PRACTICAL ACTIVITY 3: ON LINUX SYSTEM ADMINSTRATION

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. - ps
2. Display information about processes. – ps -A or ps aux
3. Display the global priority of a process and find out the column that provides. Top under pr. (or: ps -o pri -p processno. Or -e to list all)
4. Change the priority of a process with default arguments. -sudo renice -new prio -pid
5. Display Virtual Memory Statistics. – cat /proc/meminfo vmstat -s
6. Display System Event Information. -direvent -V or usage dmesg canadd less to it
7. Display Swapping Statistics. Swapon -s or proc/swaps
8. Check File Access statistics. Stat -f /
9. Check Buffer Activity statistics. Sar -b
10. Check Disk Activity statistics. Dstat -d
11. Check Inter process Communication statistics. Ipcs -b
12. Check Unused Memory in the server. Free -m
13. Check Swap Activities. Grep Swap /proc/meminfo

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.

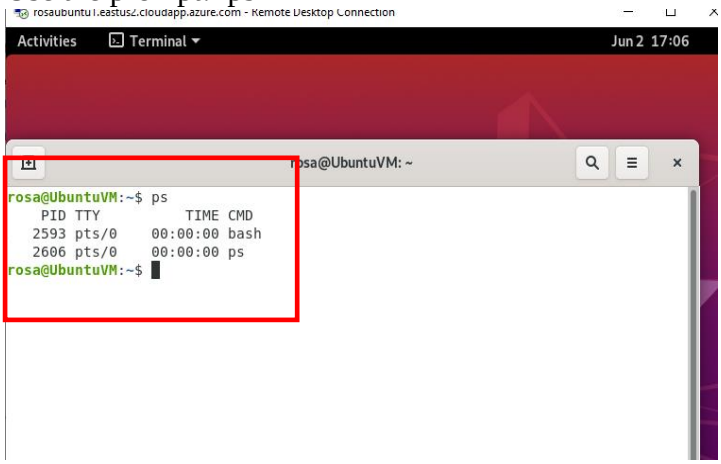
1. Create a user account called user1 and another user2
2. Ensure user1 and user2 are password protected.
3. Logout and login as user1
4. Create a testdir
5. Create a file testfile in testdir
6. Verify the ownership and the group of the testfile
7. Switch to Superuser account
8. Create a public directory 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 : sudo passwd -l user to undo psswd -u

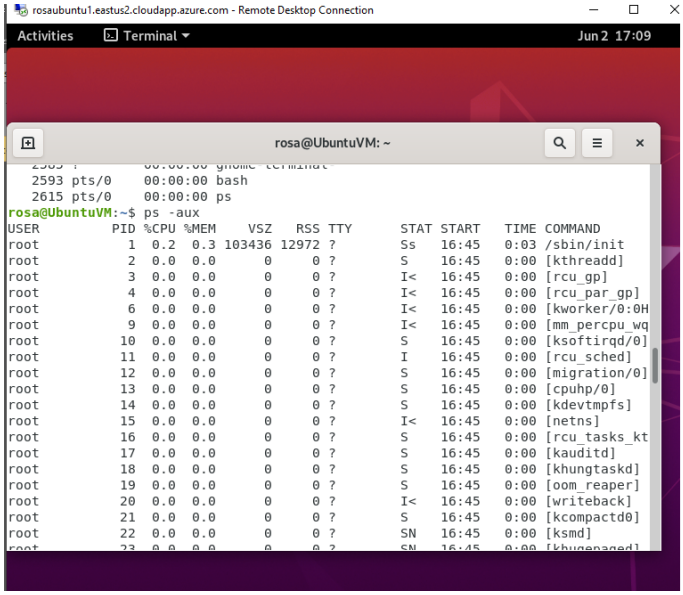
PART 1 – COMMANDS

1. List the processes for the current shell.

Use the prompt: ps



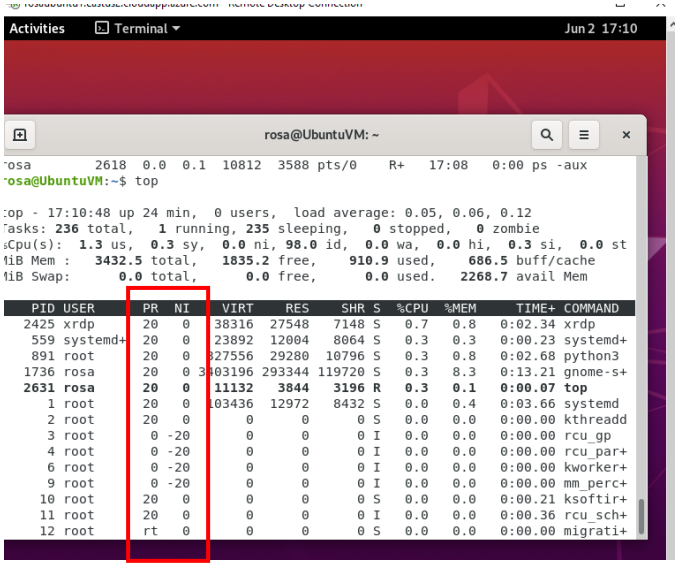
2. Display information about processes: ps -A or ps aux



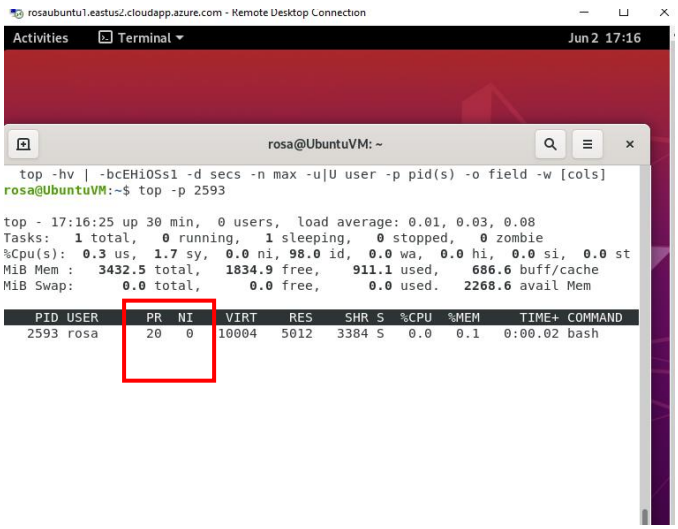
3. # Display the global priority of a process and find out the column that provides.

The column PR has the kernel priority (which is 20 + NI). The column NI has the actual priority.

