ITIM

PRACTICAL - 2

Name : Yagna Patel
Enrollment No. : 211621020
Batch : 61(CBA)

Tasks :

Question 1: Operators and Consultants are members of an IT support company. They need to start sharing information. servera contains a properly configured share directory located at /shares/content that hosts files. Currently, only members of the operators group have

access to this directory, but members of the consultants group need full access to this directory. The consultant1 user is a member of

the consultants group but has caused problems on many occasions, so this user should not have access to the directory.

Your task is to add appropriate ACL entries to the directory and its contents so that members of the consultants group have full access, but deny the consultant1 user any access. Make sure that future files and directories stored in /shares/content get appropriate ACL entries applied.

Question 2: Create a txt file in a folder and allow only a specific user the read and execute access. Ensure that the user is not able to modify the content of the file.

Question 3: A stock finance agency is setting up a collaborative share directory to hold case files, which members of the managers group will have read and write permissions on. The co-founder of the agency, manager1, has decided that members of the contractors group should also be able to read and write to the share directory. However, manager1 does not trust the contractor3 user (a member of the contractors group), and as such, contractor3 should have access to the directory restricted to

read-only. manager1 has created the users and groups, and has started the process of setting up the share directory, copying in some

templates files. Because manager1 has been too busy, it falls to you to finish the job. Your task is to complete the setup of the share

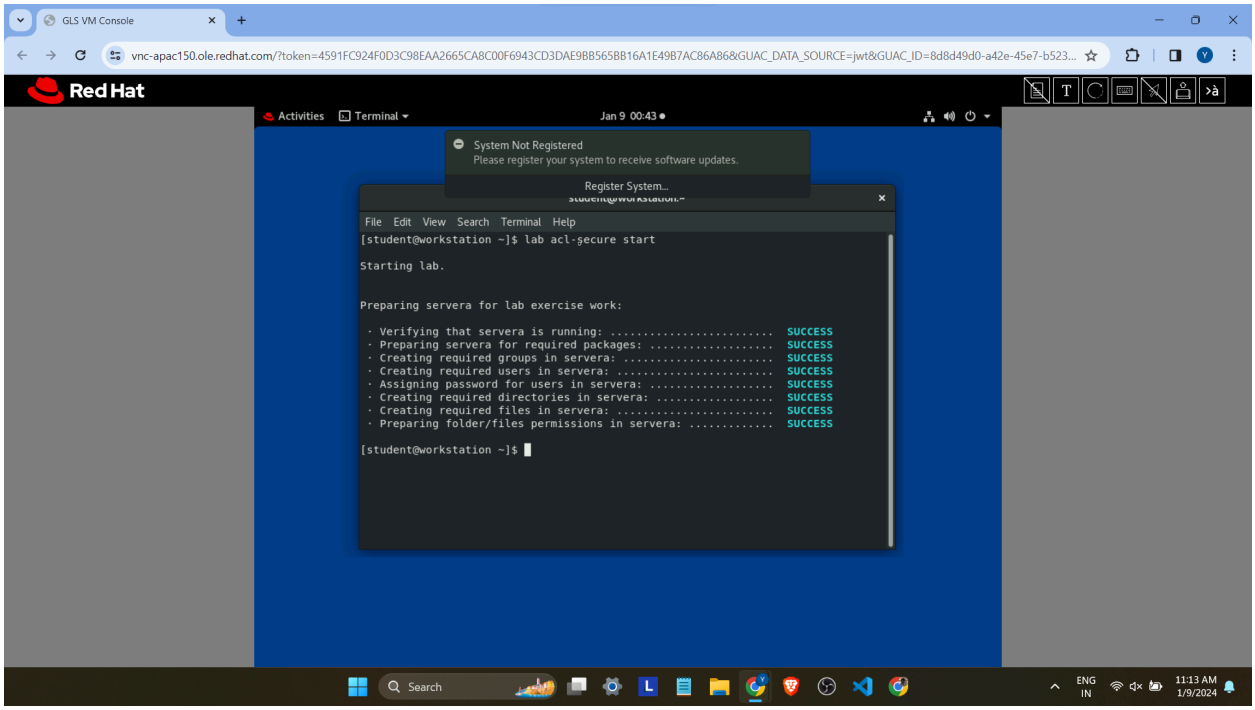
directory. The directory and all of its contents should be owned by the managers group, with the files updated to read and write for the

owner and group (managers). Other users should have no permissions. You also need to provide read and write permissions for

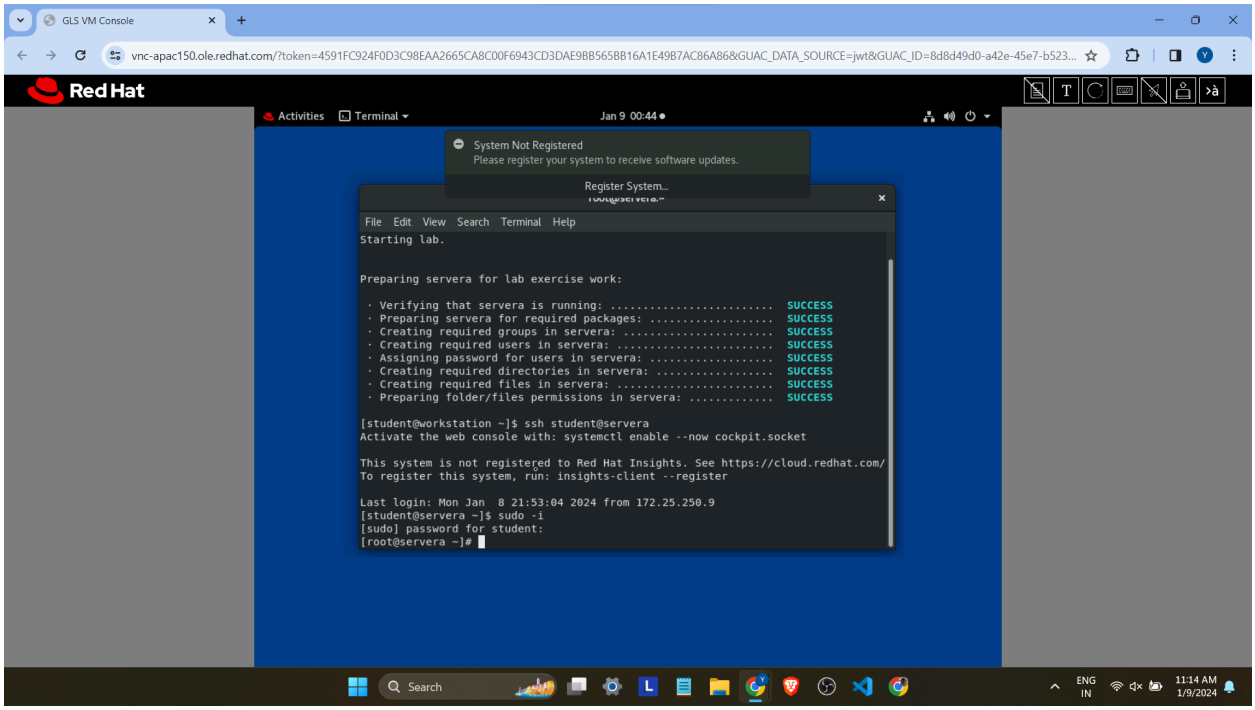
the contractors group, with the exception of contractor3, who only gets read permissions. Make sure your setup applies to existing and future files.

Question 1: Operators and Consultants are members of an IT support company. They need to start sharing information. servera contains a properly configured share directory located at /shares/content that hosts files. Currently, only members of the operators group have access to this directory, but members of the consultants group need full access to this directory. The consultant1 user is a member of the consultants group but has caused problems on many occasions, so this user should not have access to the directory.Your task is to add appropriate ACL entries to the directory and its contents so that members of the consultants group have full access, but deny the consultant1 user any access. Make sure that future files and directories stored in /shares/content get appropriate ACL entries applied.

