

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

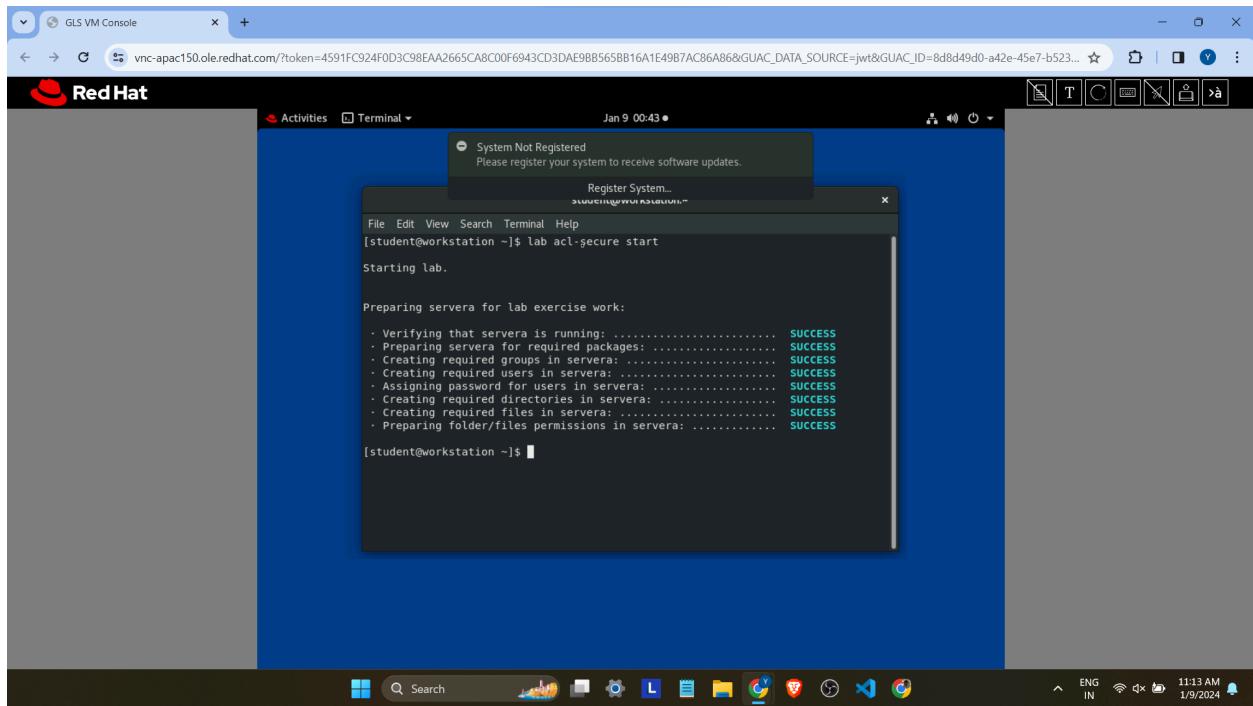
directory. The directory and all of its contents should be owned by the managers group, with the files updated to read and write for the

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**

```

System Not Registered
Please register your system to receive software updates.

Register System...
File Edit View Search Terminal Help
Starting lab.

Preparing servera for lab exercise work:
- Verifying that servera is running: ..... SUCCESS
- Preparing servera for required packages: ..... SUCCESS
- Creating required groups in servera: ..... SUCCESS
- Creating required users in servera: ..... SUCCESS
- Assigning password for users in servera: ..... SUCCESS
- Creating required directories in servera: ..... SUCCESS
- Creating required files in servera: ..... SUCCESS
- Preparing folder/files permissions in servera: ..... SUCCESS

[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Mon Jan  8 21:53:04 2024 from 172.25.250.9
[student@servera ~]$ sudo -i
[sudo] password for student:
[root@servera ~]#