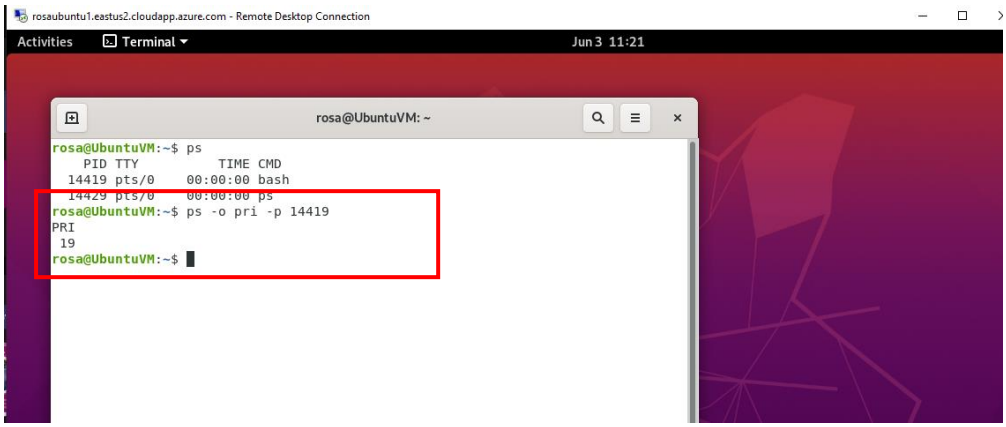
Top – for all processes



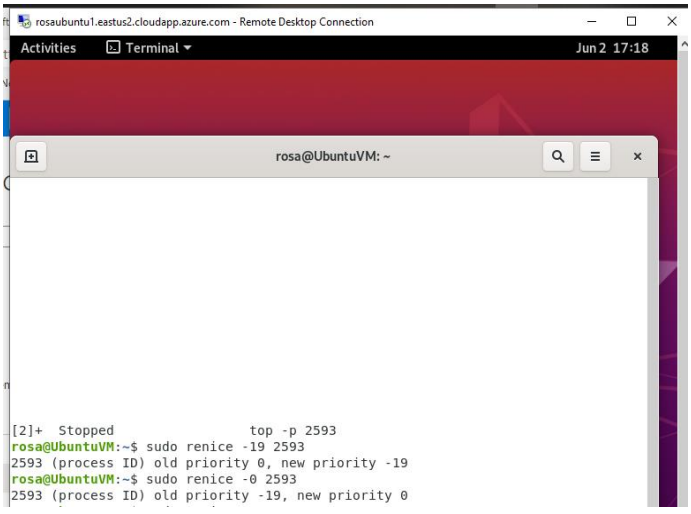
Top -p 2593 (for a particular process).



Can also use ps -o pri -p 2593 (This will give the direct priority number)

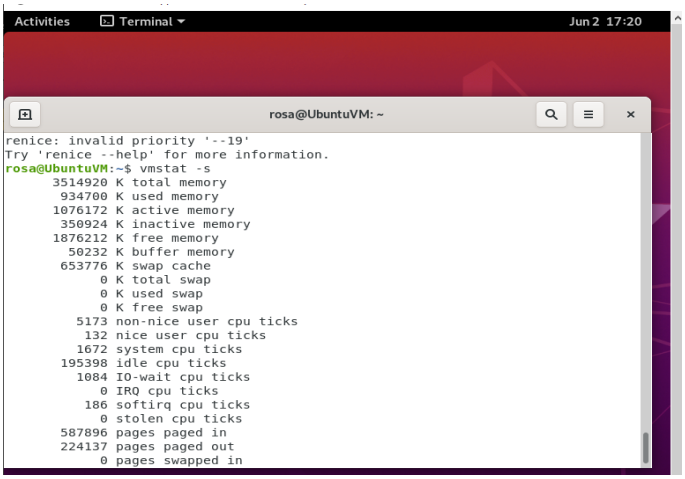


4. Change the priority of a process with default arguments. -sudo renice -new prio -pid

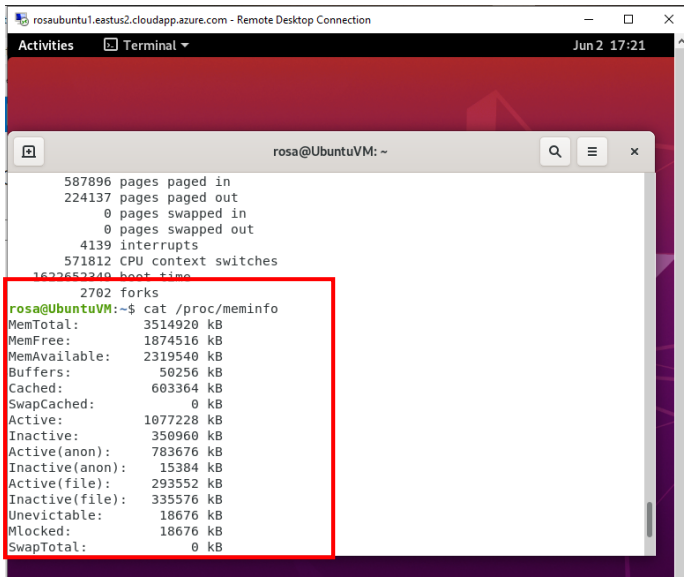


5. # Display Virtual Memory Statistics.

