# File permissions in Linux

## Project description

The research team at my organization needs to examine the existing permissions in the file system. The team needs to determine if the permissions match the authorizations that are granted. Since the system does not reflect true authorizations, permissions will need to be modified to authorize appropriate users and remove access to unauthorized users.

## Check file and directory details

Navigate to the projects directory using the **command ‘cd projects’**. Next list contents and permissions of the projects directory using the **command ‘ls -l’**.

## Describe the permissions string

1. drw-rw-rw- (project k)
2. -rw-r----- (project m)
3. -rw-rw-r-- (project r)
4. -rw-rw-r-- (project t)
5. -rw--w---- (project x)
6. -rwx--x--- (drafts)

* The 1st character indicates the file type. The d indicates it’s a directory. When this character is a hyphen (-), it's a regular file.
* The 2nd-4th 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.
* The 5th-7th 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.
* The 8th-10th characters indicate the read (r), write (w), and execute (x) permissions for the owner type of 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

* None of the files should allow the other users to write to files. **project\_k.txt** allows other users to write to files. Check to see if any files in the projects directory have write permissions to the owner type of other using **command ‘ls -l’**. Change the permissions of the file using the **command ‘chmod o-w project\_k.txt’**.
* Project\_m.txt is a restricted file and should not be readable or writable by the group or other. Only the user should have these permissions on this file. List contents and permissions of the current directory and check if the group has read or write permissions using **command ‘ls -l’**. Change permissions to read only using command **‘chmod g-r project\_m.txt’.**

## Change file permissions on a hidden file

File **.project\_x.txt** is a hidden file that has been archived and should not be written to anyone. The user and group owner types have incorrect write permissions in which they should only have read permissions but not write to permissions. Check permissions of the hidden file using **command ‘ls -la’**. Change permissions of the file using **command ‘chmod u-w, g-w, g+r .project\_x.txt’**.

## Change directory permissions

**Researcher2** should only be allowed to access the drafts directory and its contents. Check the permissions of the drafts directory using **command ‘ls -l’**. The group user has execute permissions and therefore has access to the drafts directory. Remove the execute permission for the group from the drafts directory using the command **‘chmod g-x drafts’**.

## Summary

Using the Linux Bash shell, permissions to files and directories were checked and modified using Linux commands. I ensured to match the level of authorization the organization wanted for files and directories in the projects directory. Using the **command ‘ls -ls’** I checked the permissions for the directory and using the **command ‘chmod’** I changed the permissions on files and directories.