PRACTICAL ACTIVITY 3

VIRTUOUS FANNY

[virtuous.fanny@womentechsters.org](mailto:virtuous.fanny@womentechsters.org)

**Part 1: of Practical Activity Week 3**

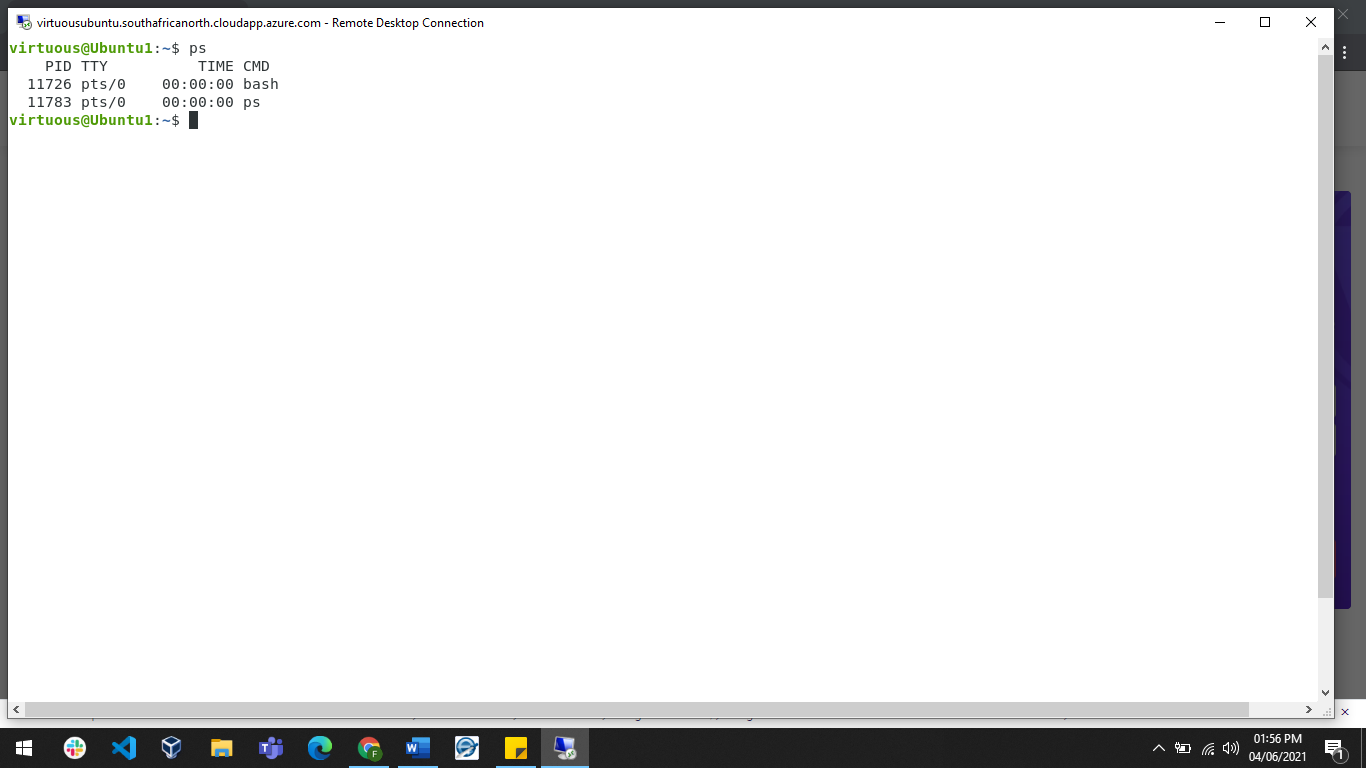
This week you will entirely learn how to manage and access different processes and statistics in a Linux environment.

Perform the following activities and screenshot your output from Ubuntu- Terminal.

Do through research for the different commands you will utilize.