- Starting the lab using **lab acl-secure start**

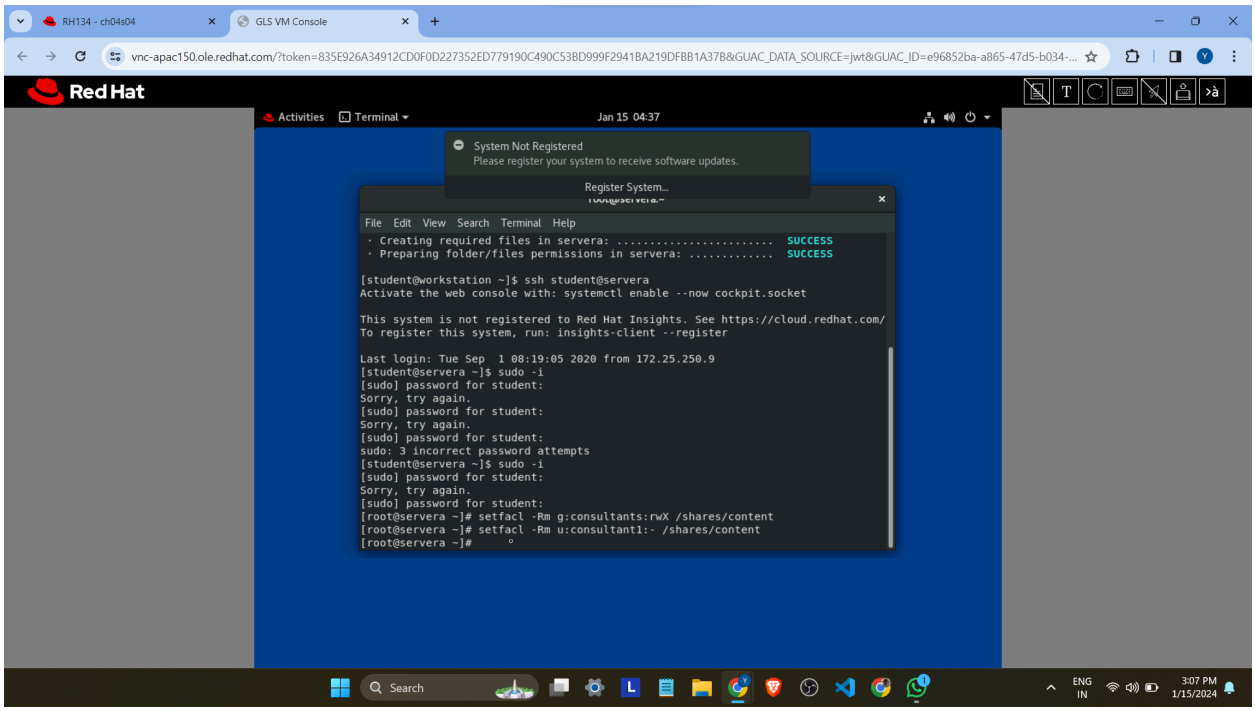


- Use the ssh command to log in to `servera` as the `student` user using **ssh student@servera** and enter into root user using **sudo -i**

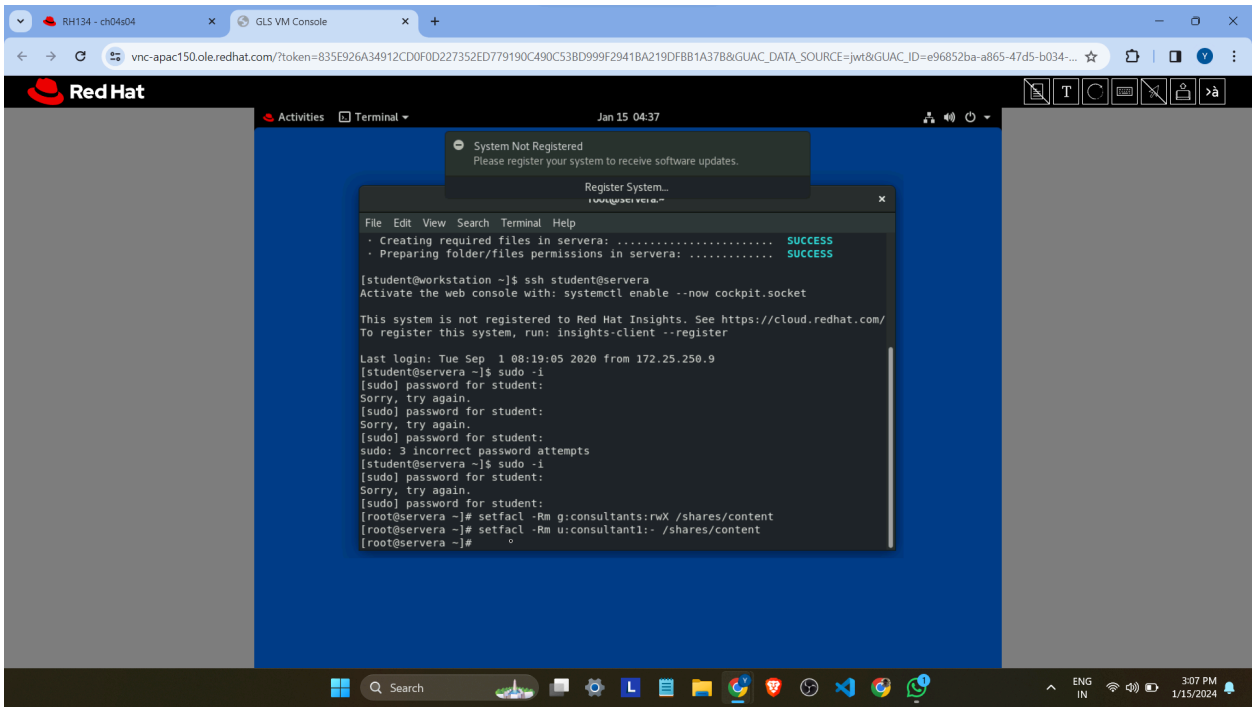


- Set ACL rules for group consultants and user consultant1

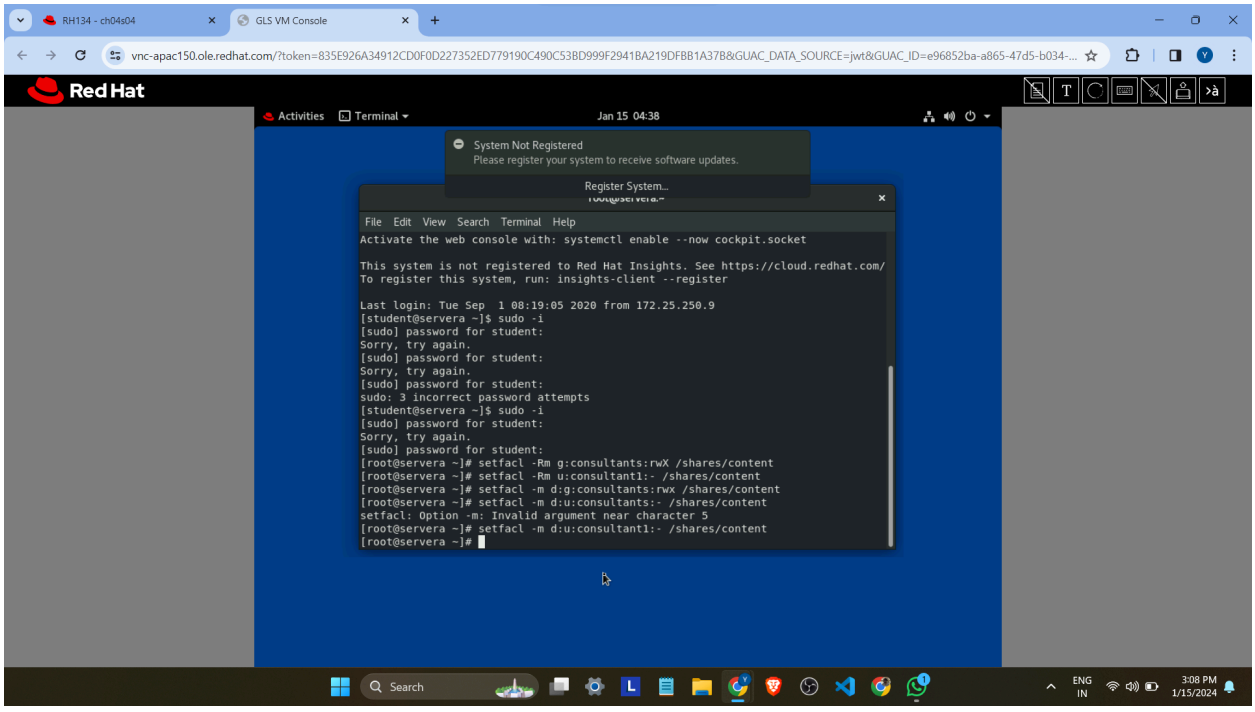
  1) **setfacl –Rm g:consultants:rwx /shares/content** to recursively update /shares/content directory and grant read, write and executive permissions to group CONSULTANTS



