File permissions in Linux

Project description

The research team at my Organization was given an assignment to update the file permissions for some files and directories within a directory called PROJECTS.
A careful study of the permissions revealed that there were some differences in the permissions and it does not reflect the proper level of authorization that should be given to different users.
I had to update these permissions by using different Linux commands.

Check file and directory details

In carrying out this task, I had to first investigate the current permissions of specific directories. To accomplish this I had to use different Linux commands.

```
researcher2@f81609b1a2d1:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 31 11:50 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 31 13:13 ..
-rw--w---- 1 researcher2 research_team   46 Aug 31 11:50 .project_x.t
xt
drwx--x--- 2 researcher2 research_team 4096 Aug 31 11:50 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Aug 31 11:50 project_k.tx
t
-rw-r----- 1 researcher2 research_team   46 Aug 31 11:50 project_m.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Aug 31 11:50 project_r.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Aug 31 11:50 project_t.tx
t
researcher2@f81609b1a2d1:~/projects$
```

I entered the Linux command ls -la and this gave me an output of the different levels of permissions of all director and the different files in it.
The output of my command also showed that i had a hidden file with the name .projects_x.txt and five other files.

Describe the permissions string

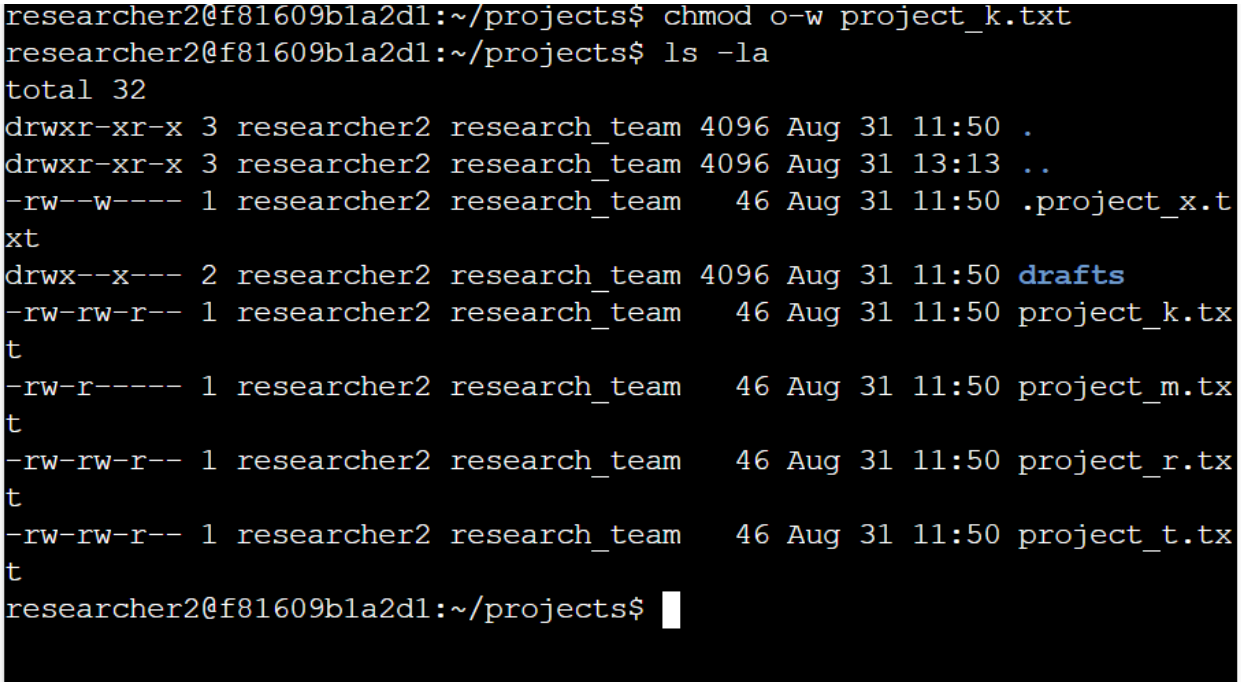
Displayed as permissions in my code are 10 character strings which describe the level of permissions each user, group and execute has.

- 1st character: This is either character d or a hyphen (-) and it shows the file type. It shows it is a directory if it's a d, and a regular file if it's a hyphen (-).
- The 2nd to the 4th characters which is rwx stands for read, write and execute. These are permissions that are granted to the users. If any of these permissions is a hyphen(-) this means that that particular permission is not given to the user, and access is denied.
- The 5th to the 7th characters which also are rwx (read,write,execute) are permissions granted to the group.If any of these permissions is a hyphen(-) this means that that particular permission is not given to the user, and access is denied.
- The 8th to the 10th characters which also are rwx (read,write,execute) are permissions granted to all other users on the system apart from users and groups..If any of these permissions is a hyphen(-) this means that that particular permission is not given to the user, and access is denied.