```

- 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

```

System Not Registered
Please register your system to receive software updates.

Register System...
File Edit View Search Terminal Help
Starting lab.

Preparing servera for lab exercise work:
- Creating required files in servera: ..... SUCCESS
- Preparing folder/files permissions in servera: ..... SUCCESS

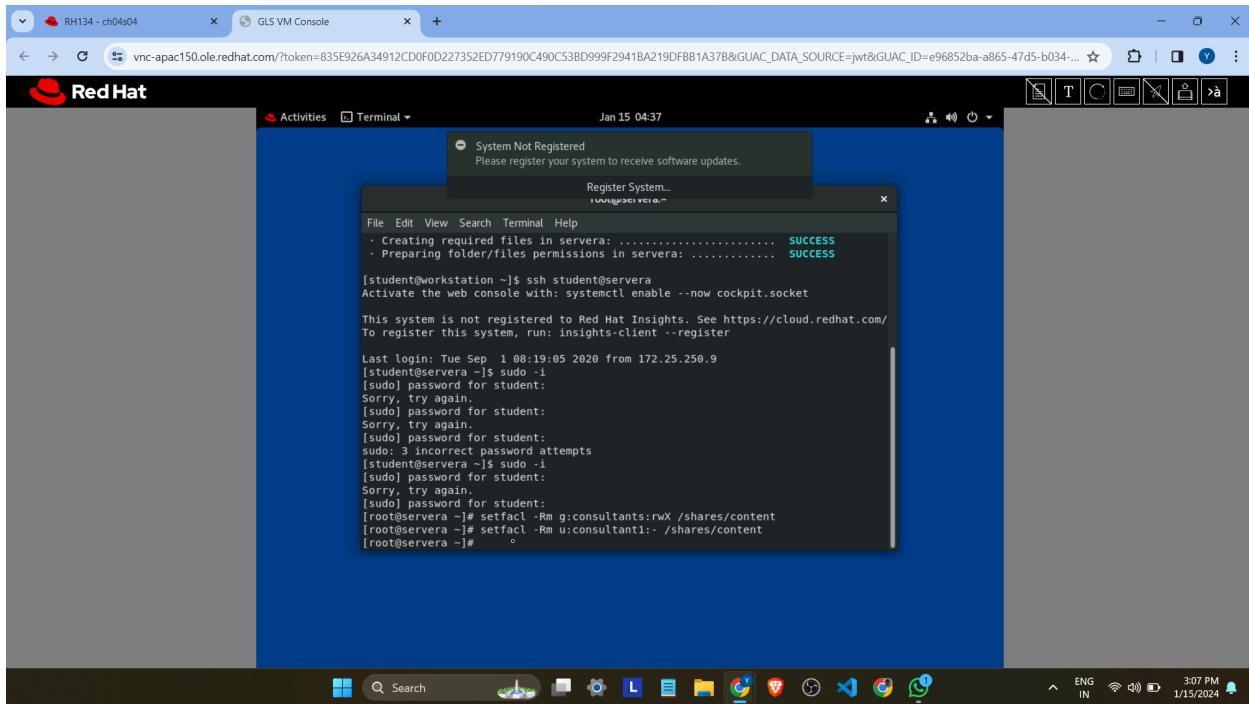
[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Tue Sep  1 08:19:05 2020 from 172.25.250.9
[student@servera ~]$ sudo -i
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
sudo: 3 incorrect password attempts
[student@servera ~]$ sudo -i
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
[root@servera ~]# setfacl -Rm g:consultants:rwx /shares/content
[root@servera ~]# setfacl -Rm u:consultant1:- /shares/content
[root@servera ~]#

```

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



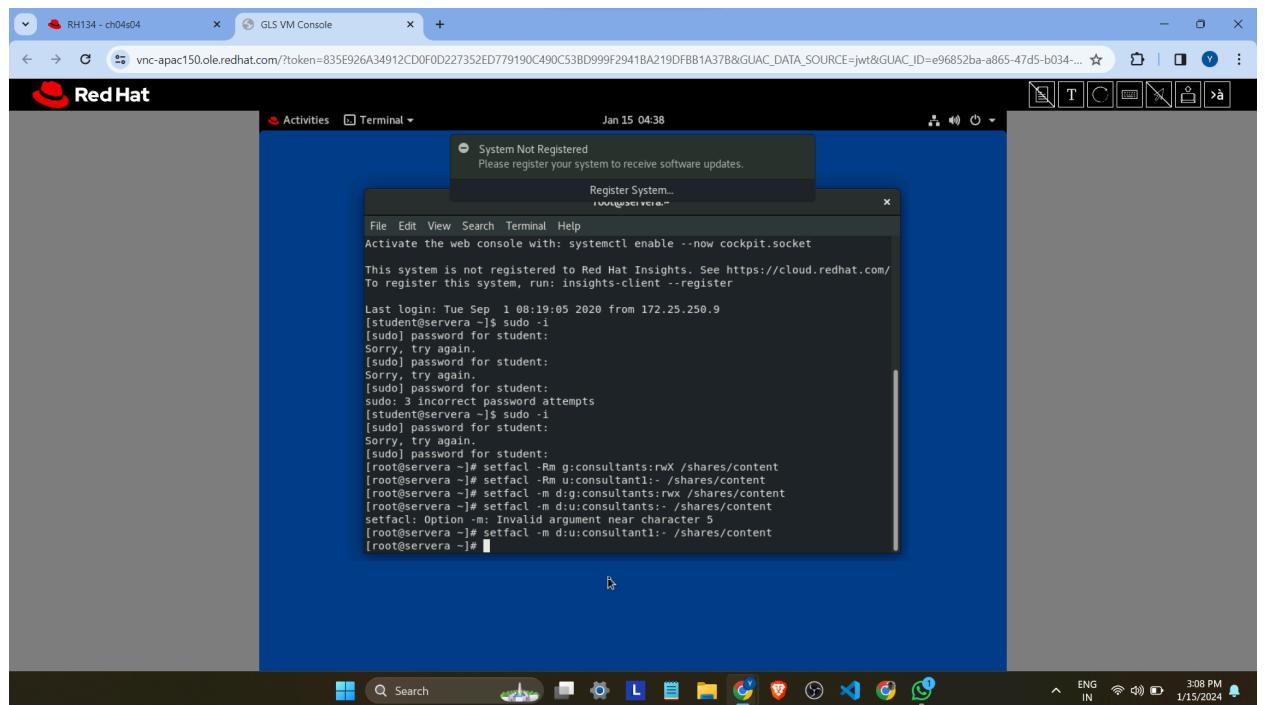
A screenshot of a Red Hat Linux desktop environment. A terminal window is open, showing the command `setfacl -Rm u:consultant1:- /shares/content` being run. The terminal output shows the command was successful. A system message box at the top of the screen says "System Not Registered" and "Please register your system to receive software updates". The desktop interface includes a taskbar with various icons and a system tray at the bottom right.

```
[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Tue Sep 1 08:19:05 2020 from 172.25.250.9
[student@servera ~]$ sudo -i
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
sudo: 3 incorrect password attempts
[student@servera ~]$ sudo -i
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
[student@servera ~]$ setfacl -Rm g:consultants:rwx /shares/content
[student@servera ~]$ setfacl -Rm u:consultant1:- /shares/content
[student@servera ~]$
```