2) **setfacl -Rm u:consultant1:- /shares/content** to recursively update /shares/content directory and grant no permissions to user consultant1.

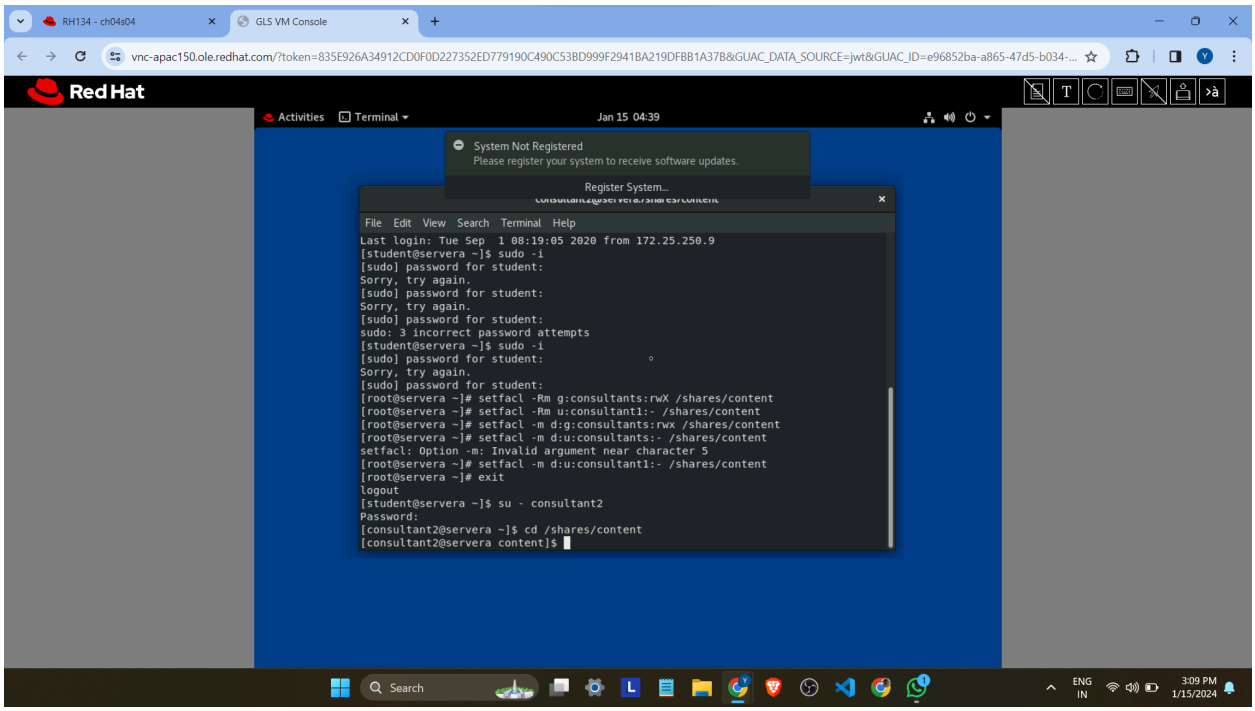


- Now set default ACL rules of groups and users with same permissions:
  setfacl -Rm d:u:consultant1:- /shares/content for users
  setfacl –Rm g:consultants:rwx /shares/content for groups

