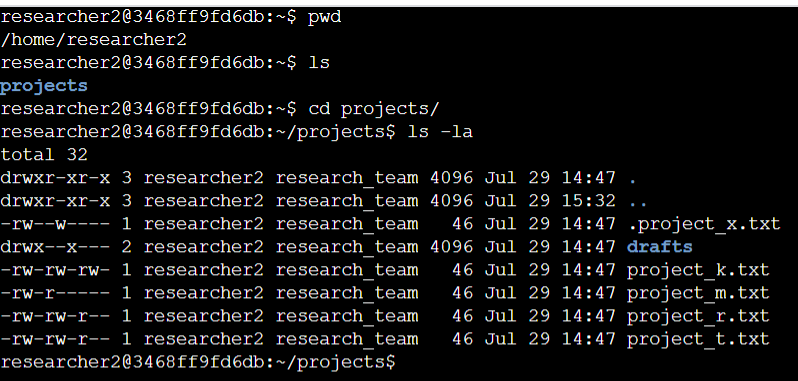
# File permissions in Linux

## Project description

I have been tasked with examining and changing permissions at my organization within the “projects” directory. They currently do not reflect the correct levels of authorization and to ensure a secure system, the following tasks were performed:

## Check file and directory details

Firstly, I check to see which directory I’m currently in with the “pwd” command. Next, I navigate to the correct directory with the “cd projects” command. Once in the correct directory, I used the “ls -la” command to check the permissions of the files, including hidden files such as “.project\_x.txt” and a directory “drafts”.



## Describe the permissions string

The 10-character string in the front determine who is authorized to access the

file and their specific permissions. The breakdown of the characters is as follows:

● 1st character: This character is either a d or hyphen (-) and indicates the file type. If it’s

a d, it’s a directory. If it’s a hyphen (-), it’s a regular file.

● 2nd-4th characters: These characters indicate the read (r), write (w), and execute (x)

permissions for the user. When one of these characters is a hyphen (-) instead, it

indicates that this permission is not granted to the user.

● 5th-7th characters: These characters indicate the read (r), write (w), and execute (x)

permissions for the group. When one of these characters is a hyphen (-) instead, it

indicates that this permission is not granted for the group.

● 8th-10th characters: These characters indicate the read (r), write (w), and execute (x)

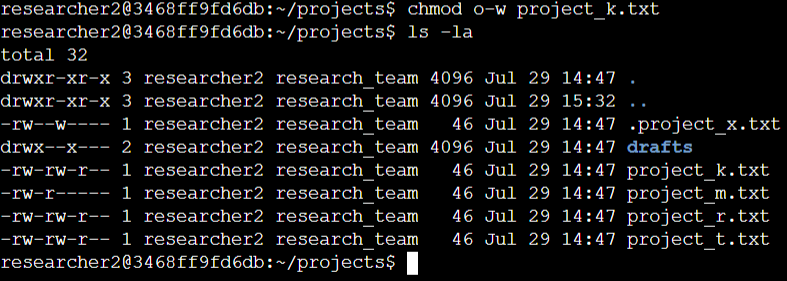
permissions for other. This owner type consists of all other users on the system apart

from the user and the group. When one of these characters is a hyphen (-) instead,

that indicates that this permission is not granted for other.

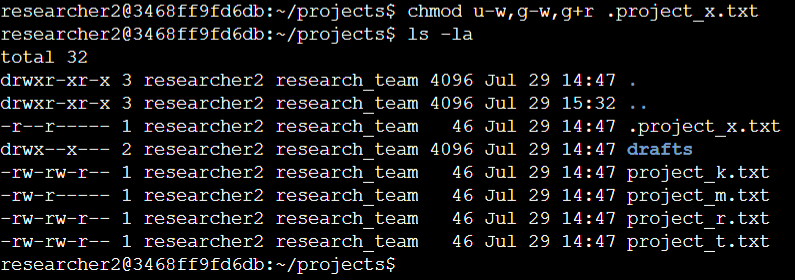
## Change file permissions

The organization had determined that “other” does not have access to write any files. To comply with this. I used the following commands to change the permissions. The first line I used “chmod o-w project\_k.txt” to remove the permission of other to write. Since it was the only one that needed to be changed, I just needed “o-w” for that file. The next line, I used “ls -la” to confirm that the permissions have been changed.



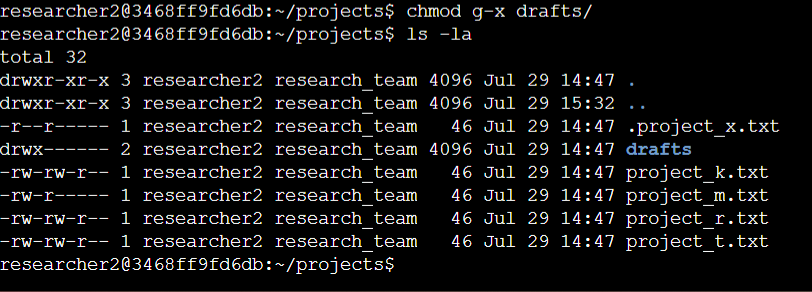
## Change file permissions on a hidden file

The file “.project\_x.txt” is a hidden file because it has been archived. For this reason, the organization has determined that no one should have access to write in that file, but the user and group are able to read the file only. To comply with this I use the following commands below to change the permissions and “ls -la” to confirm once again that the changes have taken effect. I used “u-w” and “g-w” to remove the write permission for user and group. I then used “g+r” to grant the group permission to read the file.



## Change directory permissions

Since the files and directories belong to “researcher2”, Only “researcher2” should be allowed to access the “drafts” directory and its contents. The following commands are to change access to the “drafts” directory to only the user.



The output shows confirmation that the commands worked and only the user has access to read, write, and execute the “drafts” directory. With use of the “chmod” and “ls -la” command, we were able to achieve this.

## Summary

After locating where I was in the system and navigating to the correct directory, I used the “chmod” multiple times to change permissions to the correct level of authorization deemed by my organization. Also, using the “ls -la” command was integral to examine and confirm the changes that were made.