- 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



A screenshot of a Red Hat Linux desktop environment. A terminal window is open, showing the commands `setfacl -Rm d:u:consultant1:- /shares/content` and `setfacl -Rm g:consultants:rwx /shares/content` being run. The terminal output shows both commands were successful. A system message box at the top of the screen says "System Not Registered" and "Please register your system to receive software updates". The desktop interface includes a taskbar with various icons and a system tray at the bottom right.

```
[student@servera ~]$ sudo -i
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
sudo: 3 incorrect password attempts
[student@servera ~]$ sudo -i
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
[student@servera ~]$ setfacl -Rm g:consultants:rwx /shares/content
[student@servera ~]$ setfacl -Rm u:consultant1:- /shares/content
[student@servera ~]$ setfacl -Rm d:u:consultant1:- /shares/content
[student@servera ~]$ setfacl -Rm m:dig:consultants:rwx /shares/content
[student@servera ~]$ setfacl -Rm m:du:consultants:- /shares/content
setfacl: Option -m: Invalid argument near character 5
[student@servera ~]$ setfacl -Rm d:u:consultant1:- /shares/content
[student@servera ~]$
```

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

```

RH134 - ch04s04          GLS VM Console
vnc-apac150.ole.redhat.com/?token=835E926A34912CD0F0D227352ED779190C490C53BD999F2941BA219DFBB1A37B&GUAC_DATA_SOURCE=jwt&GUAC_ID=e96852ba-a865-47d5-b034-...
Red Hat
Activities Terminal
System Not Registered
Please register your system to receive software updates.
Register System...
File Edit View Search Terminal Help
Last login: Tue Sep 1 08:19:05 2020 from 172.25.250.9
[student@servera ~]$ sudo -
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
sudo: 3 incorrect password attempts
[student@servera ~]$ sudo -
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
[root@servera ~]# setfacl -Rm g:consultants:rwx /shares/content
[root@servera ~]# setfacl -Rm u:consultant1:- /shares/content
[root@servera ~]# setfacl -m d:g:consultants:rwx /shares/content
[root@servera ~]# setfacl -m d:u:consultant1:- /shares/content
setfacl: Option -m: Invalid argument near character 5
[root@servera ~]# setfacl -m d:u:consultant1:- /shares/content
[root@servera ~]# exit
logout
[student@servera ~]$ su -
Password:
[consultant2@servera ~]$ cd /shares/content
[consultant2@servera content]$ 