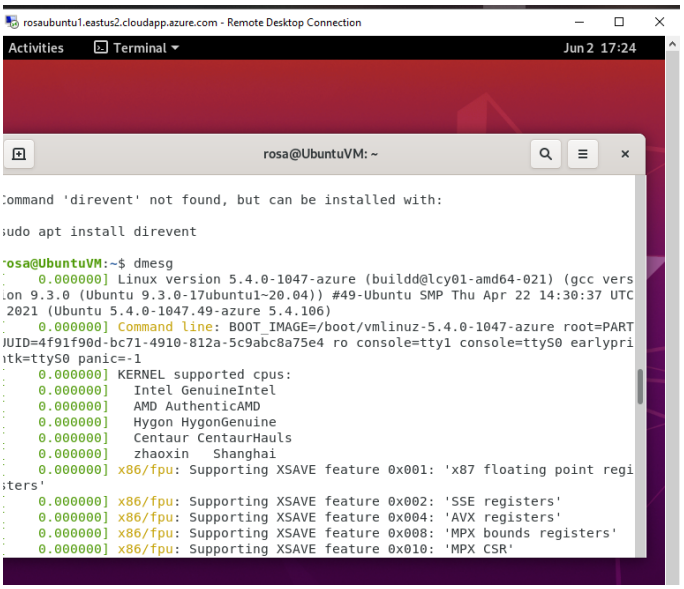
vmstat -s



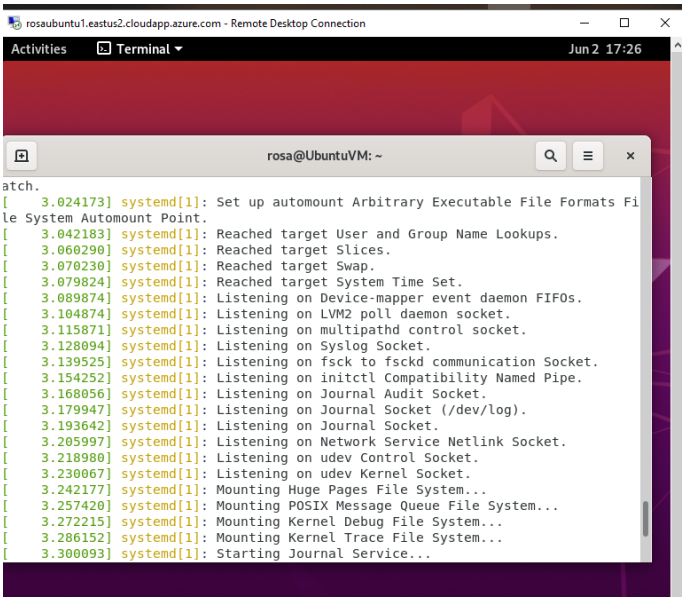
Or: cat /proc/meminfo



6. # Display System Event Information. dmesg command

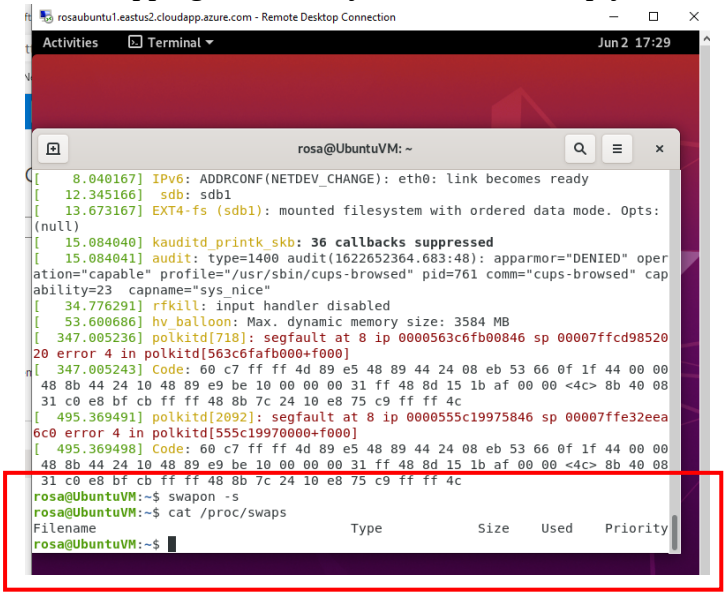


Output continued,

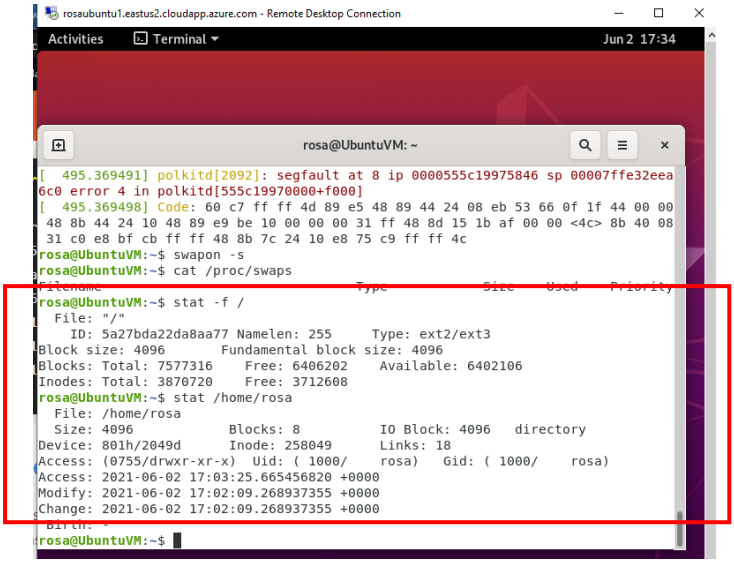


7. # Display Swapping Statistics.

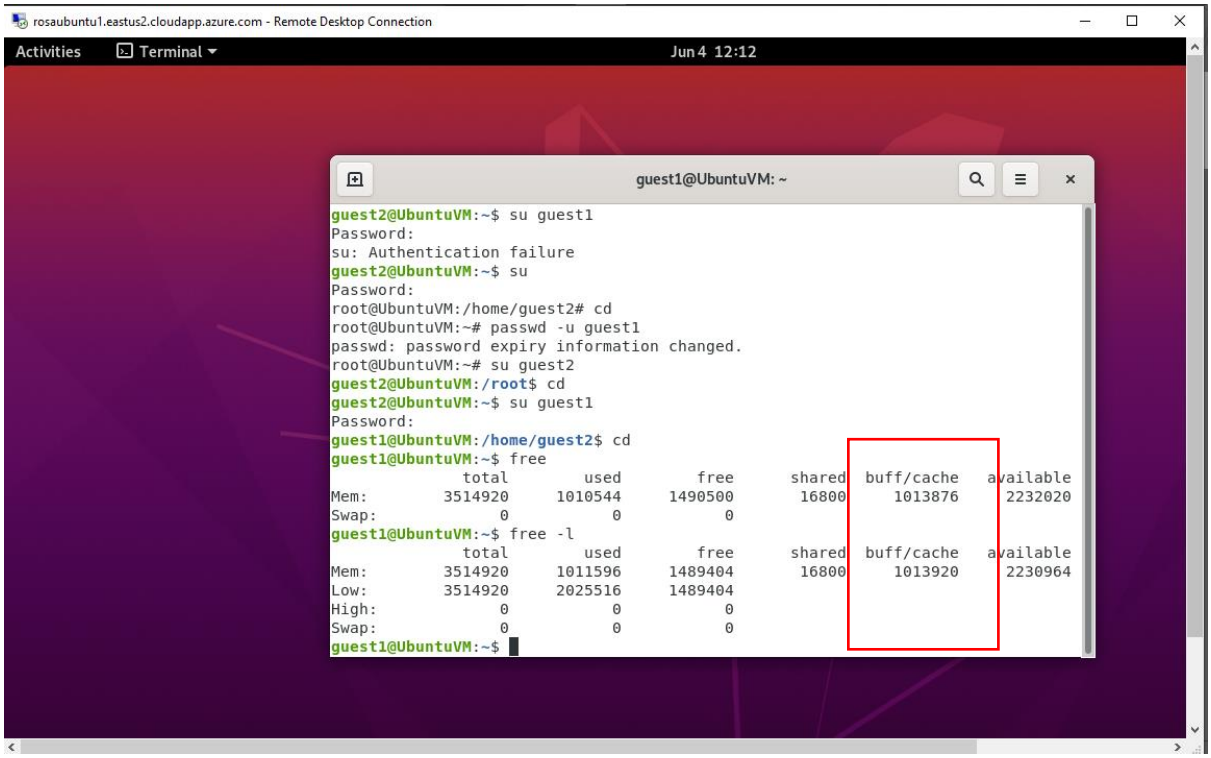
The swapping stats for my machine was empty, but the command is there. :swapon -s