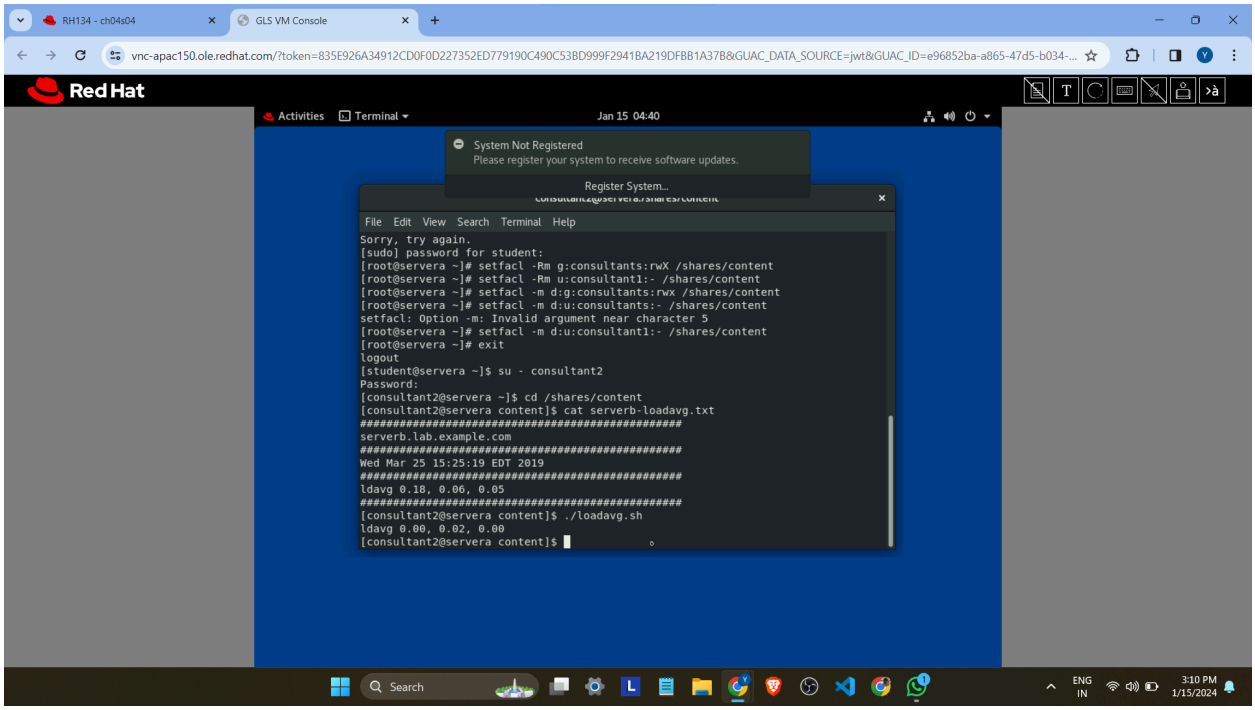


-

- Now to check our ACL rules login into consultant2 and access the shared folder

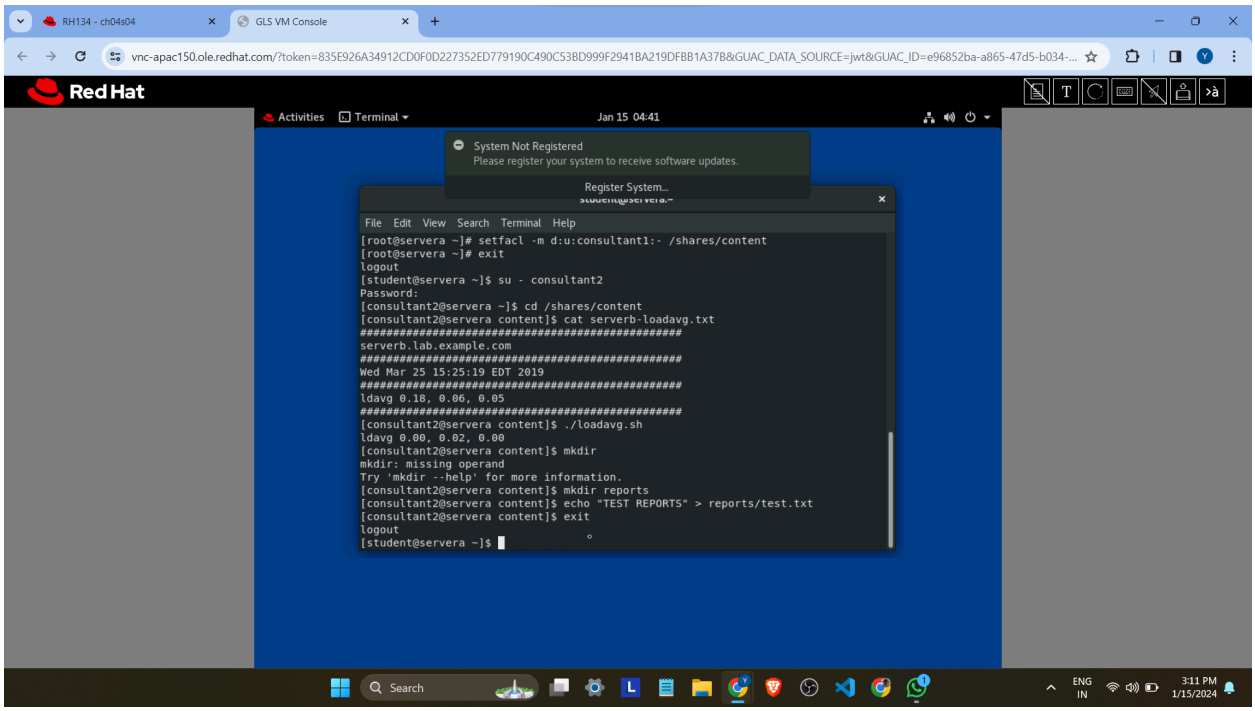


Reading a file inside /shares/content folder using **cat serverb-loadavg.txt** and **./loadavg.sh**

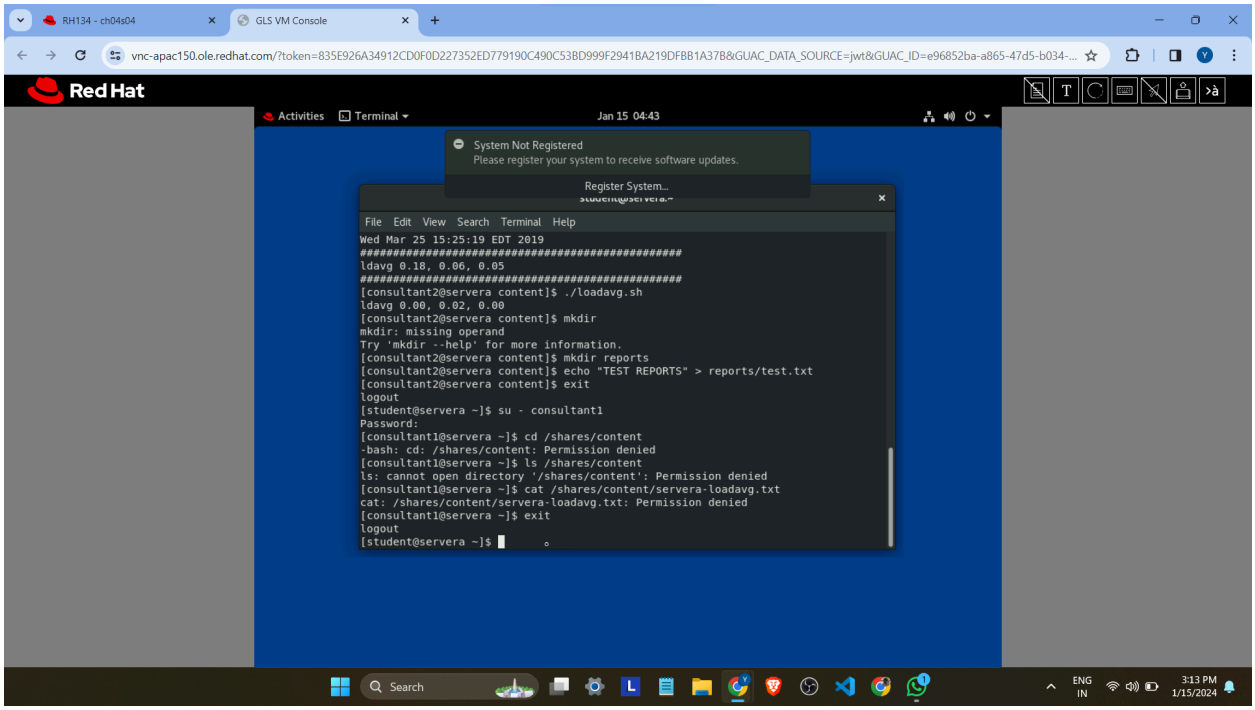


- Now make a new folder insider shared folder “reports” and a file “test.txt” with TEST REPORTS inside the file
  Commands: **mkdir reports** to make folder and

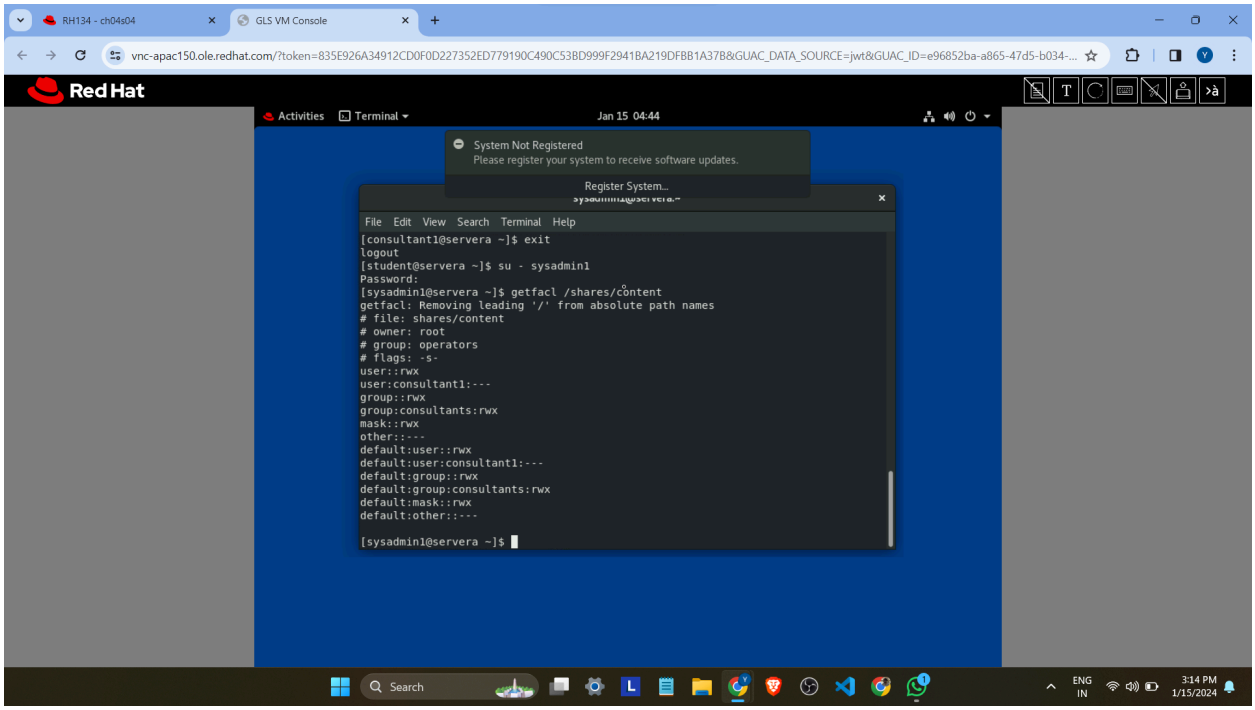
echo “TEST REPORTS” > reports/text.txt and to make file and add text init