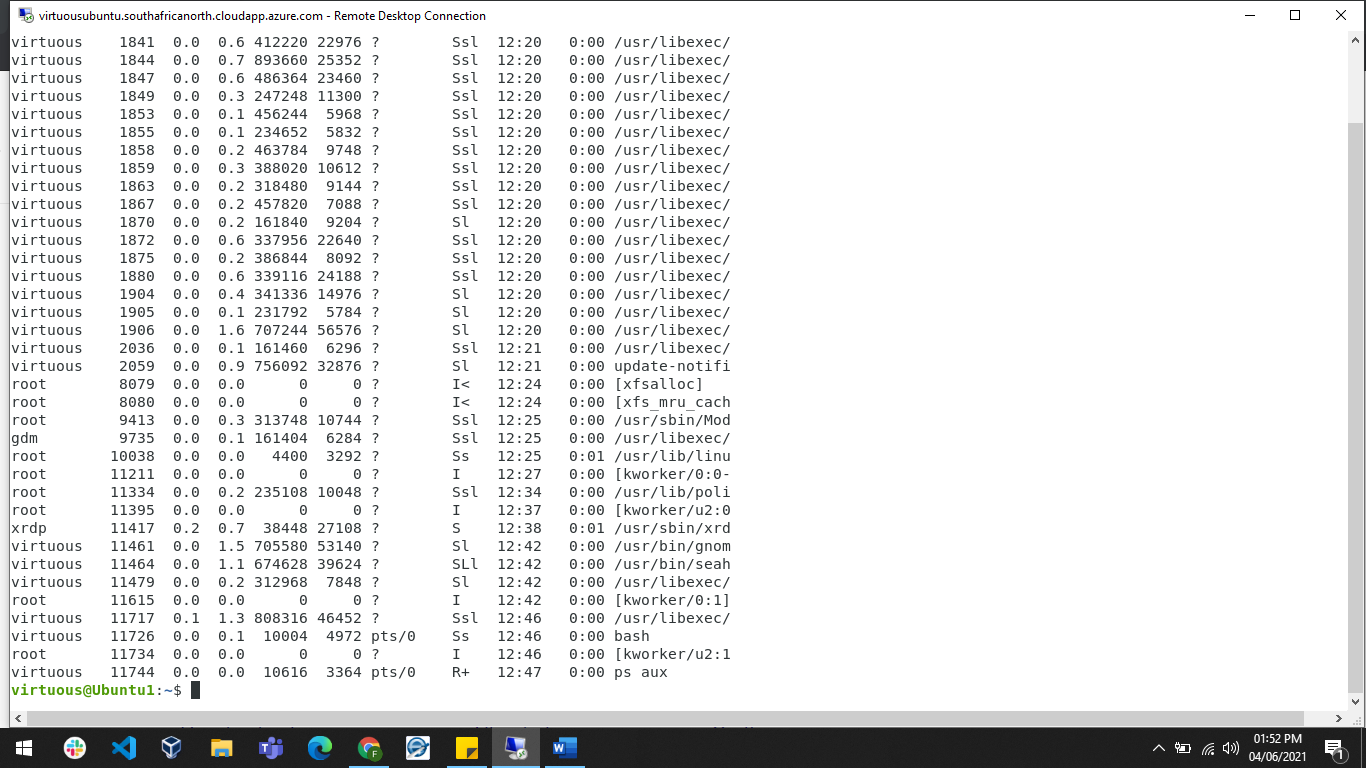
1. List the processes for the current shell.

The command for this is “ps”