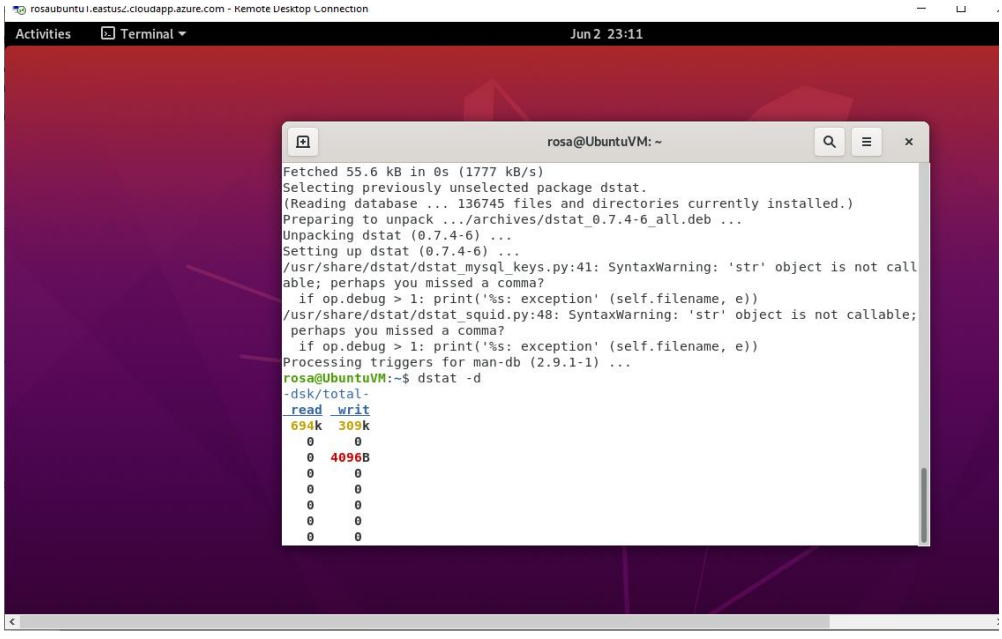
8. # Check File Access statistics. :stat -f



9. Check Buffer analysis statistics. :free or free -l

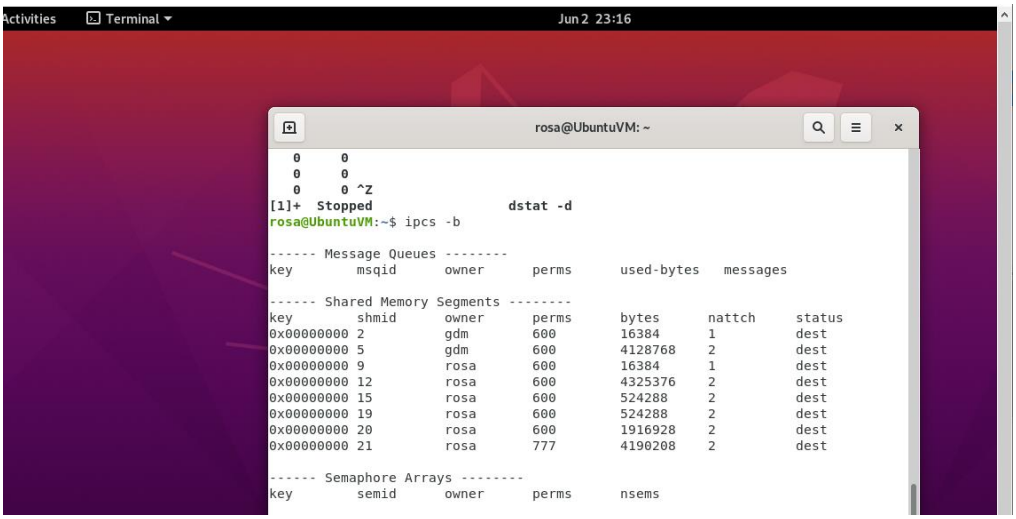


10. Check Disk Activity statistics. :dstat -d

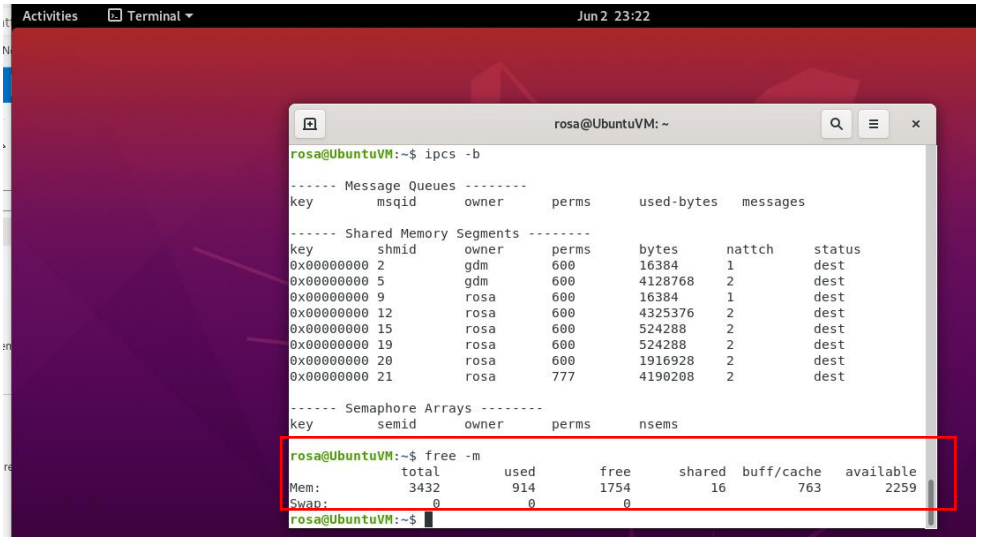


11. # Check Inter process Communication statistics.