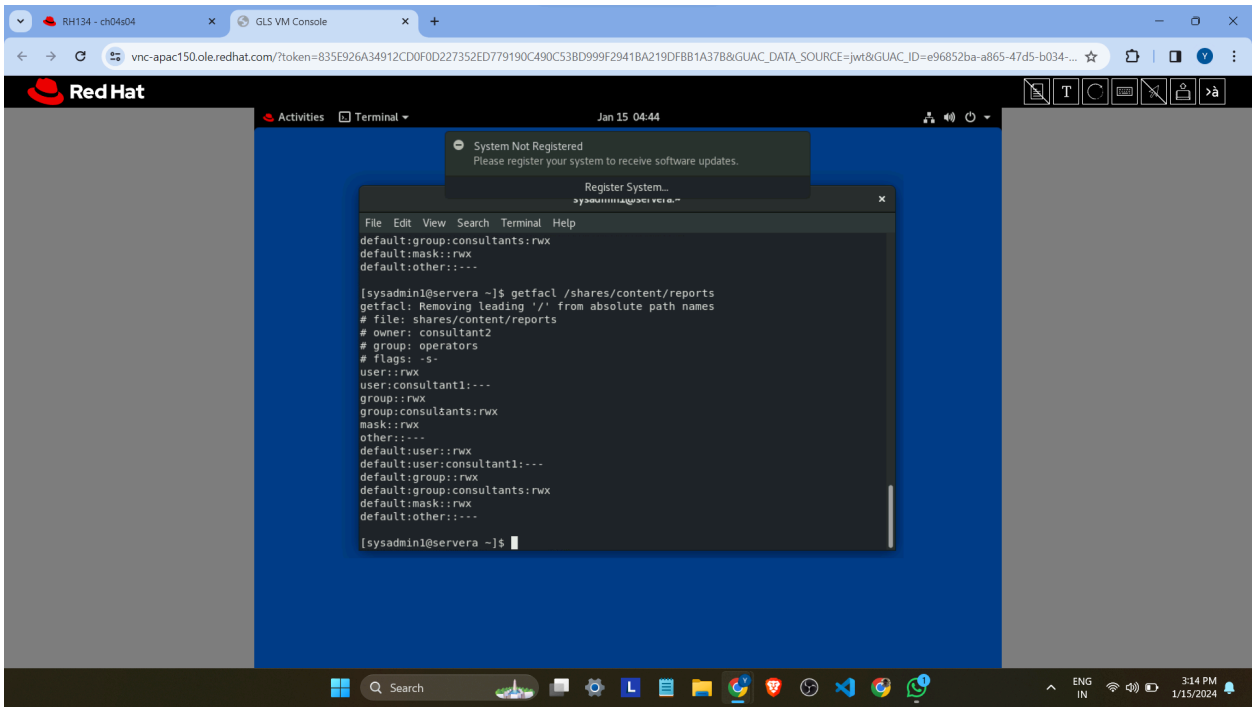


- Now get into user consultant1 which has no permissions and try accessing the shared folder using the same commands as consultant2.

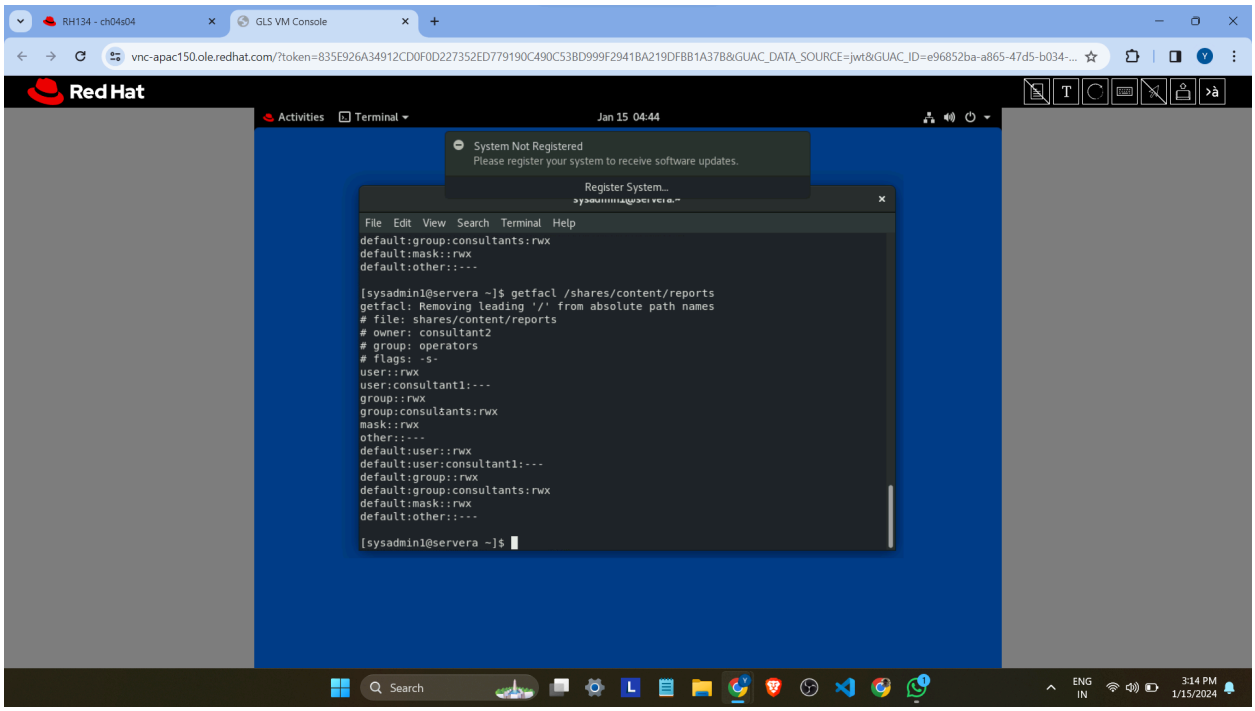


- Now Login to admin user sysadmin and Use getfacl to see all the ACL entries on `/shares/content` and the ACL entries on `/shares/content/reports`.using commands : **getfacl /shares/content** and **getfacl /shares/content/reports**


