' activity vboxuser and root, alongside what processes they are running etc.

- We can also use the w command to see the users logged in, the uptime and other info.

```
oot@LinuxServer:/# w
11:05:00 up 16:55, 3 users, load average: 0,02, 0,13, 0,15
                  FROM
                                                     JCPU
SER
        TTY
                                    LOGIN@
                                             IDLE
                                                            PCPU WHAT
                                             4days 0.02s
                                                    0.02s 0.02s /usr/libexec/gnome-session-
0.43s 0.43s ssh localhost
oxuser tty2
                                     wo11
                  tty2
ot
                                     do18
                                              1.00s
        pts/2
                  127.0.0.1
                                     do18
                                              1.00s
                                                     2.27s 0.01s w
oot@LinuxServer:/#
```

- JCPU shows us the joint CPU runtime whichis the total amount of CPU time used by all processes attached to the user's session.
- PCPU: Displays the percentage of CPU time used by the user's processes since the last update of w.
- What: Shows the current command or activity being performed by the user. This typically includes the name of the command or program the user is running.
- User: Lists the username of each logged-in user.
- TTY: Indicates the terminal (or pseudo-terminal) associated with each user session.
- From: Displays the remote hostname or IP address from which a user is logged in, if applicable. If a user is logged in locally, it usually shows -.
- Login Time: Shows the time when each user logged in.
- Idle Time: Indicates how long each user has been idle. If a user has been active recently, it shows 0:00.
- In this example we can see we have 3 users and that our average load time for a minute is 0.02, for five it is 0.13 and finally for fifteen is 0.15

Now let's have a look at prometheus, I will mention later how it can be used to analyze different metrics mentioned in part one:

- First, we want to install prometheus to take a look at my application metrics
- To do so we go on the prometheus website and select the correct file to add to our system.

2.51.1 / 2024-03-27 Release notes								
File name	os	Arch	Size	SHA256 Checksum				
prometheus-2.51.1.darwin-amd64.tar.gz	darwin	amd64	97.42 MiB	f8046dd097538ba7lc33fa6cfd83d8fb4bf5f58c90le58ec0c66288ec95db4bd				
prometheus-2.51.1.linux-amd64.tar.gz	linux	amd64	96.98 MiB	1f933ea7515e3a6e60374ee0bfdb62bc4701c7b12c1dbafe1865c327c6e0e7d2				
prometheus-2.51.1.windows-amd64.zip	windows	amd64	99.13 MiB	15cc0d176ccc5149ffaa895440e325db7a4ceb3c4804913c635b1215dff31e8e				
2.45.4 / 2024-03-18 LTS Release notes								
File name	os	Arch	Size	SHA256 Checksum				

- Then we go into the directory where the file was downloaded and unzip it running tar xvfz /prometheus/prometheus-2.30.3.linux-amd64/

- The go into the folder <u>cd prometheus-2.30.3.linux-amd64/</u>
- Change the config file by running <u>sudo nano prometheus.yml</u> according to what we need, here I will put the demo recommended config given by official documentation:

## global: scrape\_interval: 5s

scrape\_configs:

- job\_name: "prometheus" static\_configs:

- targets:

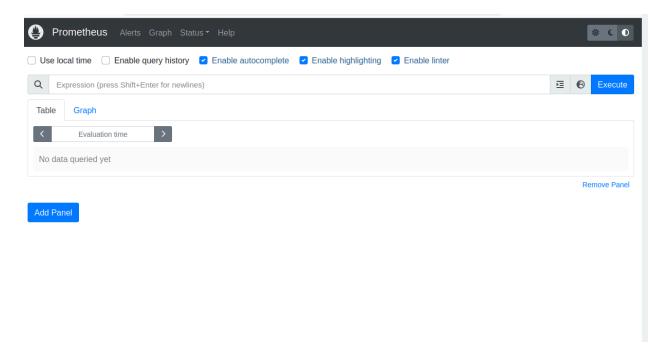
- localhost:9090

- job\_name: "demo" static\_configs:

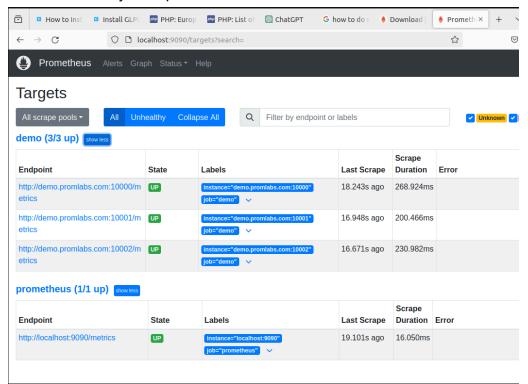
- targets:

demo.promlabs.com:10000demo.promlabs.com:10001demo.promlabs.com:10002

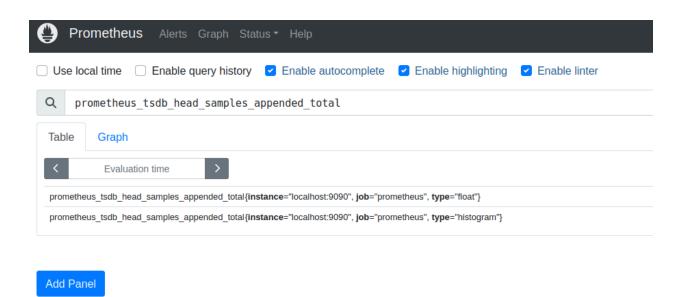
- And now run ./prometheus to start the server
- Now go to you browser of choice and go to localost:9090