```

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

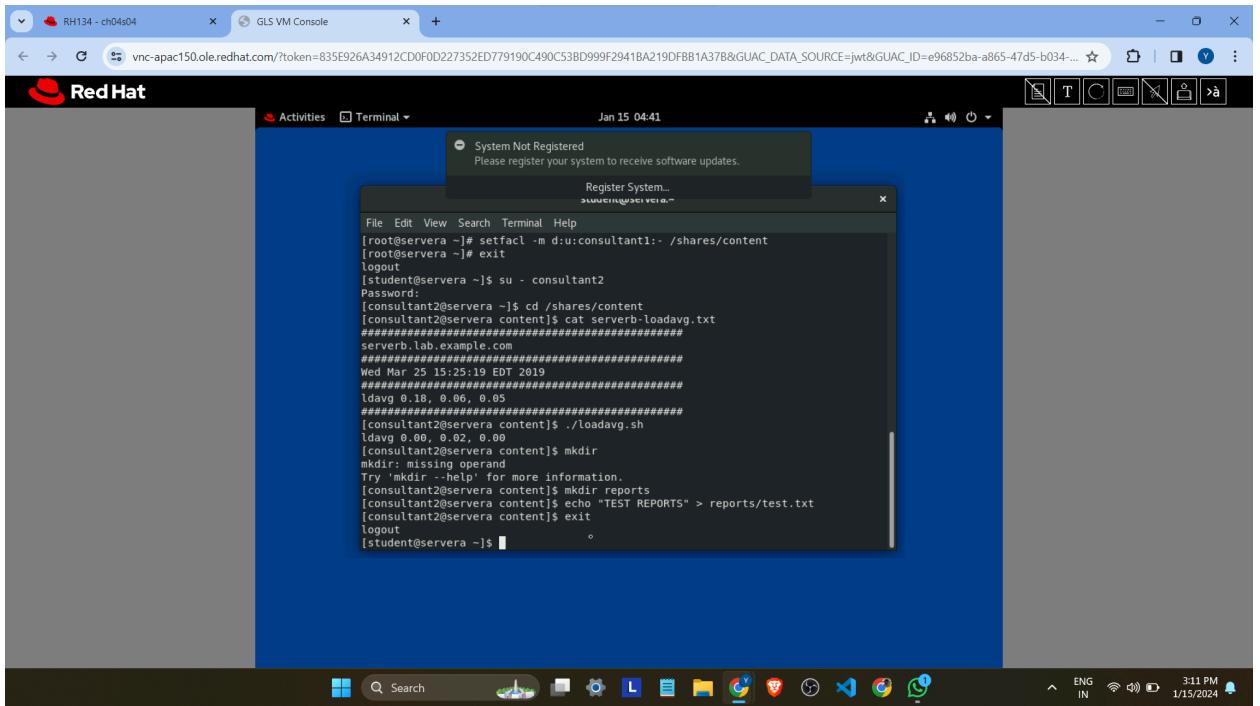
```

RH134 - ch04s04          GLS VM Console
vnc-apac150.ole.redhat.com/?token=835E926A34912CD0F0D227352ED779190C490C53BD999F2941BA219DFBB1A37B&GUAC_DATA_SOURCE=jwt&GUAC_ID=e96852ba-a865-47d5-b034-...
Red Hat
Activities Terminal
System Not Registered
Please register your system to receive software updates.
Register System...
File Edit View Search Terminal Help
Sorry, try again.
[sudo] password for student:
[root@servera ~]# setfacl -Rm g:consultants:rwx /shares/content
[root@servera ~]# setfacl -Rm u:consultant1:- /shares/content
[root@servera ~]# setfacl -m d:g:consultants:rwx /shares/content
[root@servera ~]# setfacl -m d:u:consultant1:- /shares/content
setfacl: Option -m: Invalid argument near character 5
[root@servera ~]# setfacl -m d:u:consultant1:- /shares/content
[root@servera ~]# exit
logout
[student@servera ~]$ su -
Password:
[consultant2@servera ~]$ cd /shares/content
[consultant2@servera content]$ cat serverb-loadavg.txt
#####
serverb.10.example.com
#####
Wed Mar 25 15:25:19 EDT 2019
#####
ldavg 0.18 0.06 0.05
#####
[consultant2@servera content]$ ./loadavg.sh
ldavg 0.00 0.02 0.00
[consultant2@servera content]$ 

```

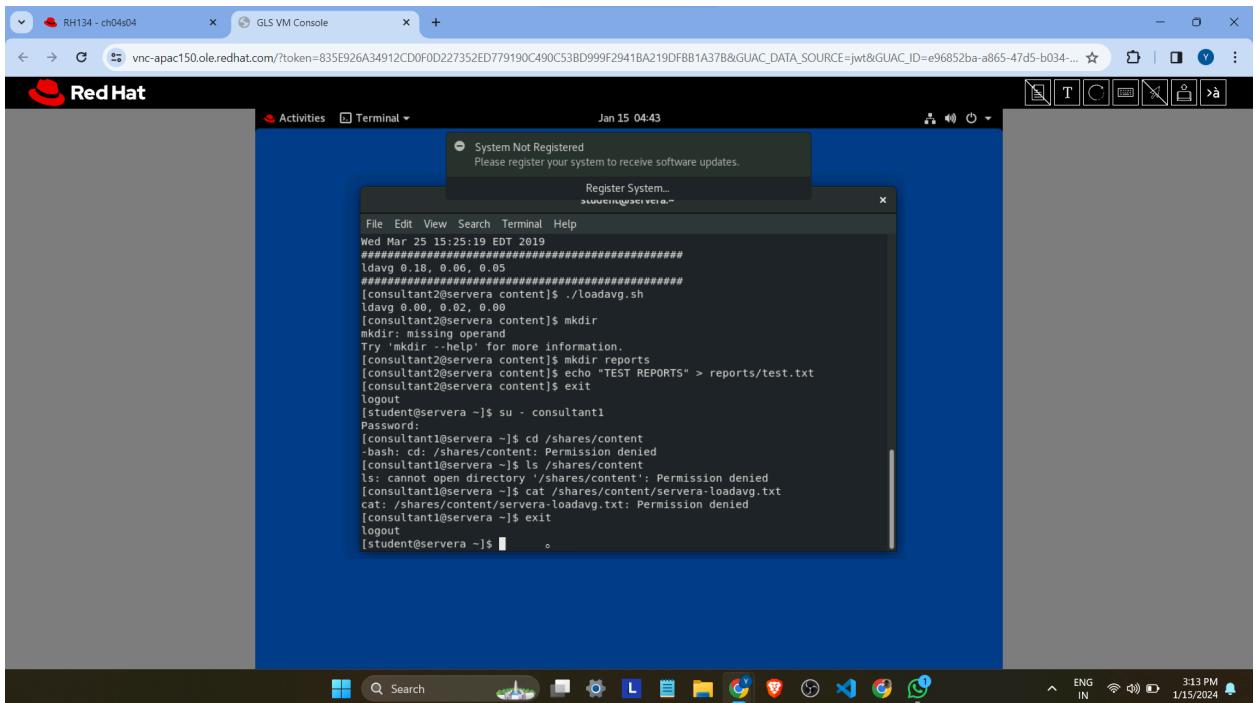
- Now make a new folder inside shared folder “reports” and a file “test.txt” with TEST REPORTS inside the file
Commands: **mkdir reports** to make folder and