RH134 - ch04s04
GLS VM Console
vnc-apac150.ole.redhat.com/?token=835E926A34912CD0F0D227352ED779190C490C53BD999F2941BA219DFBB1A37B8&GUAC_DATA_SOURCE=jwt&GUAC_ID=e96852ba-a865-47d5-b034-...
Red Hat
Activities
Terminal
Jan 15 04:44
System Not Registered
Please register your system to receive software updates.
Register System...
File Edit View Search Terminal Help
[consultant1@servera ~]$ exit
logout
[student@servera ~]$ su - sysadmin1
Password:
[sysadmin1@servera ~]$ getfacl /shares/content
getfacl: Removing leading '/' from absolute path names
file: shares/content
owner: root
group: operators
flags: -s-
user::rwx
user:consultant1:---
group::rwx
group:consultants:rwx
mask::rwx
other::---
default:user::rwx
default:user:consultant1:---
default:group::rwx
default:group:consultants:rwx
default:mask::rwx
default:other::---
[sysadmin1@servera ~]$
Search
ENG
IN
3:14 PM
1/15/2024


RH134 - ch04s04
GLS VM Console
vnc-apac150.ole.redhat.com/?token=835E926A34912CD0F0D227352ED779190C490C53BD999F2941BA219DFBB1A37B8&GUAC_DATA_SOURCE=jwt&GUAC_ID=e96852ba-a865-47d5-b034-...
Red Hat
Activities
Terminal
Jan 15 04:44
System Not Registered
Please register your system to receive software updates.
Register System...
File Edit View Search Terminal Help
default:group:consultants:rwx
default:mask::rwx
default:other::---
[sysadmin1@servera ~]$ getfacl /shares/content/reports
getfacl: Removing leading '/' from absolute path names
file: shares/content/reports
owner: consultant2
group: operators
flags: -s-
user::rwx
user:consultant1:---
group::rwx
group:consul&ants:rwx
mask::rwx
other::---
default:user::rwx
default:user:consultant1:---
default:group::rwx
default:group:consultants:rwx
default:mask::rwx
default:other::---
[sysadmin1@servera ~]$
Search
ENG
IN
3:14 PM
1/15/2024

- - now logout from admin and server using **exit** and close the lab using **lab acl-secure finish**



Question 2: Create a txt file in a folder and allow only a specific user the read and execute access. Ensure that the user is not able to modify the content of the file.

- Create a file name hello.txt inside shared folder name prac2

```
touch: cannot touch 'prac2/hello.txt': No such file or directory
[root@servera content]# mkdir prac2
[root@servera content]# echo "hello" > prac2>hello.txt
-bash: prac2: Is a directory
[root@servera content]# echo "hello" > prac2/hello.txt
```

- Give permissions to the users that access it ie consultant2

```
[root@servera ~]# cd /shares/content
[root@servera content]# ls -l
total 12
-rw-rwx---+ 1 sysadmin1 operators 835 Jan 15 12:14 loadavg.sh
drwxrwsr-x+ 2 root      operators  23 Jan 15 12:20 prac2
-rw-rw----+ 1 operator1 operators 276 Jan 15 12:14 servera-loadavg.txt
-rw-rw----+ 1 operator1 operators 276 Jan 15 12:14 serverb-loadavg.txt
drwxrws---+ 2 root      operators 100 Jan 15 12:14 server-info
[root@servera content]# setfacl -Rm u:consultant2:r-x prac2
[root@servera content]# setfacl -m d:u:consultant2:r-x prac2
[root@servera content]# ls -l
total 12
-rw-rwx---+ 1 sysadmin1 operators 835 Jan 15 12:14 loadavg.sh
drwxr-sr-x+ 2 root      operators  23 Jan 15 12:20 prac2
-rw-rw----+ 1 operator1 operators 276 Jan 15 12:14 servera-loadavg.txt
-rw-rw----+ 1 operator1 operators 276 Jan 15 12:14 serverb-loadavg.txt
drwxrws---+ 2 root      operators 100 Jan 15 12:14 server-info
```

- Check if consultant 2 can access the folder and check if it can write in the files

```
[root@servera content]# su - consultant2
Last login: Mon Jan 15 12:19:46 EST 2024 on pts/0
[consultant2@servera ~]$ cd /shares/content
[consultant2@servera content]$ ls
loadavg.sh  prac2  servera-loadavg.txt  serverb-loadavg.txt  server-info
[consultant2@servera content]$ cat prac2/hello.txt
hello
[consultant2@servera content]$ echo "hello" > prac2/hello.txt
-bash: prac2/hello.txt: Permission denied
[consultant2@servera content]$
```

Question 3: A stock finance agency is setting up a collaborative share directory to hold case files, which members of the managers group will have read and write permissions on. The co-founder of the agency, manager1, has decided that members of the contractors group should also be able to read and write to the share directory. However, manager1 does not trust the contractor3 user (a member of the contractors group), and as such, contractor3 should have access to the directory restricted to

read-only. manager1 has created the users and groups, and has started the process of setting up the share directory, copying in some

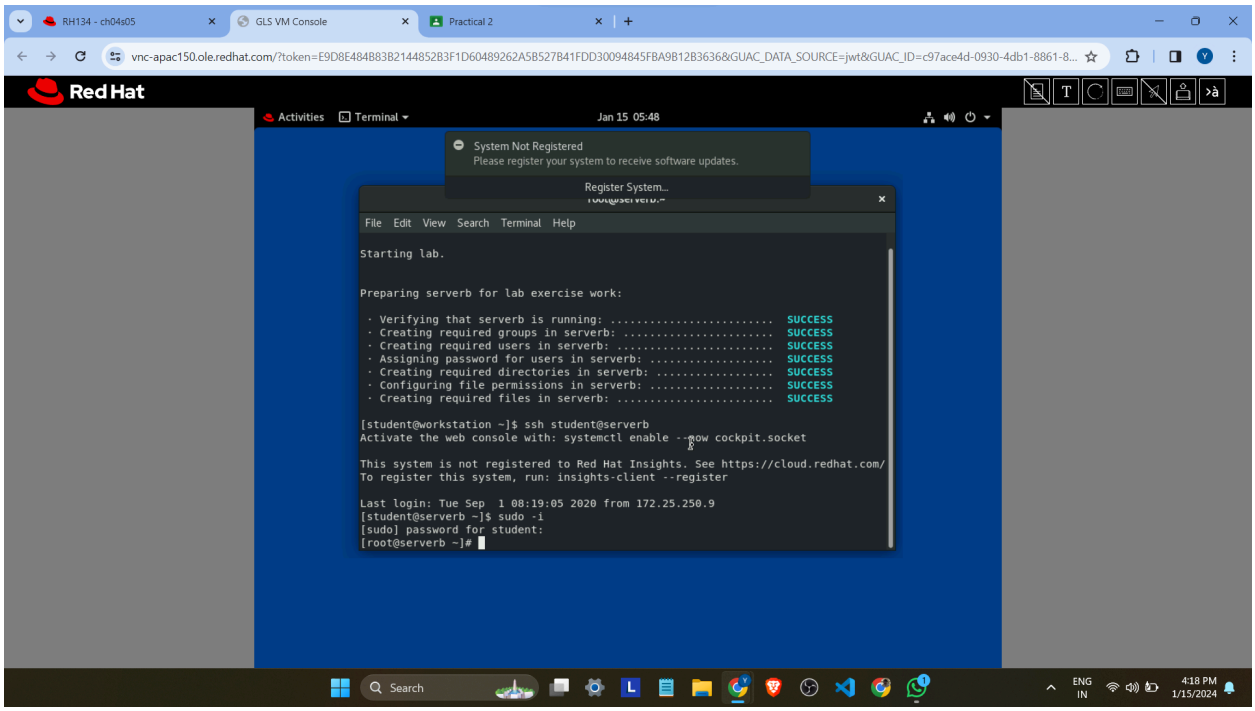
templates files. Because manager1 has been too busy, it falls to you to finish the job. Your task is to complete the setup of the share

directory. The directory and all of its contents should be owned by the managers group, with the files updated to read and write for the