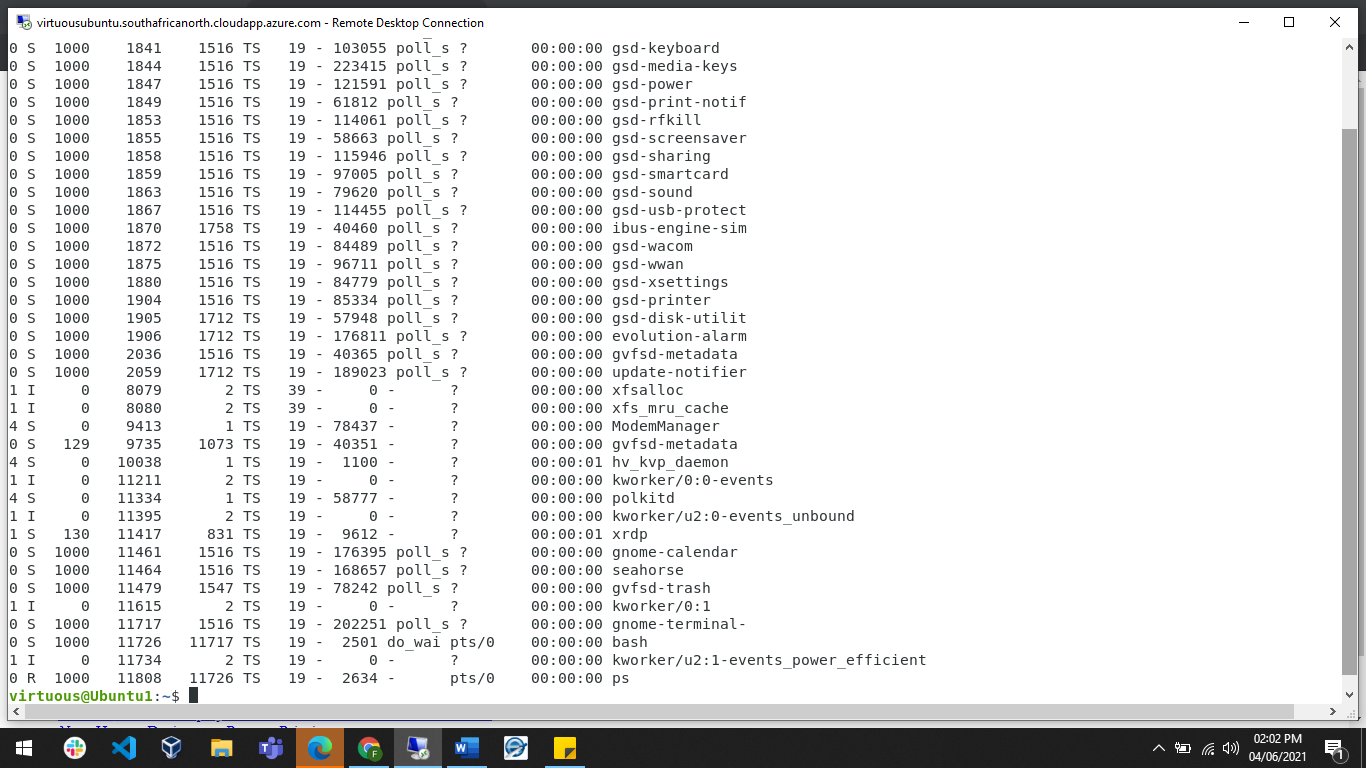
1. Display information about processes.

The command for this is “ps aux”



1. Display the global priority of a process and find out the column that provides.

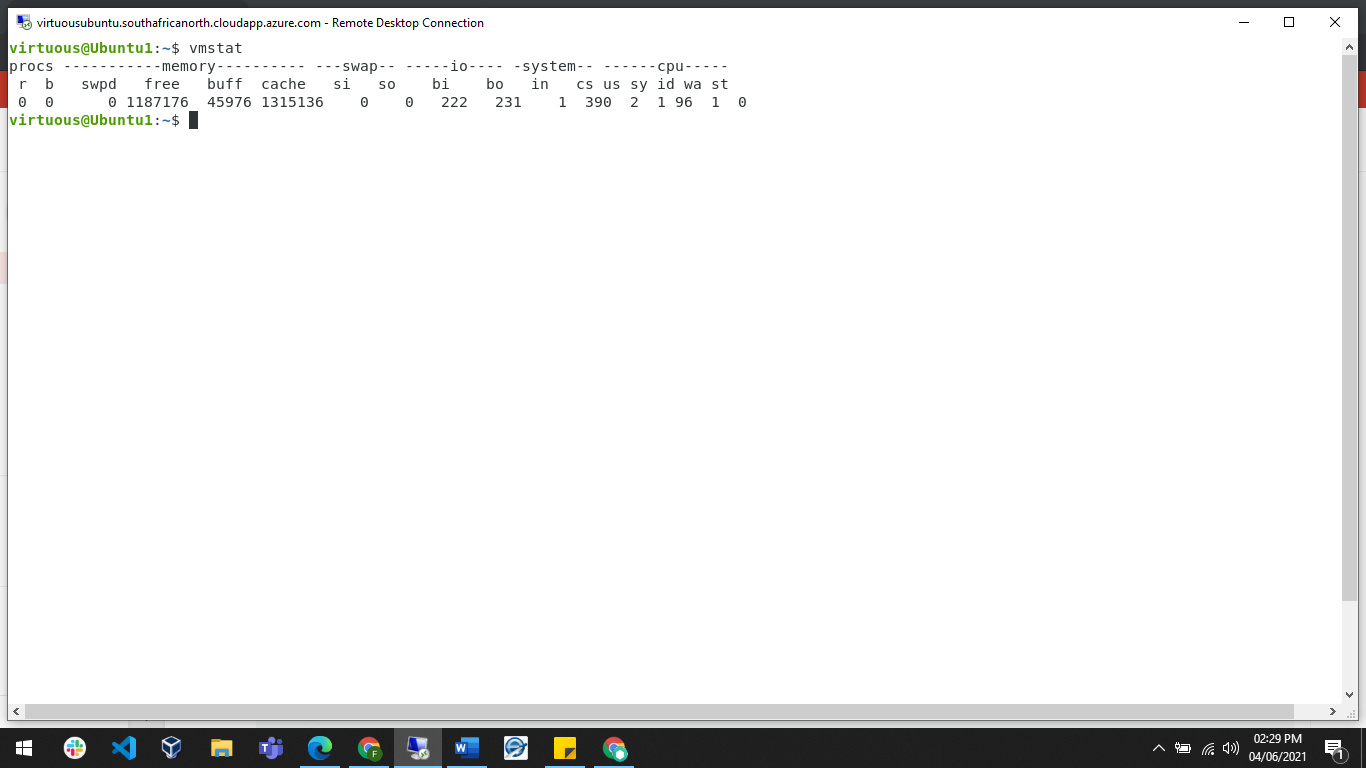
The command for this is “ps -ecl”



