

## **Part 1 Monitoring:**

- CPU load, RAM memory usage, Disk usage, top processes
- Using the top command, htop tends to be the preferred tool of choice.
- Log files are files that keep track of events happening on a computer system such as errors, operations running and problems. On a computer they tend to be located in `/var/log/syslog`. If you want to check the logs you can do so by using `cat`, `cat /var/log/syslog`.
- To check on user activity, we need to use tools such as accounting utilities. First, we will need to install it by running `sudo apt install acct`. Then we need to first enable it then, start it. We are able to do so by running: `sudo systemctl enable acct` (to enable it) then `sudo systemctl start acct` to start it. To check on the status ACCT we can do so by running: `sudo systemctl status acct`. Here are some commands you can use with ACCT:
  - `ac`: displays stats on how long the user has been logged on.
  - `lastcomm`: shows information on previously executed commands.
  - `accton`: turns process accounting on or off.
  - `dump-acct`: transforms accton file from its default format to a readable format for humans.
  - `dump-utmp`: dumps utmp files into human readable format.
  - `sa`: summarizes info about previously executed commands.
  - Or if we just want a summary in general we can use `lastcomm` to access the logs.
- Here are a few metrics to keep track of:
  - Host metrics:
    - ☐ Associated with general health and performance of an individual computer without the services it serves.
    - ☐ CPU metrics
    - ☐ Disk metrics
    - ☐ Memory metrics
    - ☐ Can access these running htop
  - Application Metric:
    - ☐ Shows if an application runs correctly and efficiently
    - ☐ Average Response time
    - ☐ Error Rates
    - ☐ Request Rate
    - ☐ Service failures and restarts
    - ☐ Can generally be checked with logs
    - ☐ We can use prometheus (download it from the official website)
      - We first need to unzip the file running `tar xvfz /prometheus/prometheus-2.30.3.linux-amd64/`
      - Then you need to configure the config file by running `sudo nano ~/prometheus/prometheus-2.30.3.linux-amd64/` if you want to focus on a specific application

- You can also use the prometheus UI on <http://localhost:9090> to view metrics etc.
- Network performance metric:
  - ☐ Shows how structures and infrastructures are performing as part of short term and long term assessments of the network.
  - ☐ Packet loss
  - ☐ Connectivity
  - ☐ Throughput
  - ☐ Can use iftop to check on it.
- Server pool metric:
  - ☐ Server pool metrics measure the ability of a collection of servers to work and respond appropriately to requests.
  - ☐ Number of running instances
  - ☐ Total number of instances
  - ☐ Scaling Adjustment Metric
  - ☐ Can use prometheus again
- External Dependencies metric:
  - ☐ Services status and availability
  - ☐ Error rate
  - ☐ Service response speed
  - ☐ Our friend prometheus can help again
- Events:
  - ☐ Do not have a defined periodicity
  - ☐ Tend to contain detailed info about what is going on.
  - ☐ Often triggers for alerts.
  - ☐ Can be monitored using syslogs
- You can run the w command to check runtime.
- iftop, shows a list of network connections and their corresponding data rates.
  - First install it: sudo apt install iftop
  - Then run it: sudo iftop