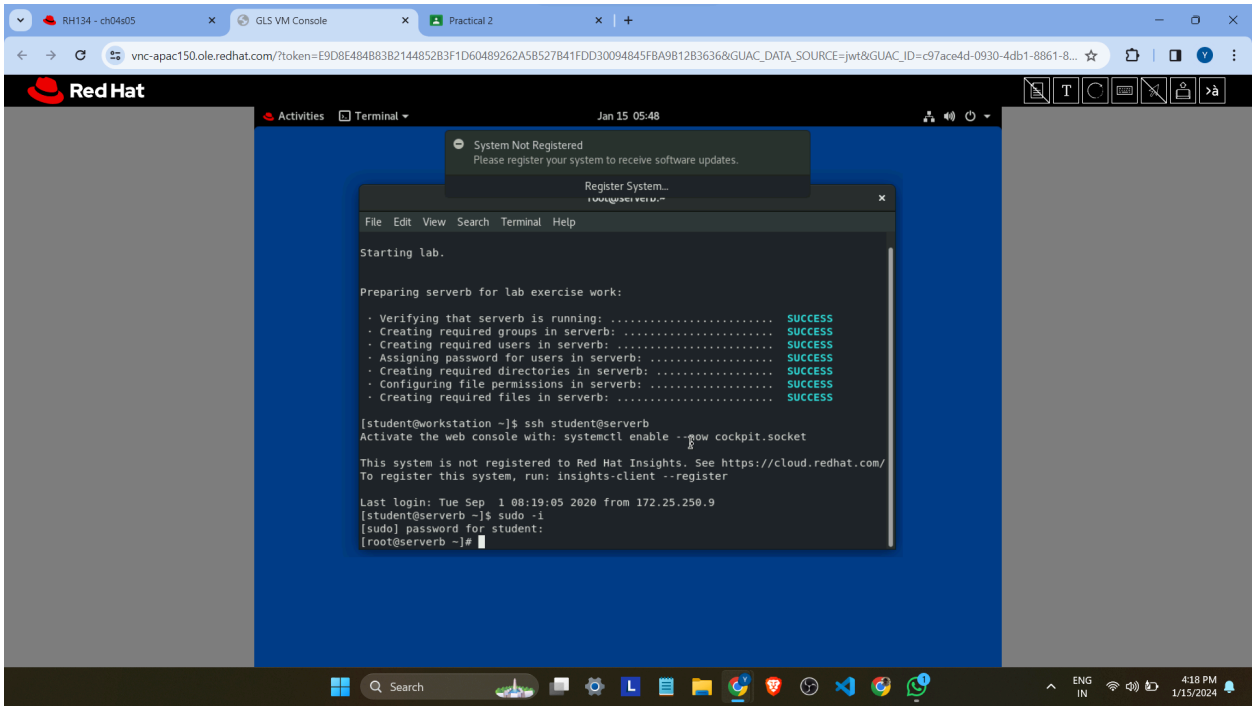
owner and group (managers). Other users should have no permissions. You also need to provide read and write permissions for

the contractors group, with the exception of contractor3, who only gets read permissions. Make sure your setup applies to existing and future files.

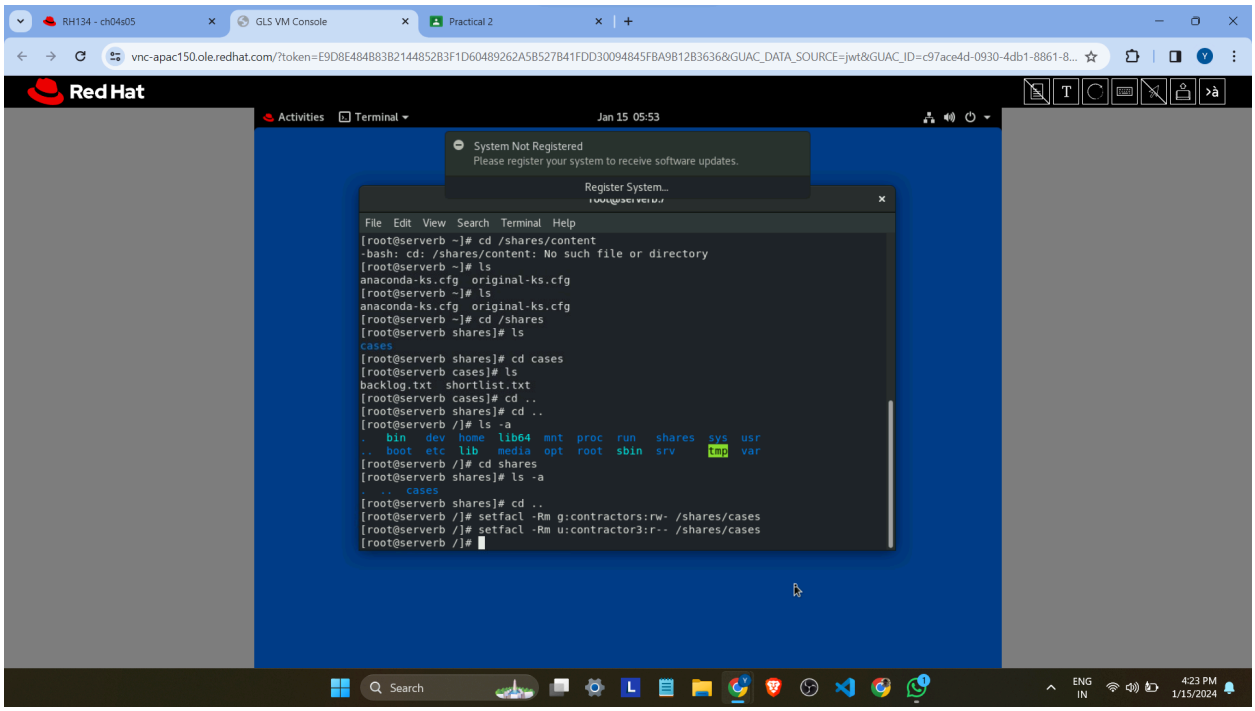
- Starting the lab using **lab acl-review start**



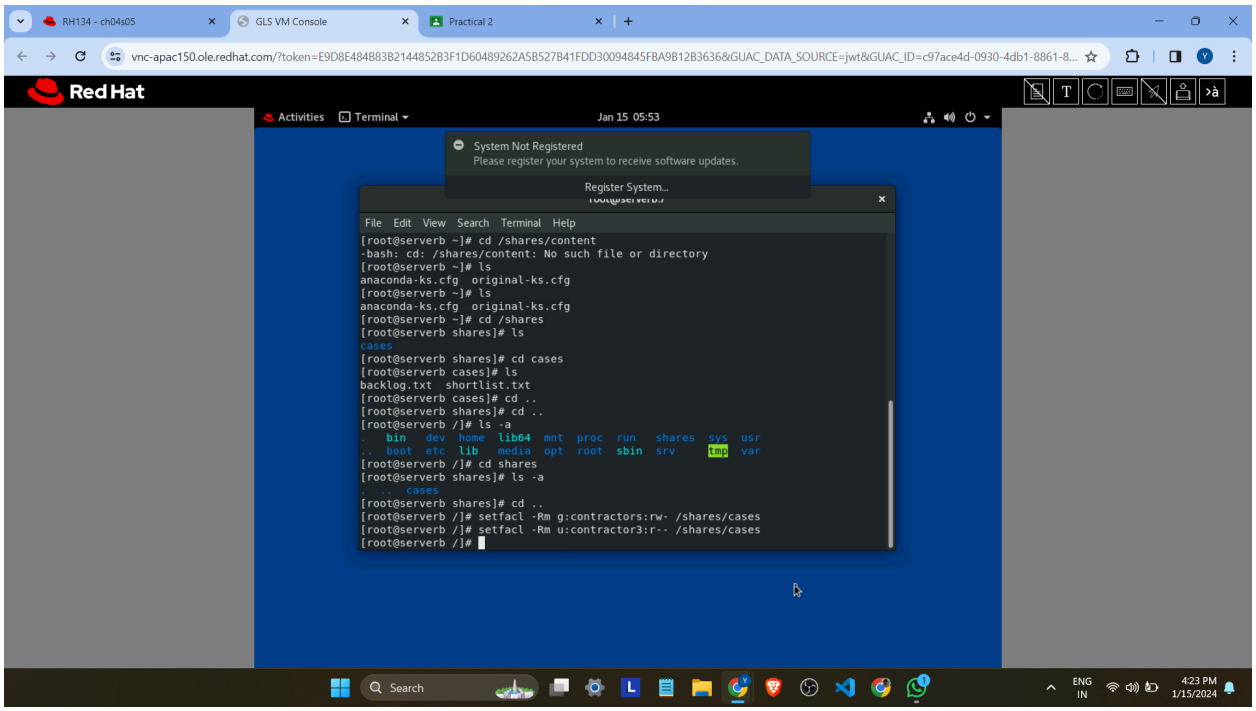
- Use the ssh command to log in to `servera` as the `student` user using **ssh student@serverb** and enter into root user using **sudo -i**