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



```
[root@servera ~]# setfacl -m d:u:consultant1: /shares/content
[root@servera ~]# exit
logout
[student@servera ~]$ su - consultant2
Password:
[consultant2@servera ~]$ cd /shares/content
[consultant2@servera content]$ cat servera-loadavg.txt
#####
#####serverb.lab.example.com#####
#####Wed Mar 25 15:25:19 EDT 2019#####
#####ldavg 0.18. 0.06. 0.05#####
#####ldavg 0.00. 0.02. 0.00#####
[consultant2@servera content]$ ./loadavg.sh
ldavg 0.00. 0.02. 0.00
[consultant2@servera content]$ mkdir
mkdir: missing operand
Try `mkdir --help' for more information.
[consultant2@servera content]$ mkdir reports
[consultant2@servera content]$ echo "TEST REPORTS" > reports/test.txt
[consultant2@servera content]$ exit
logout
[student@servera ~]$
```

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



```
Wed Mar 25 15:25:19 EDT 2019
#####
#####ldavg 0.18. 0.06. 0.05#####
[consultant2@servera content]$ ./loadavg.sh
ldavg 0.00. 0.02. 0.00
[consultant2@servera content]$ mkdir
mkdir: missing operand
Try `mkdir --help' for more information.
[consultant2@servera content]$ mkdir reports
[consultant2@servera content]$ echo "TEST REPORTS" > reports/test.txt
[consultant2@servera content]$ exit
logout
[student@servera ~]$ su - consultant1
Password:
[consultant1@servera ~]$ cd /shares/content
-bash: cd: /shares/content: Permission denied
[consultant1@servera ~]$ ls /shares/content
ls: cannot open directory '/shares/content': Permission denied
[consultant1@servera ~]$ cat /shares/content/servera-loadavg.txt
cat: /shares/content/servera-loadavg.txt: Permission denied
[consultant1@servera ~]$ exit
logout
[student@servera ~]$
```

- 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**

The image shows a Red Hat Linux desktop environment with two terminal windows open. Both terminals are running the command `getfacl /shares/content`. The top terminal shows the output for the directory `/shares/content`, which has permissions set for root, operators, and consultants. The bottom terminal shows the output for the directory `/shares/content/reports`, which has permissions set for root, operators, and consultant2.

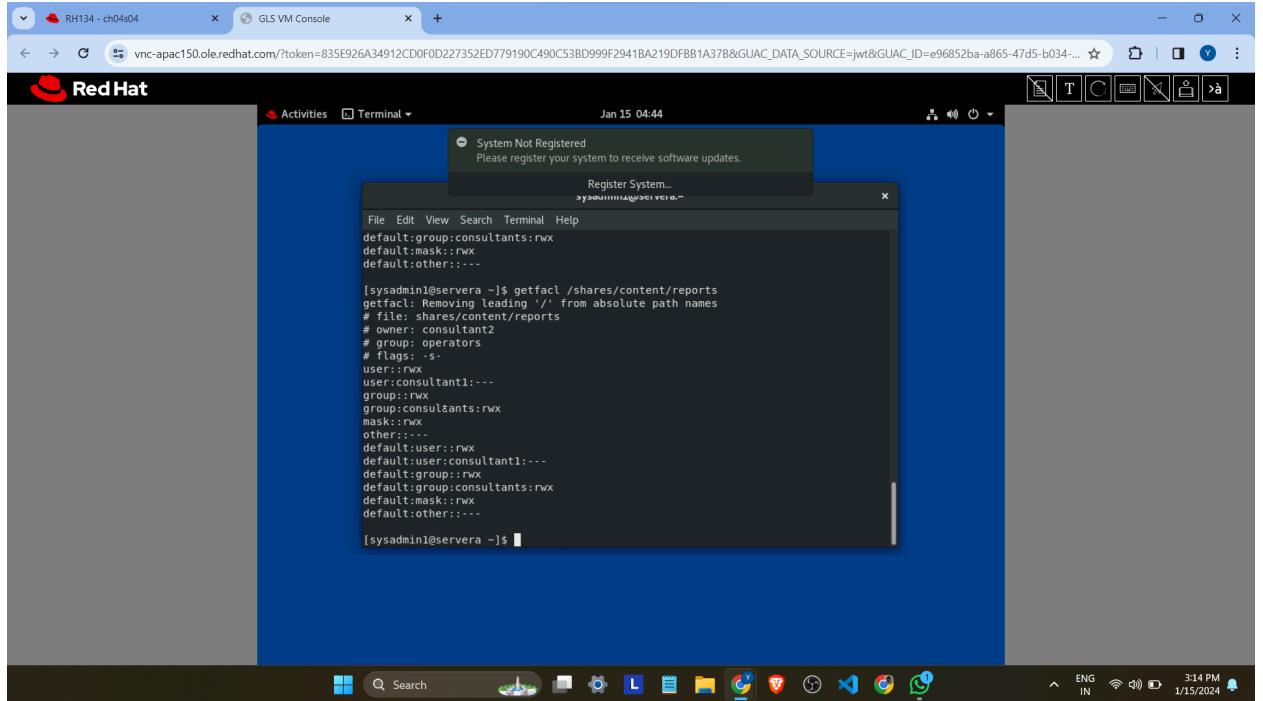
```
[student1@servera ~]$ su - sysadmin1
Password:
[sysadmin1@servera ~]$ getfacl /shares/content
getfacl: Removing leading '/' from absolute path names
# file: shares/content
# owner: root
# group: operators
# flags: -s-
user::rwx
user:consultant1:---
group::rwx
group:consultants:rwx
mask::rwx
other::---
default:user:consultant1:---
default:group:consultants:rwx
default:mask::rwx
default:other:---

[sysadmin1@servera ~]$
```



```
[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:consultants:rwx
mask::rwx
other::---
default:user:consultant1:---
default:group::rwx
default:group:consultants:rwx
default:mask::rwx
default:other:---
```