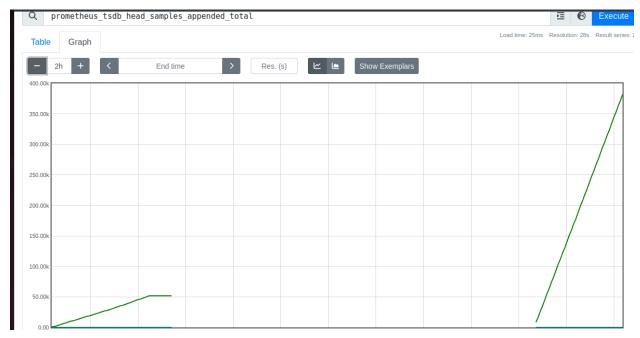
- Here we can see the prometheus UI. We can check under status then targets to see if they are up:



- All of them are up. Now we can focus on trying to look at a metric and the data Prometheus scraped on it:



- Here I entered the prometheus\_tsdb\_head\_amples\_appended\_total (total number of samples that have been appended to the head of the time series database)
- In Prometheus, the "head" of the TSDB refers to the most recent data that has been ingested and stored in memory or the most actively queried portion of the time series data. This typically includes the most recent data points.
- Each time a new data point (sample) is ingested into Prometheus and stored at the most recent part of the TSDB (the head), this metric value increases.
- Monitoring this metric can provide insights into the rate at which new data is being collected and added to Prometheus. It's useful for understanding the data ingestion rate and the activity level of the monitoring system.



- Here we can see how the data has changed over the last 2 hours going into the graph section. Showing how we ccan keep track of different application metrics and monitor them using prometheus.
- This can be used from server metrics to External dependencies metrics to Application metrics. We can even set it up to scrape particular metrics of interest etc.

## Let's look at our network performance:

- First we need to intsall the iftop tool: sudo apt-get install iftop.
- Then we run it using sudo iftop

```
root@LinuxServer:/home/vboxuser/Downloads/prometheus-2.51.1.linux-amd64# sudo iftop interface: enp0s3
IP address is: 10.0.2.15
MAC address is: 08:00:27:ab:66:c8
root@LinuxServer:/home/vboxuser/Downloads/prometheus-2.51.1.linux-amd64#
```

So here we can see basic info about our network.

```
12,5Kb
                                         25,0Kb
                                                                                    50,0Kb
                                                               37,5Kb
                                                                                                  62,5Kb
TX:
                                    peak:
                                                                     rates:
                                                                                                     0b
RX:
                              0B
                                                 0b
                                                                                  0Ь
                                                                                                     0b
                                                                                            0b
TOTAL:
                              0B
                                                 οь
                                                                                  0Ь
                                                                                           0Ь
```

 And here the tool is listening enp0s3 here we do not have much going on but if that changes we will see it on here and be able to keep track of efficiency etc for our network.

## Now lets take a look at events:

Here we do not need a specific tool we can just look at our logs by running <u>cat</u> /<u>var/log/syslog</u>.

```
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 32 with keysym 32 (keycode b).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 31 with keysym 31 (keycode a).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 33 with keysym 33 (keycode c).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 34 with keysym 34 (keycode d).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 36 with keysym 36 (keycode f).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 37 with keysym 37 (keycode 10).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 38 with keysym 38 (keycode 11).
Apr 9 14:17:48 LinuxServer gnome-shell[6304]: Window manager warning: Overwriting existing
binding of keysym 39 with keysym 39 (keycode 12).
Apr 9 14:17:48 LinuxServer dbus-daemon[5956]: [session uid=1000 pid=5956] Activating servic
e name='org.gnome.ArchiveManager1' requested by ':1.263' (uid=1000 pid=72480 comm="gjs /usr/
share/gnome-shell/extensions/ding@rasters" label="unconfined")
Apr 9 14:17:49 LinuxServer dbus-daemon[5956]: [session uid=1000 pid=5956] Successfully acti
vated service 'org.gnome.ArchiveManager1'
Apr 9 14:17:49 LinuxServer gnome-shell[6304]: DING: Detected async api for thumbnails
     9 14:17:49 LinuxServer gnome-shell[6304]: DING: GNOME nautilus 42.6
```

 Here we can see my logs warning me of a recent even where existing binding is being overwritten - We can also see that a service was activated successfully

And we pretty much covered everything covered everything in part one and tried it in this part! Hope this helps!