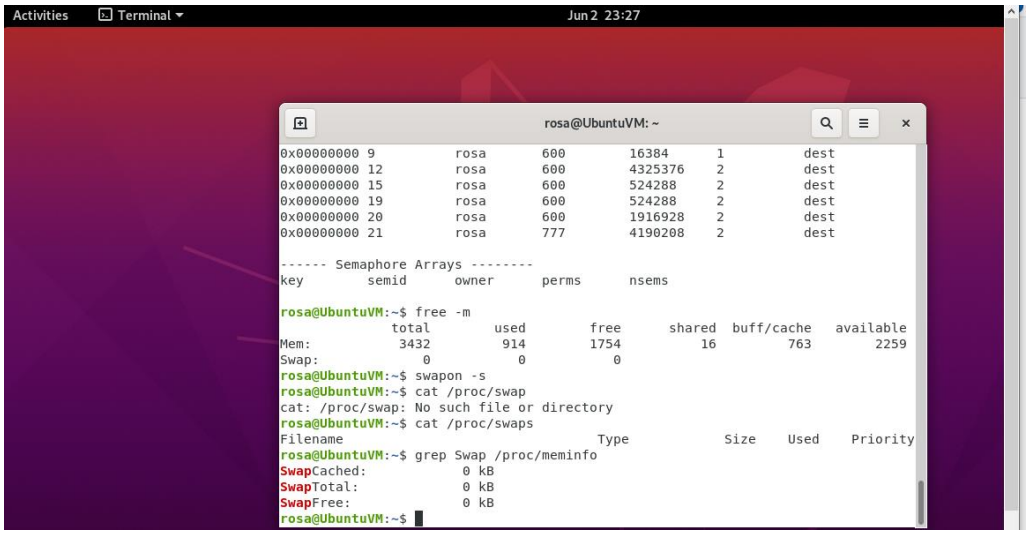
ipcs -b



12. # Check Unused Memory in the server. Free -m



13. Check Swap Activities. Grep Swap /proc/meminfo

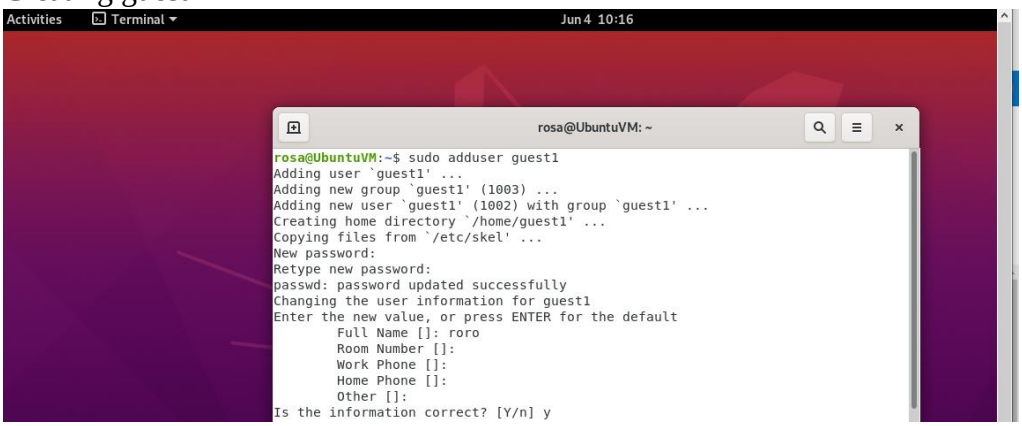


PART B – USER ACTIVITIES

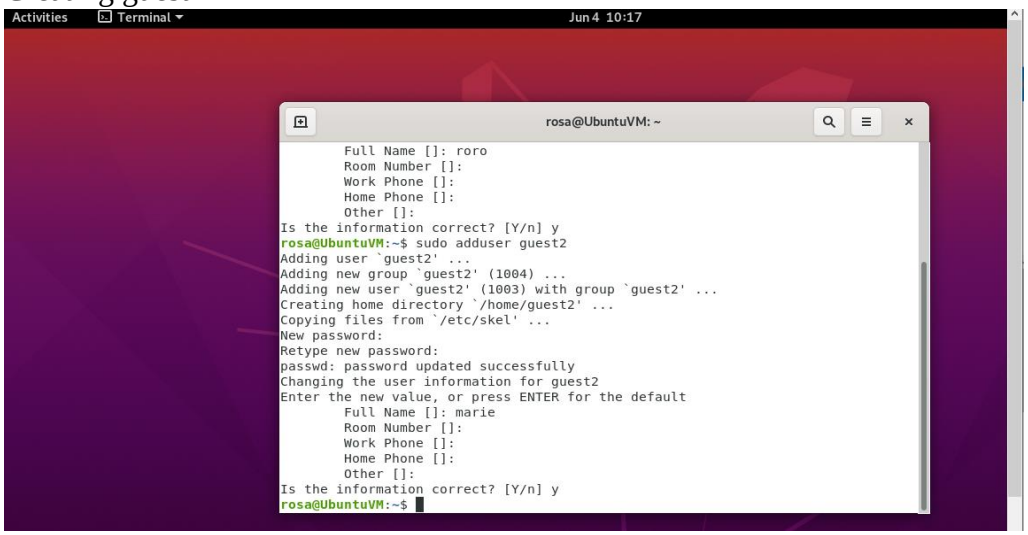
Login to your terminal in Ubuntu. After logging in, the following were performed.

Create a user account called user1 and another user2

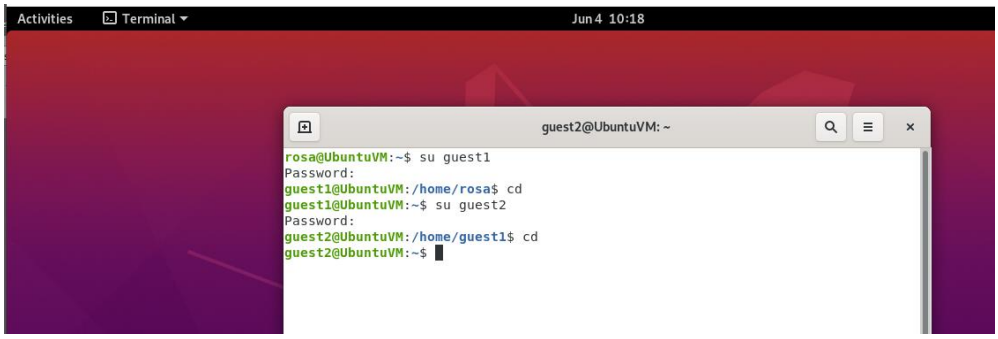
Creating guest 1



Creating guest2

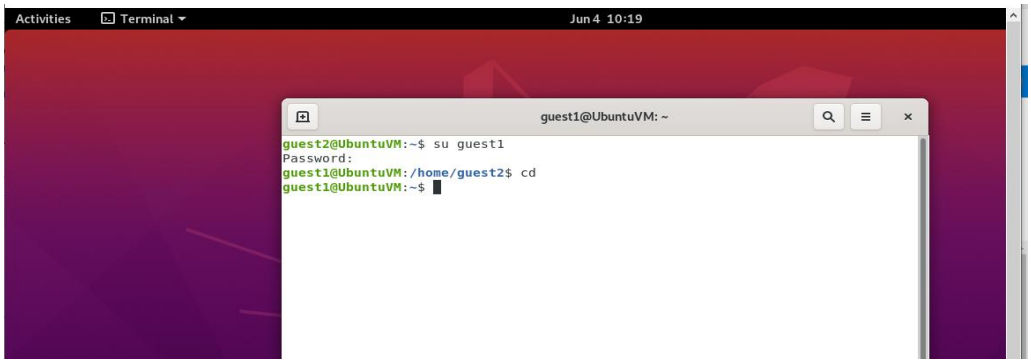


Ensure user1 and user2 are password protected.