The global priority is listed under the PRI column.

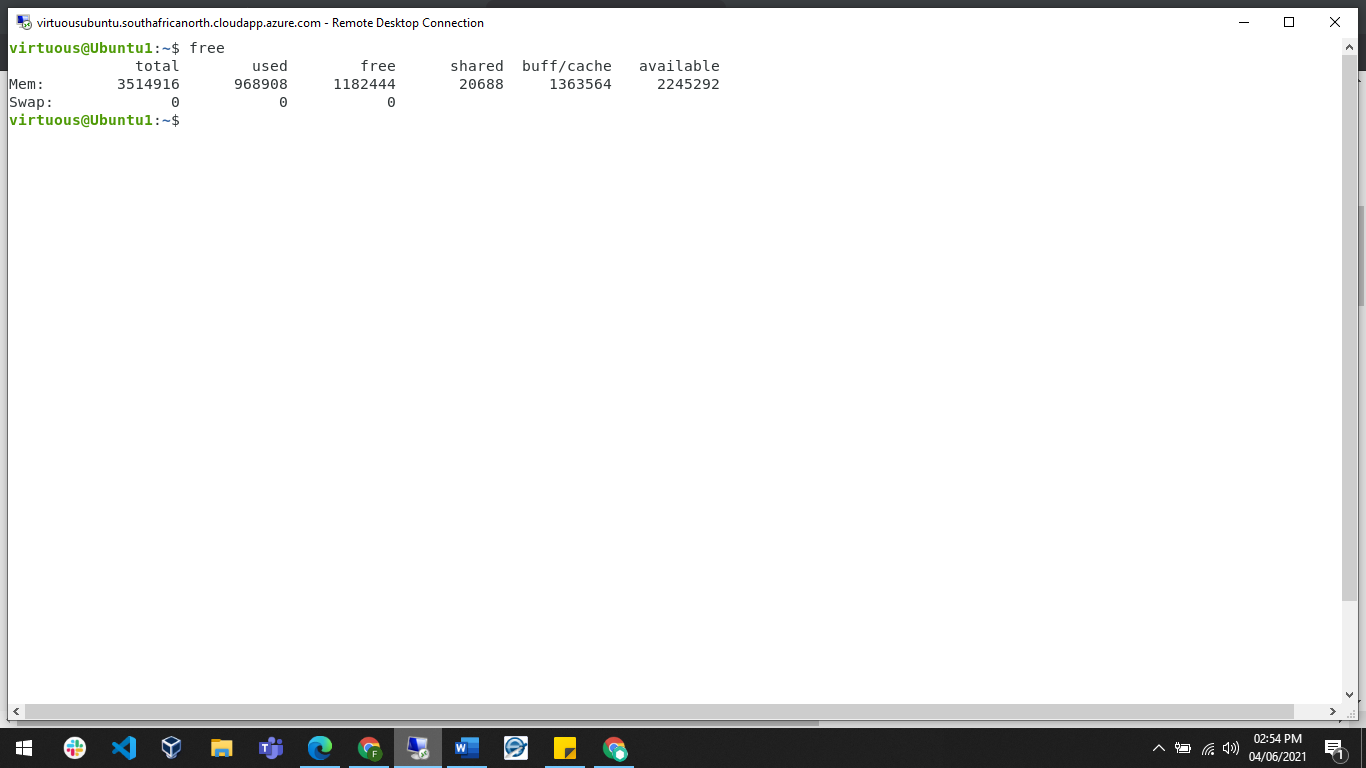
1. Change the priority of a process with default arguments.
2. Display Virtual Memory Statistics.