- 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

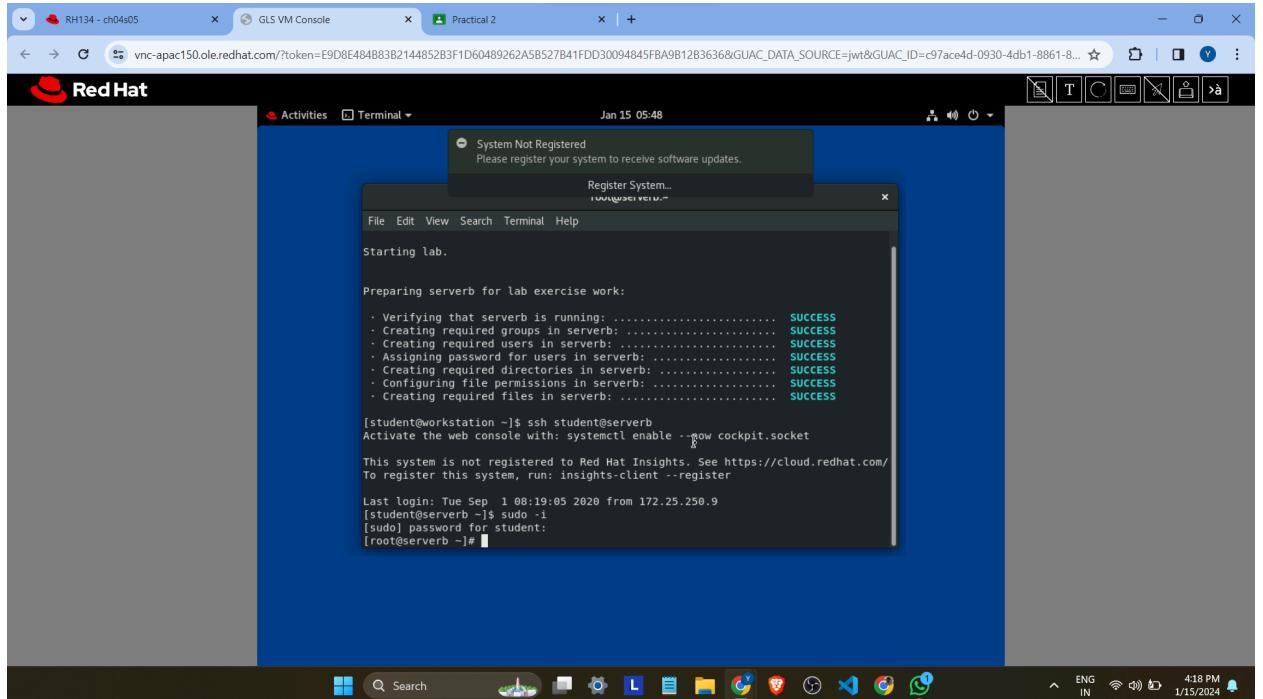
templates files. Because manager1 has been too busy, it falls to you to finish the job. Your task is to complete the setup of the share

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**

```

System Not Registered
Please register your system to receive software updates.

Register System...
TUTORIALS.RHCE.COM

File Edit View Search Terminal Help
Starting lab.

Preparing serverb for lab exercise work:
- Verifying that serverb is running: SUCCESS
- Creating required groups in serverb: SUCCESS
- Creating required users in serverb: SUCCESS
- Assigning password for users in serverb: SUCCESS
- Creating required directories in serverb: SUCCESS
- Configuring file permissions in serverb: SUCCESS
- Creating required files in serverb: SUCCESS

[student@workstation ~]$ ssh student@serverb
Activate the web console with: systemctl enable --now cockpit.socket
This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register
Last login: Tue Sep  1 08:19:05 2020 from 172.25.250.9
[student@serverb ~]$ sudo -i
[sudo] password for student:
[root@serverb ~]#