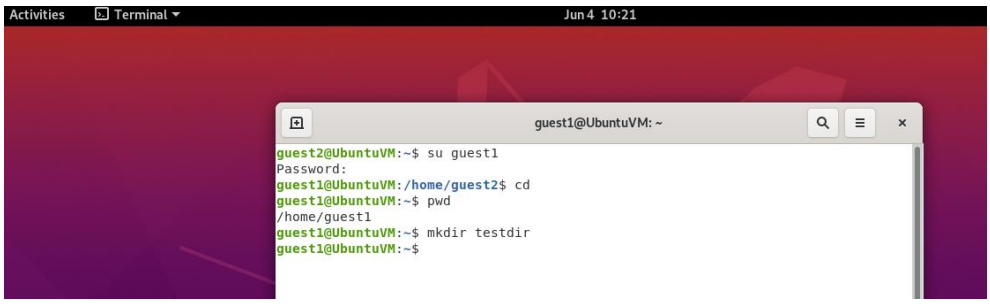
Logout and login as user1

To login to guest1, use the su guest1 command and type the password



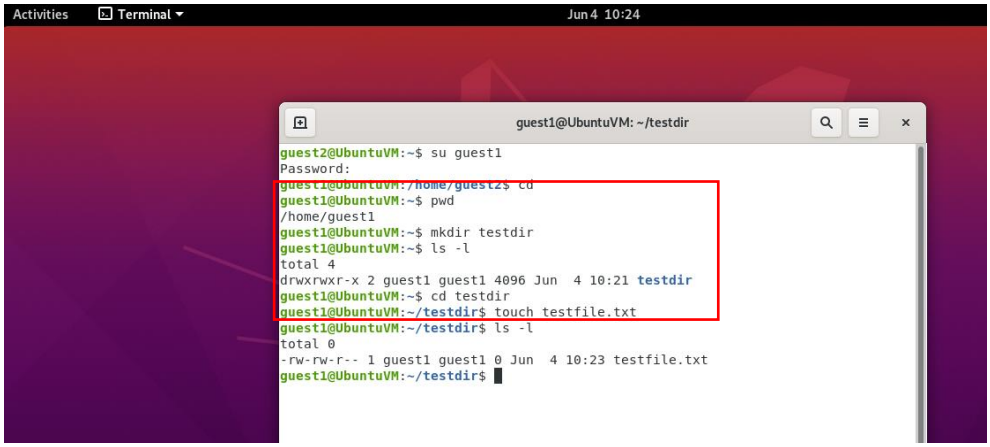
Create a testdir

Whiles in guest1, create a testdir folder with the mkdir command



Create a file testfile in testdir

Use cd to enter the testdir folder, and use the touch command to create the testfile

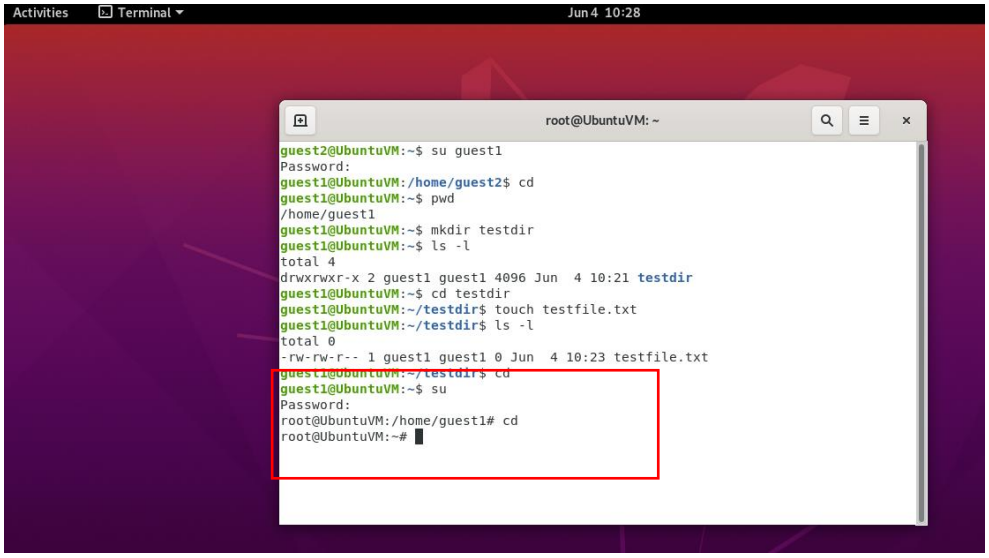


Verify the ownership and the group of the testfile

To verify, use the ls -l command to display information about the file. The ownership and group are all guest1.

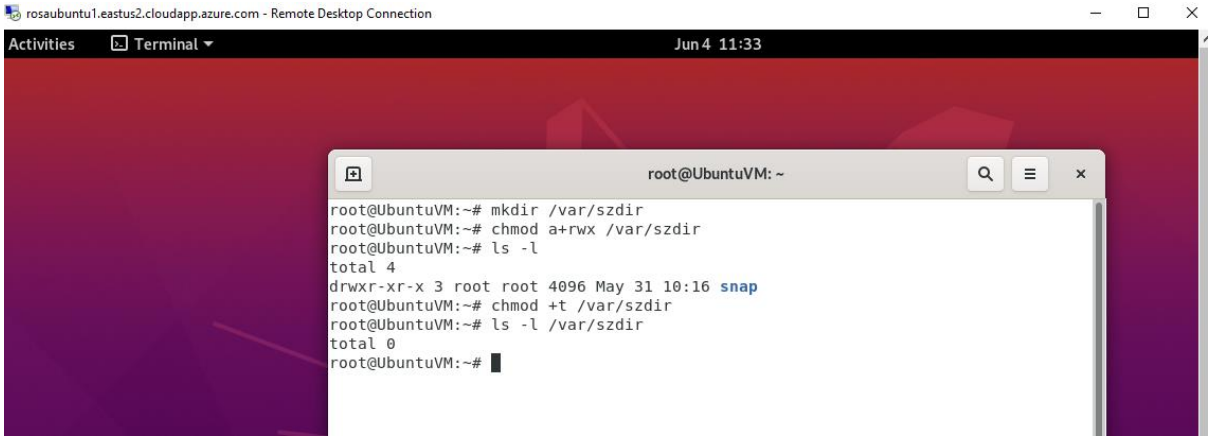
Switch to Superuser account

Switching to superuser or root user with su command. Then after, enter the password.