  An example from our project_t.txt shows the characters -rw-rw-r—,this is telling us that it is a file and not a directory and also that the users, groups and others have read permissions into this file.While the users and group have write permissions, the others do not. From the permissions assigned we can see no one has execute permissions into this file.

Change file permissions

The Organization decided that others should not have permission to write into any of their files because of the sensitivity of these files. So I went back to the file permissions I recently used which is the ls -la command and I saw that the file project_k.txt must have the access to write to the file removed.
I used the change mode command to remove the permissions from the others.

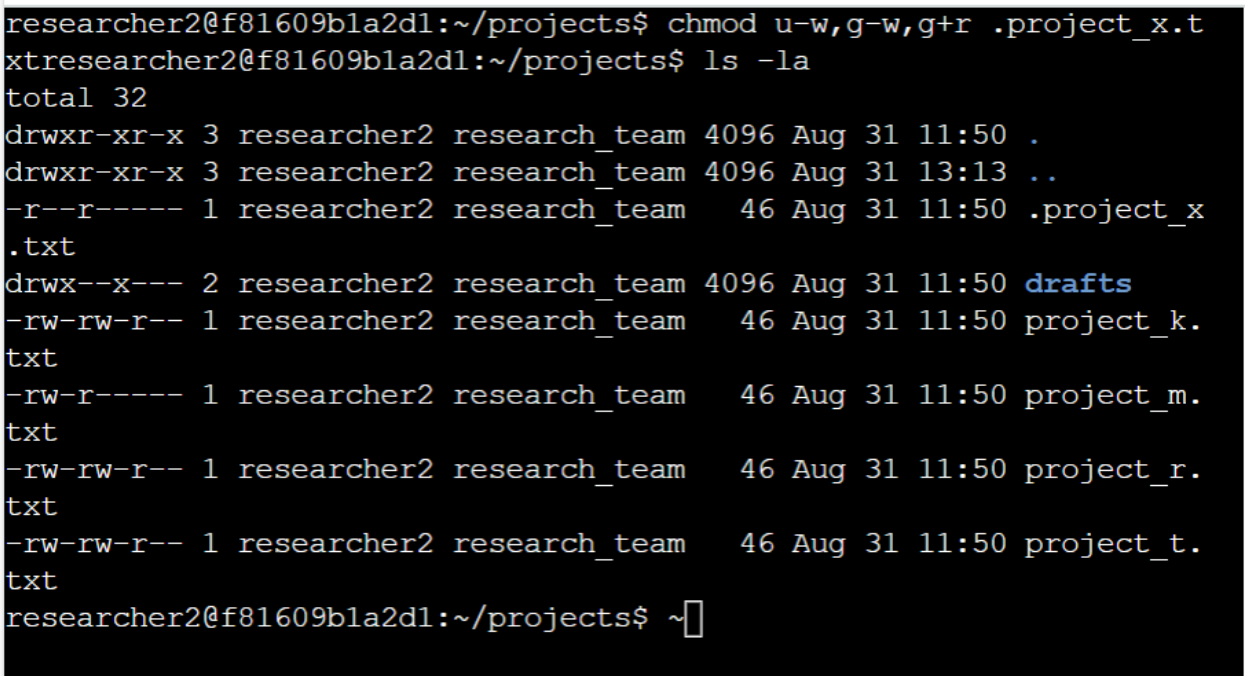


Chmod o-w project_k.txt.

The chmod command the permission on the files and the directory. The first argument indicates what permissions should be changed, and the second argument specifies the file or directory. After this I then used the ls -la to confirm that the write permission has been removed from others.

Change file permissions on a hidden file

The research team after some modifications on a file project_x.txt decided to archive this file. They don't want anyone to have write access into this file, but the user and the group should have only read access.
I used this linux command to change the permissions. Chmod u-w,g-w,g+r .project_x.txt.



The file is a hidden file because it started with a period(.). So from this we can see that I removed the write permission from the user and the group then added the read permission to the group.

Change directory permissions

My Organization also wanted the drafts directory and its content to be only accessed by the researcher2 user. This means that only researcher2 should have execute permissions.
I used the g-x drafts to remove the group having execute permissions.

```
researcher2@f81609b1a2d1:~/projects$ chmod g-x drafts
researcher2@f81609b1a2d1:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 31 11:50 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 31 13:13 ..
-r--r----- 1 researcher2 research_team   46 Aug 31 11:50 .project_x
.txt
drwx------ 2 researcher2 research_team 4096 Aug 31 11:50 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Aug 31 11:50 project_k.
txt
-rw-r----- 1 researcher2 research_team   46 Aug 31 11:50 project_m.
txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 31 11:50 project_r.
txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 31 11:50 project_t.
txt
researcher2@f81609b1a2d1:~/projects$
```

Summary

I was able to use the linux command to determine the level of access that users, groups and others were given to be able to gain access into directories and files. Also after consulting with my Organization and finding out they wanted some permissions to be changed I was also able to use other linux commands to change the permissions to the different levels required.