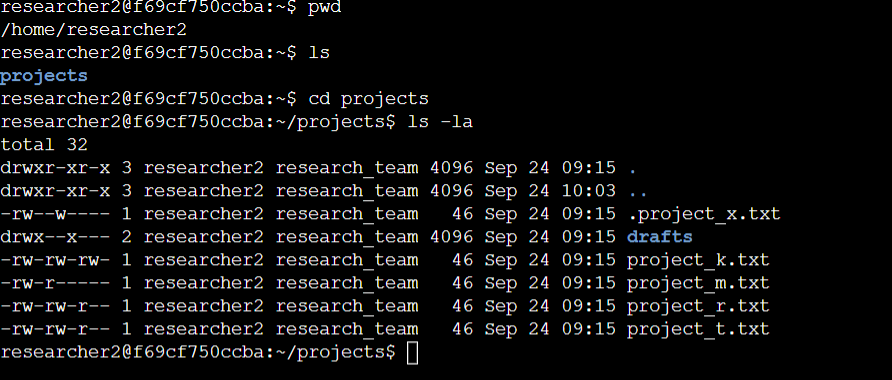
# File permissions in Linux

## Project description

To examine existing permissions on the file system and to determine if the permissions match the authorization that should be given. If they do not match, I will need to modify the permissions to authorize the appropriate users and remove any unauthorized access. The permissions do not currently reflect the level of authorization that should be given. Checking and updating these permissions will help keep their system secure. To complete this task, I performed the following tasks.

## Check file and directory details



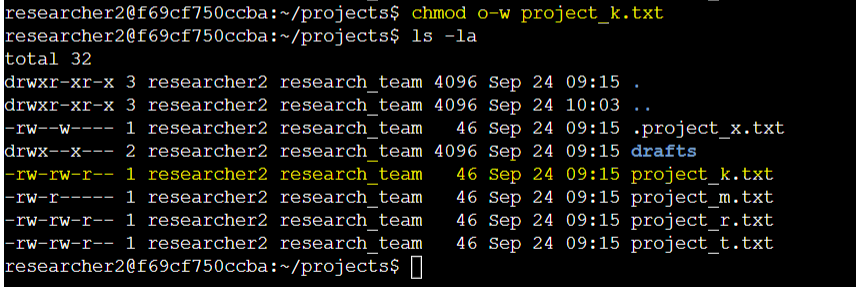
## Describe the permissions string

  
Here, d represents that it is a directory with the following permissions mentioned below,  
User - read, write and execute   
Group - execute   
Other - no permission  
The 10-character string can be deconstructed to determine who is authorized to access the file and their specific permissions. The characters and what they represent are 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.

For example, the file permissions for project\_t.txt are -rw-rw-r--. Since the first character is a hyphen (-), this indicates that project\_t.txt is a file, not a directory. The second, fifth, and eighth characters are all r, which indicates that user, group, and other all have read permissions. The third and sixth characters are w, which indicates that only the user and group have write permissions. No one has execute permissions for project\_t.txt.

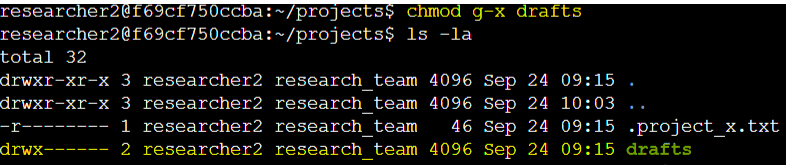
## Change file permissions

  
Write permission for Other group is removed from project\_k.txt

## Change file permissions on a hidden file

  
The research team has archived **.project\_x.txt**, which is why it’s a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file.

## Change directory permissions

  
Only **researcher2** should be allowed to access the **drafts** directory and its contents.

## Summary

I changed multiple permissions to match the level of authorization my organization wanted for

files and directories in the projects directory. The first step in this was using ls -la to

check the permissions for the directory. This informed my decisions in the following steps. I

then used the chmod command multiple times to change the permissions on files and

directories.