The command for this is “vmstat”



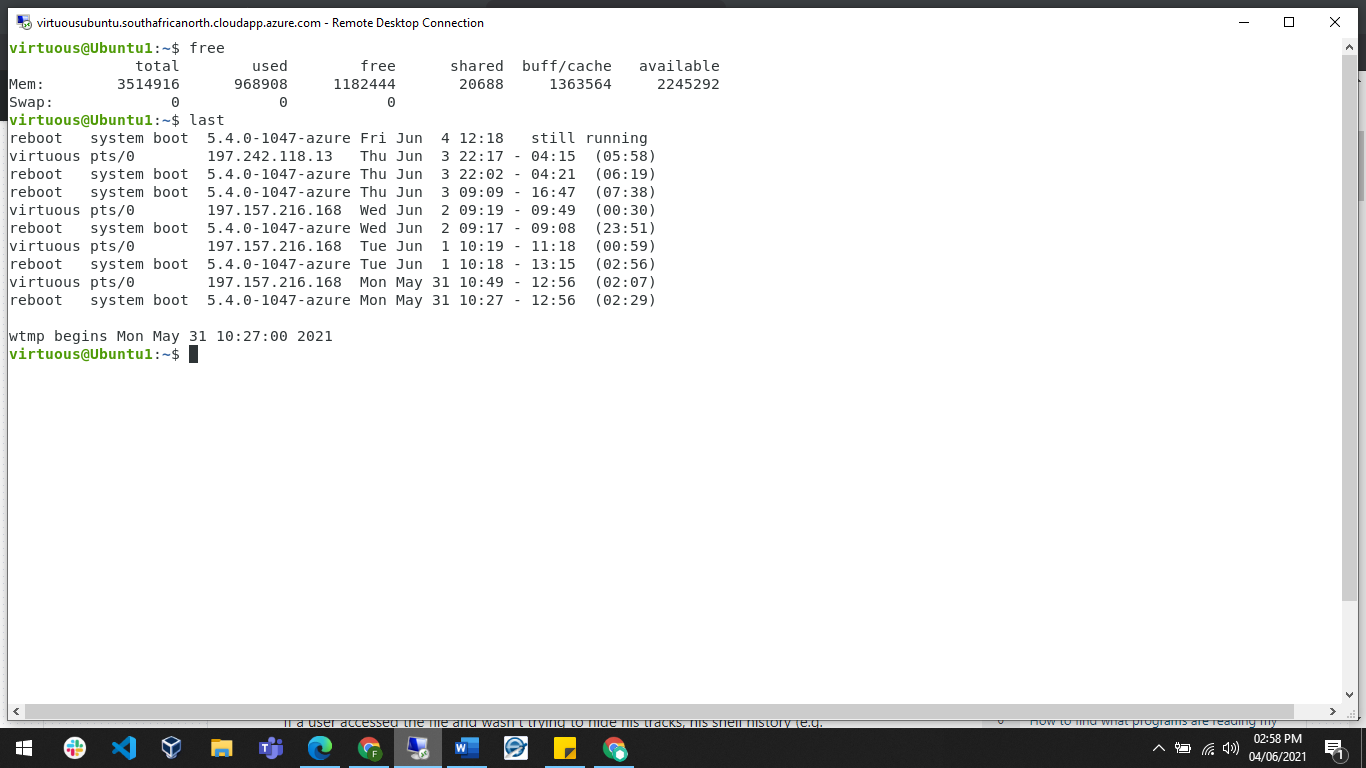
1. Display System Event Information.
2. Display Swapping Statistics.