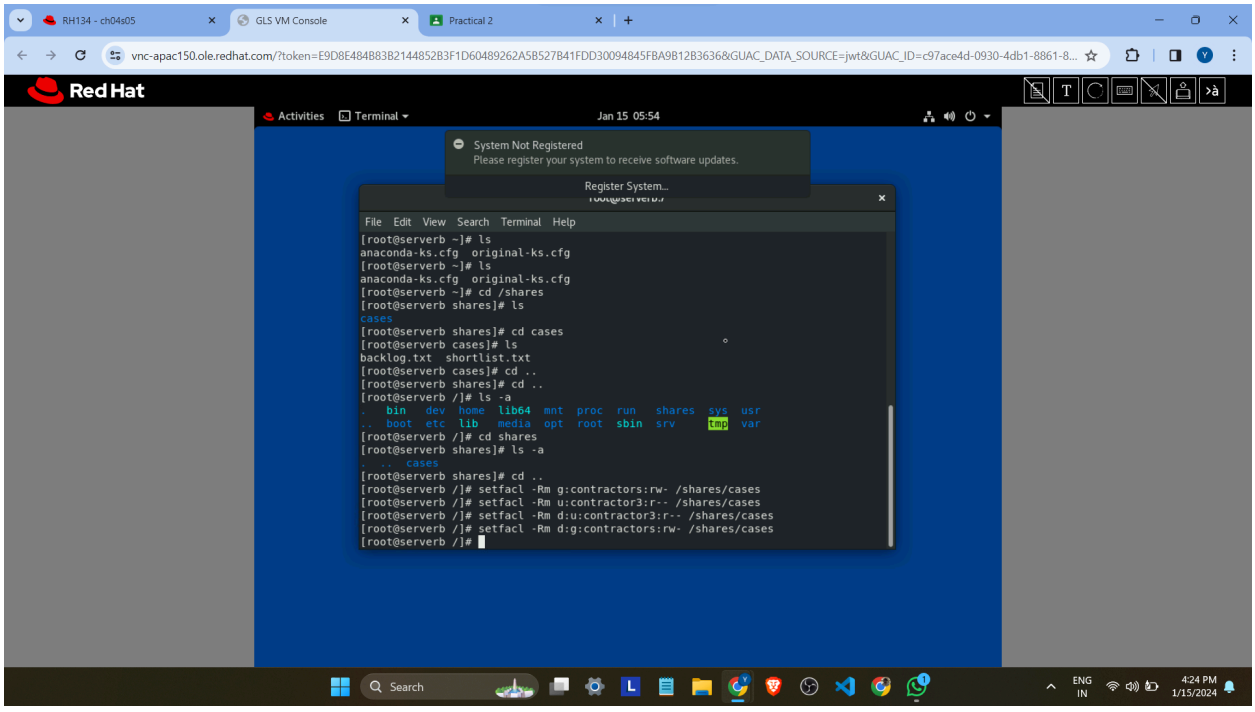
- Set ACL rules for group consultants and user consultant1
  1) **setfacl –Rm g:consultants:rw- /shares/content** to recursively update /shares/content directory and grant read, write and executive permissions to group CONTRACTORS



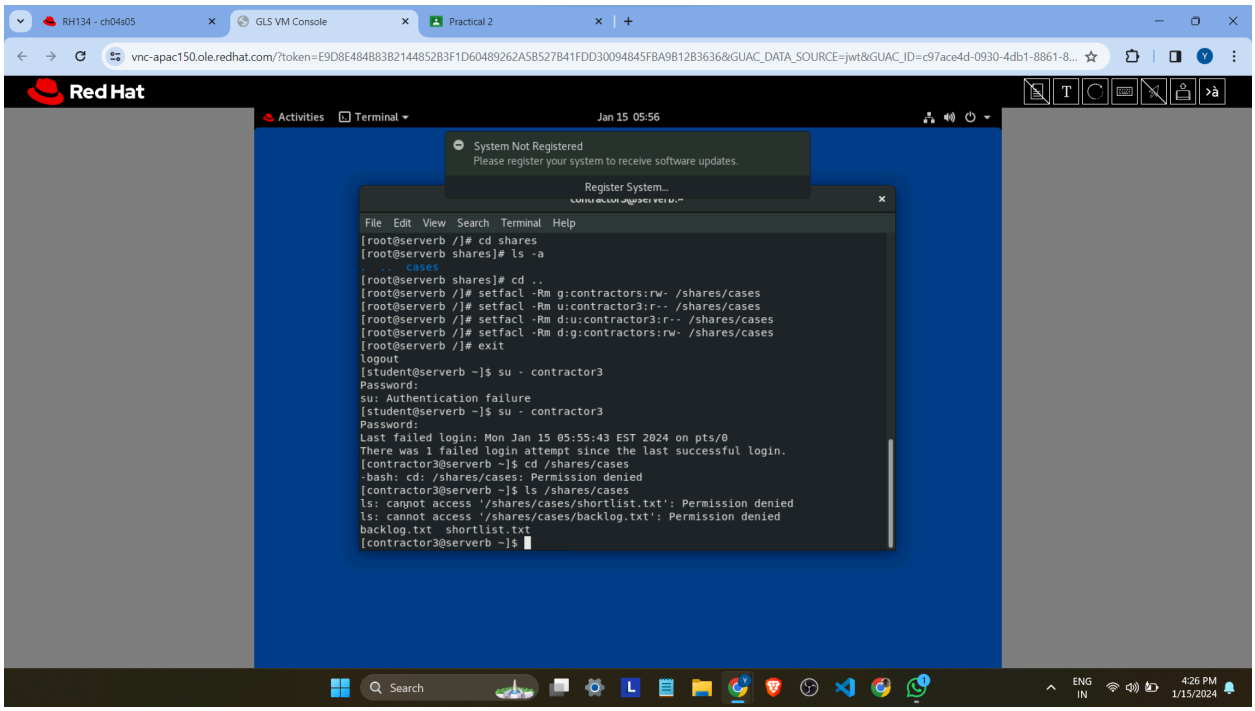
2) **setfacl -Rm u:contractor3:r- /shares/content** to recursively update /shares/content directory and grant no permissions to user consultant1.



- Now set default ACL rules of groups and users with same permissions:
  setfacl -m d:u:contractor3:r- /shares/cases for users
  setfacl –m g:contractors:rw- /shares/cases for groups



- Now to check our ACL rules login into contractor3 and access the shared folder



Trying the same files with manager group Reading a file inside /shares/content folder using **cat serverb-loadavg.txt** and **./loadavg.sh**