```

- 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 CONTRACTORS

```

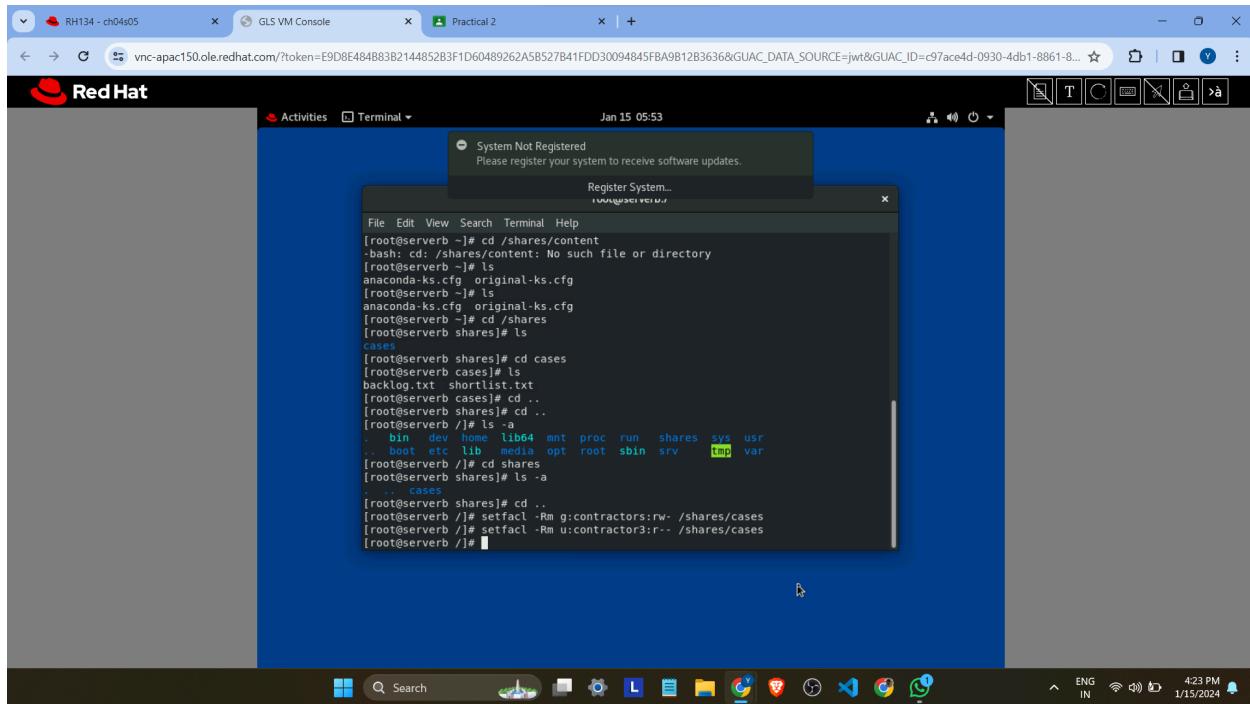
System Not Registered
Please register your system to receive software updates.

Register System...
TUTORIALS.RHCE.COM

File Edit View Search Terminal Help
[root@serverb ~]# cd /shares/content
[bash]: cd: /shares/content: No such file or directory
[root@serverb ~]# ls
anaconda-ks.cfg original-ks.cfg
[root@serverb ~]# cd ..
[root@serverb ~]# ls
anaconda-ks.cfg original-ks.cfg
[root@serverb ~]# cd /shares
[root@serverb shares]# ls
cases
[root@serverb shares]# cd cases
[root@serverb cases]# ls
backlog.txt shortlist.txt
[root@serverb cases]# cd ..
[root@serverb shares]# cd ..
[root@serverb ~]# ls -a
. bin dev home lib64 mnt proc run shares sys usr
.. boot etc lib media opt root sbin srv tmp var
[root@serverb ~]# cd shares
[root@serverb shares]# ls -a
cases
[root@serverb shares]# cd ..
[root@serverb ~]# setfacl -Rm g:contractors:rwx /shares/cases
[root@serverb ~]# setfacl -Rm u:contractor3:r-- /shares/cases
[root@serverb ~]#

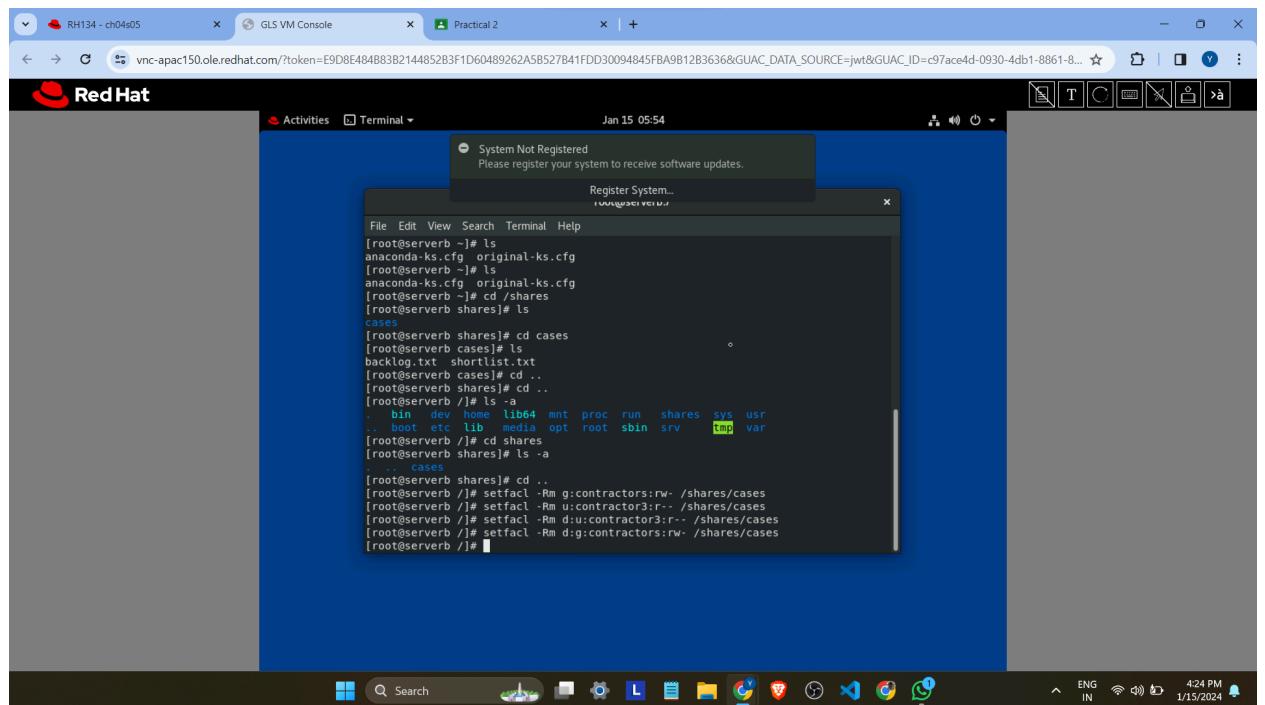
```