The command for this is “free” or “swapon -s”



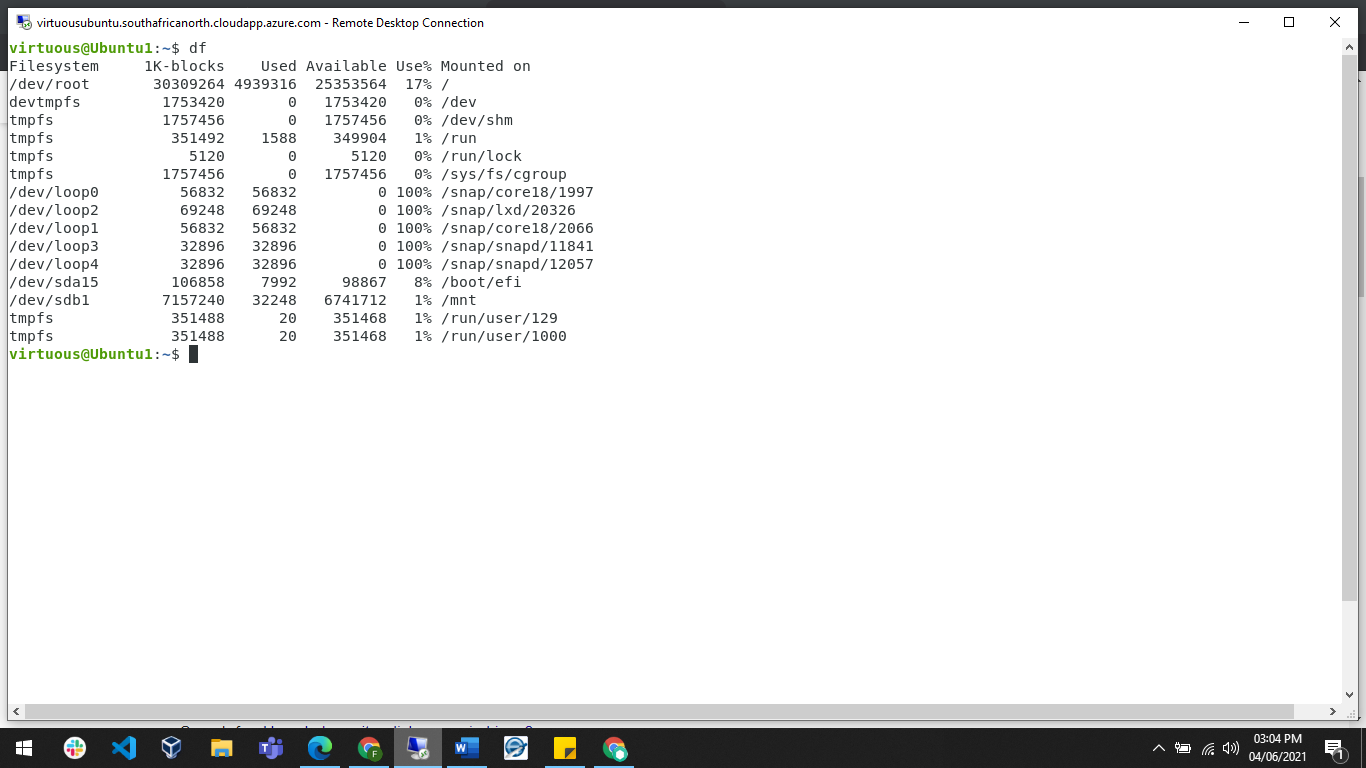
1. Check File Access statistics.