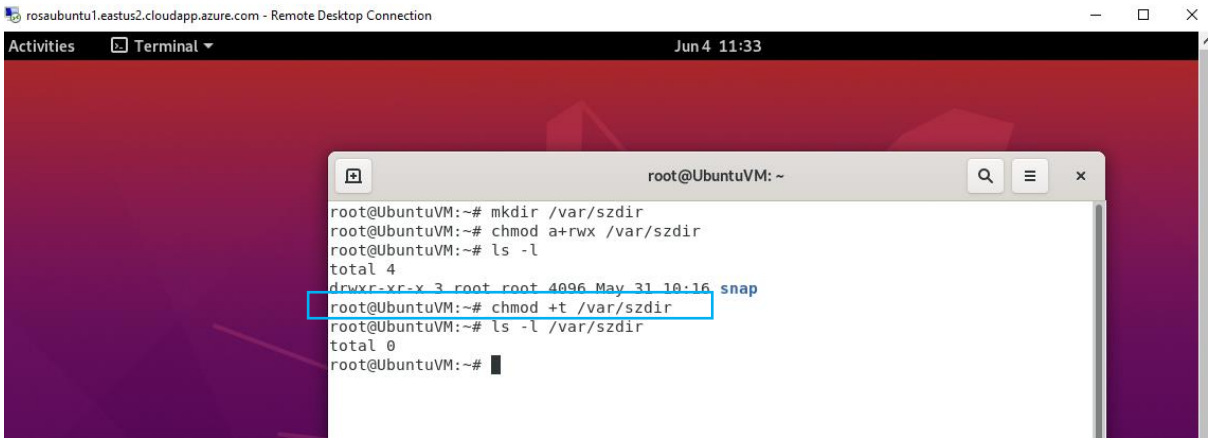
Create a public directory dir

Created a public directory from root. Gave all users the permission to read, write and execute (using chmod a+rwx).



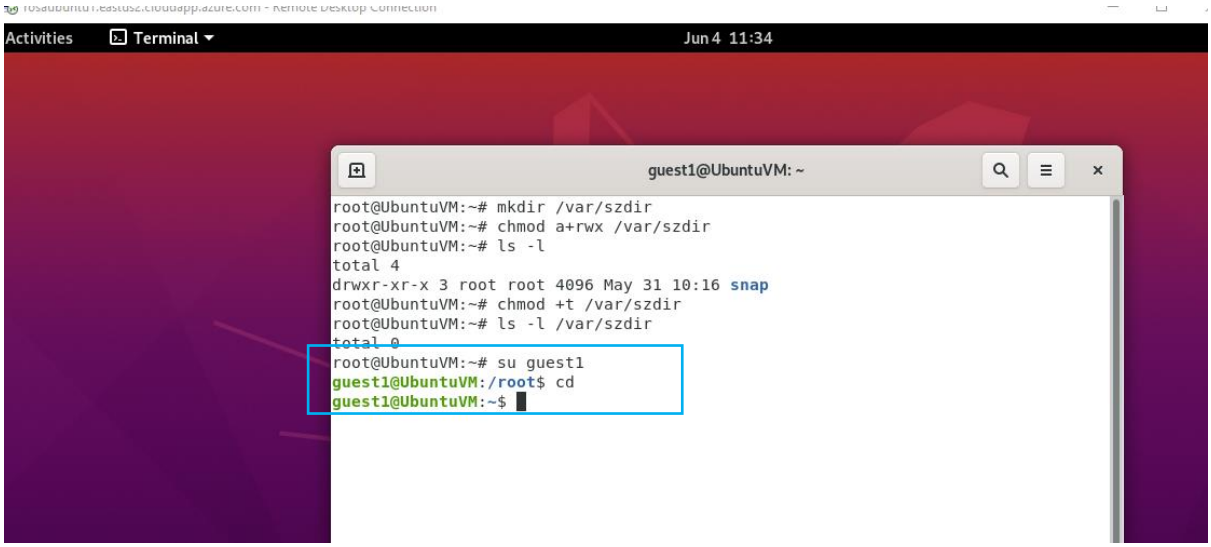
Set stickybit (save text attribute) on dir1

Also set sticky bit on dir with the chmod +t directorypath command.



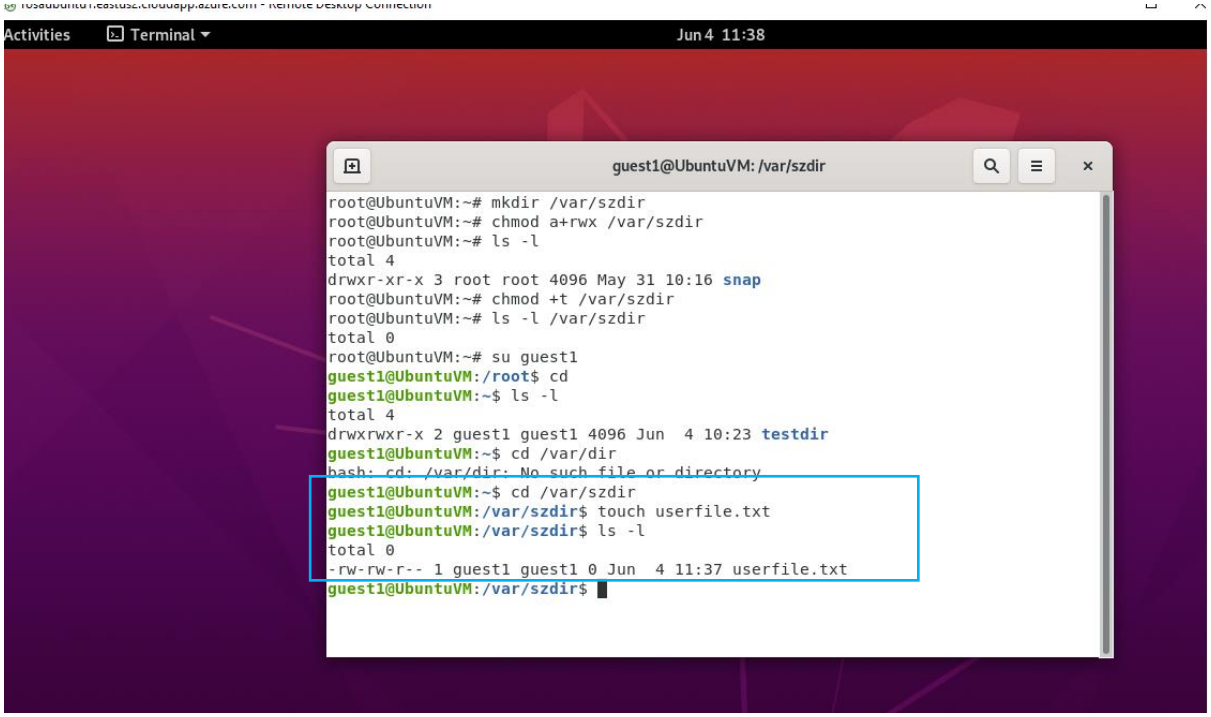
Logout and login as a normal user user1

Login to guest1 using the su guest1 command.



