# File permissions in Linux

## Project description

## Through Linux commands, I examine and modify file system permissions to ensure that users on the research team have the appropriate authorization and remove any unauthorized access.

## Check file and directory details.

## Describe the permissions string.

## 1st character: Indicates the file type. "d" signifies a directory, while a hyphen "-" indicates a regular file.

## 2nd-4th characters: Represent read (r), write (w), and execute (x) permissions for the user. A hyphen (-) indicates the absence of that permission for the user.

## 5th-7th characters: Represent read (r), write (w), and execute (x) permissions for the group. A hyphen (-) indicates the absence of that permission for the group.

## 8th-10th characters: Represent read (r), write (w), and execute (x) permissions for others (users on the system apart from the owner and group). A hyphen (-) indicates the absence of that permission for others.

## Change file permissions.

## In the chmod command, u sets the permissions for the user who owns the file, g sets the permissions for the group that owns the file, and o sets the permissions for others.

## Change file permissions on a hidden file.

## The -l denotes the list of properties along with the permissions, while the -a denotes the visibility of hidden files.

## Change directory permissions.

## Each MODE is of the form '[ugoa]\*([-+=]([rwxXst]\*|[ugo]))+|[-+=][0-7]+'.

## Summary

In the given tasks, I modified file and directory permissions using the chmod command. I removed execute permission for the group from the "drafts" directory, adjusted permissions for ".project\_x.txt" to allow read access for the user and group while restricting write permissions, and restricted both read and write permissions for the group on "project\_m.txt". Additionally, I further restricted write permissions for the owner type of others on "project\_m.txt". Lastly, I explored the permissions of the "projects" directory and its contents using the ls -l command, ensuring proper access control in the specified Linux environment.