The command for this is “last”



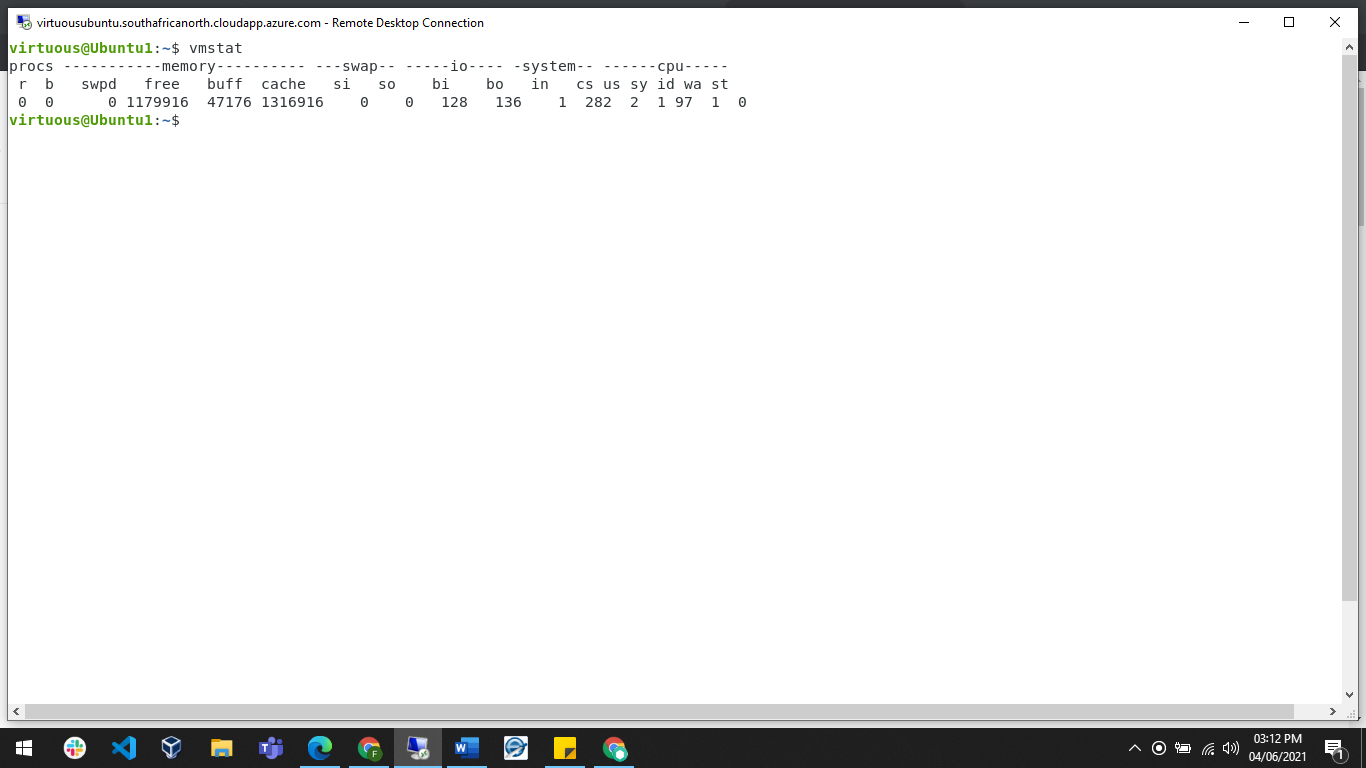
1. Check Buffer Activity statistics.
2. Check Disk Activity statistics.

The command for this is “df”



1. Check Inter process Communication statistics.
2. Check Unused Memory in the server.

The command for this is “vmstat”



1. Check Swap Activities.

The command for this is “swapon -s”

**Part 2 : Practical Activity Week 3**

This exercise is based on management of users accounts and creating of files. As linux security Administrator you should be able to assign different file permission and revoke permissions to unauthorized users. To improve your skills practice with this exercise.

**Entirely use the Terminal utilization of GUI will not be awarded any marks.**

Login to your terminal in Ubuntu.

1. Create a user account called user1 and another user2
2. Ensure user1 and user2 are password protected.
3. Logout and login as user1
4. Create a testdir
5. Create a file testfile in testdir
6. Verify the ownership and the group of the testfile
7. Switch to Superuser account
8. Create a public directory dir1
9. Set stickybit (save text attribute) on dir1
10. Logout and login as a normal user user1
11. Create a file userfile1 in dir1
12. Login as a different user user2
13. Try to edit or remove the file
14. Temporarily disable user logins