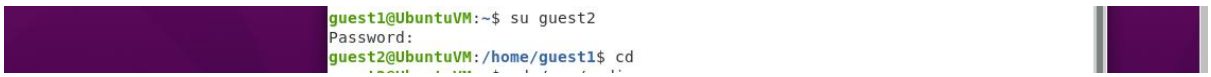
Create a file userfile1 in dir1

Navigate/ cd to the public folder and create the userfile in there with the touch command.



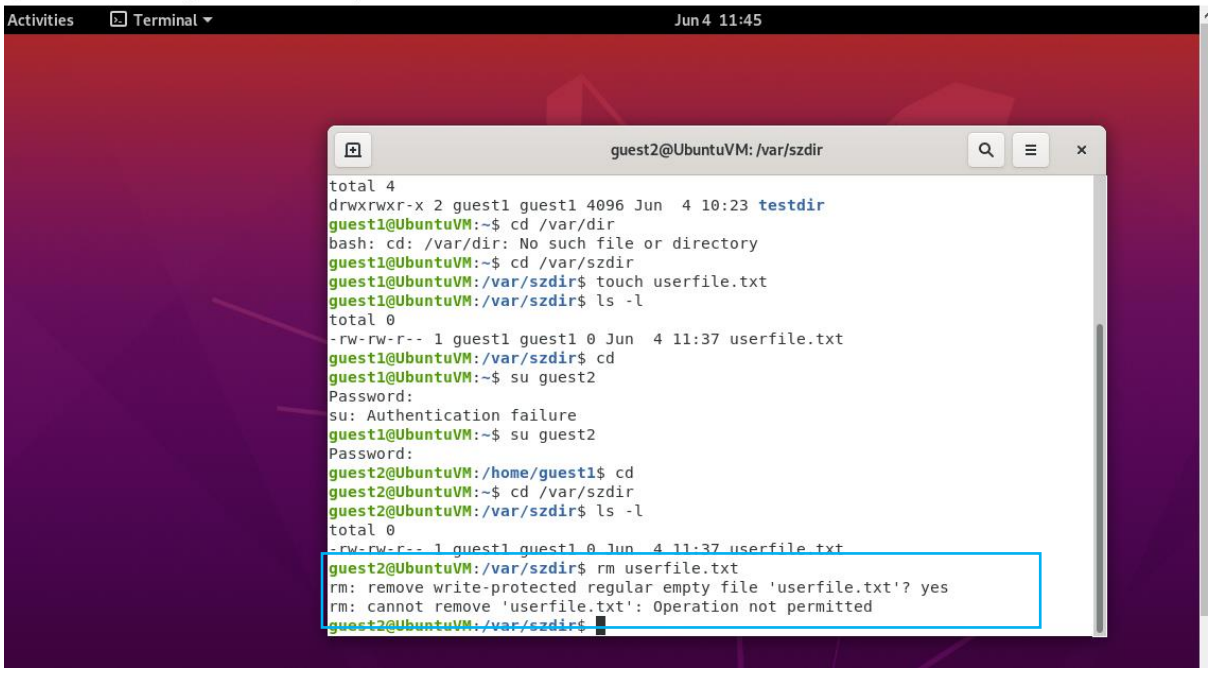
Login as a different user user2

Use the su guest2 to login to a different user called guest2



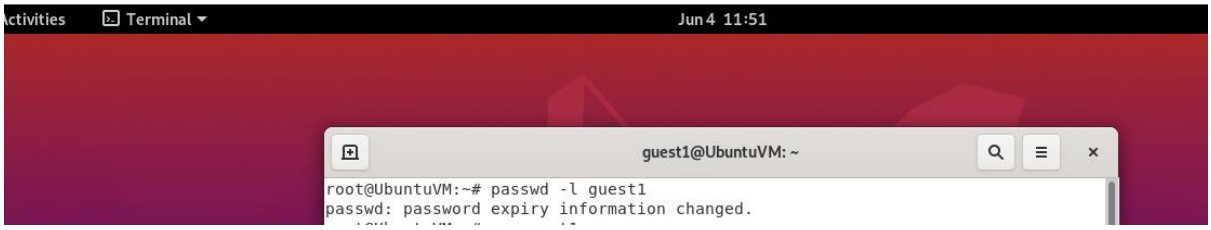
Try to edit or remove the file

Trying to remove the userfile created by guest1 in guest2 using the rm command. Permission was denied due to sticky bit placed on folder.

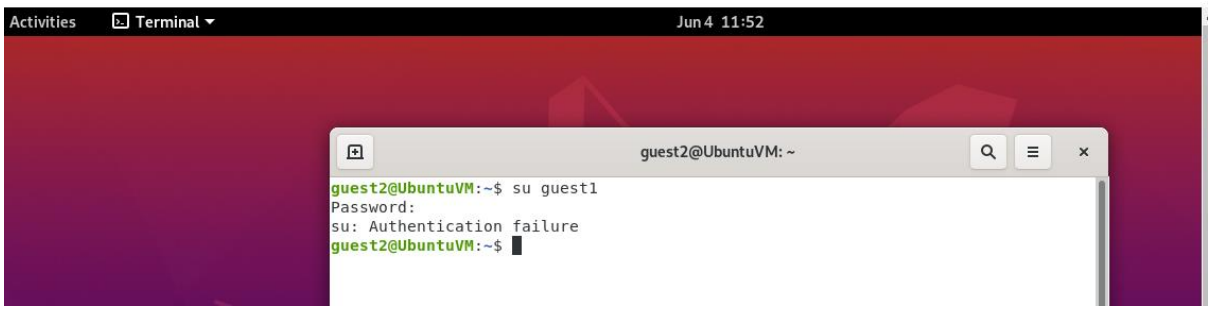


Temporarily disable user logins

To temporarily disable the login of user: guest1, I locked the password from the root.



To verify that the password was locked and guest1 could not login, I tried logging in from guest2 with the password, but access/ authentication failed.



I re-enabled the password for guest1 so they could login again and verified.