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



```
[root@serverb ~]# cd /shares/content
[bash: cd: /shares/content: No such file or directory]
[root@serverb ~]# ls
anaconda-ks.cfg original-ks.cfg
[root@serverb ~]# ls
anaconda-ks.cfg original-ks.cfg
[root@serverb ~]# cd /shares
[root@serverb shares]# ls
cases
[root@serverb shares]# cd cases
[root@serverb cases]# ls
backlog.txt shortlist.txt
[root@serverb cases]# cd ..
[root@serverb shares]# cd ..
[root@serverb /]# ls -a
. bin dev home lib64 mnt proc run shares sys usr
.. boot etc lib media opt root sbin srv tmp var
[root@serverb /]# cd shares
[root@serverb shares]# ls -a
.
[root@serverb shares]# cd ..
[root@serverb /]# setfacl -Rm g:contractors:r- /shares/cases
[root@serverb /]# setfacl -Rm u:contractor3:r- /shares/cases
[root@serverb /]#
```

- 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



```
[root@serverb ~]# ls
anaconda-ks.cfg original-ks.cfg
[root@serverb ~]# ls
anaconda-ks.cfg original-ks.cfg
[root@serverb ~]# cd /shares
[root@serverb shares]# ls
cases
[root@serverb shares]# cd cases
[root@serverb cases]# ls
backlog.txt shortlist.txt
[root@serverb cases]# cd ..
[root@serverb shares]# cd ..
[root@serverb /]# ls -a
. bin dev home lib64 mnt proc run shares sys usr
.. boot etc lib media opt root sbin srv tmp var
[root@serverb /]# cd shares
[root@serverb shares]# ls -a
.
[root@serverb shares]# cd ..
[root@serverb /]# setfacl -Rm g:contractors:r- /shares/cases
[root@serverb /]# setfacl -Rm u:contractor3:r- /shares/cases
[root@serverb /]# setfacl -Rm d:u:contractor3:r- /shares/cases
[root@serverb /]# setfacl -Rm d:g:contractors:rw- /shares/cases
[root@serverb /]#
```

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

```

System Not Registered
Please register your system to receive software updates.

Register System...
CONTRACTOR3@SERVERB ~

File Edit View Search Terminal Help
[root@serverb ~]# cd shares
[root@serverb shares]# ls -a
. . cases
[root@serverb shares]# cd ..
[root@serverb ~]# setfacl -Rm g:contractors:r-- /shares/cases
[root@serverb ~]# setfacl -Rm u:contractor3:r-- /shares/cases
[root@serverb ~]# setfacl -Rm d:u:contractor3:r-- /shares/cases
[root@serverb ~]# setfacl -Rm dg:contractors:r-- /shares/cases
[root@serverb ~]# exit
logout
[student@serverb ~]$ su - contractor3
Password:
su: Authentication failure
[student@serverb ~]$ su - contractor3
Password:
Last failed login: Mon Jan 15 05:55:43 EST 2024 on pts/0
There was 1 failed login attempt since the last successful login.
[contractor3@serverb ~]$ cd /shares/cases
-bash: cd: /shares/cases: Permission denied
[contractor3@serverb ~]$ ls /shares/cases
ls: cannot access '/shares/cases/shortlist.txt': Permission denied
ls: cannot access '/shares/cases/backlog.txt': Permission denied
backlog.txt shortlist.txt
[contractor3@serverb ~]$ 

```

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

```

logout
[student@serverb ~]$ su - manager1
Password:
Last login: Mon Jan 15 06:04:58 EST 2024 on pts/0
[manager1@serverb ~]$ cd /shares/cases
[manager1@serverb cases]$ ls
backlog.txt shortlist.txt
[manager1@serverb cases]$ cat backlog.txt
###Backlog of Clients to call###TEMPLATE###
[manager1@serverb cases]$ 

```