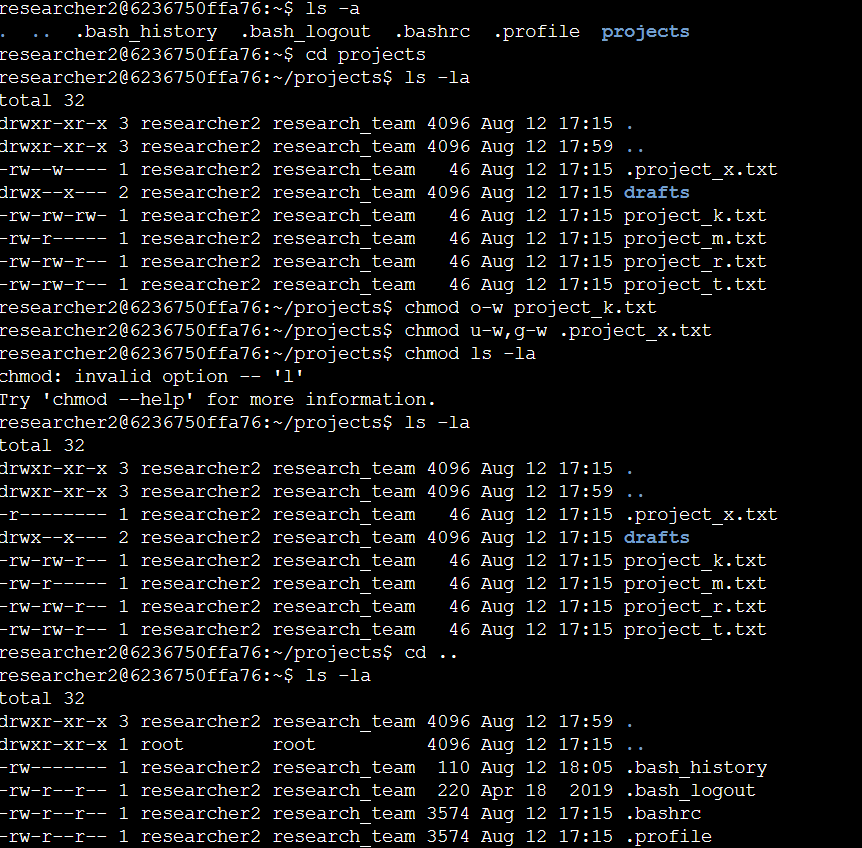
# File permissions in Linux

## Project description

In this sample organization’s files, I was tasked to change the permissions of certain text files to align with the organization’s wishes. This included removing and adding permissions from directories and files.

## File and directory details

ls -la was used to view the projects directory, its hidden files, and all file permissions.

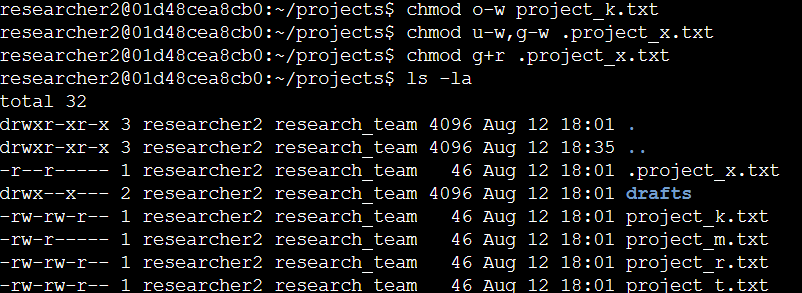


## Describe the permissions string

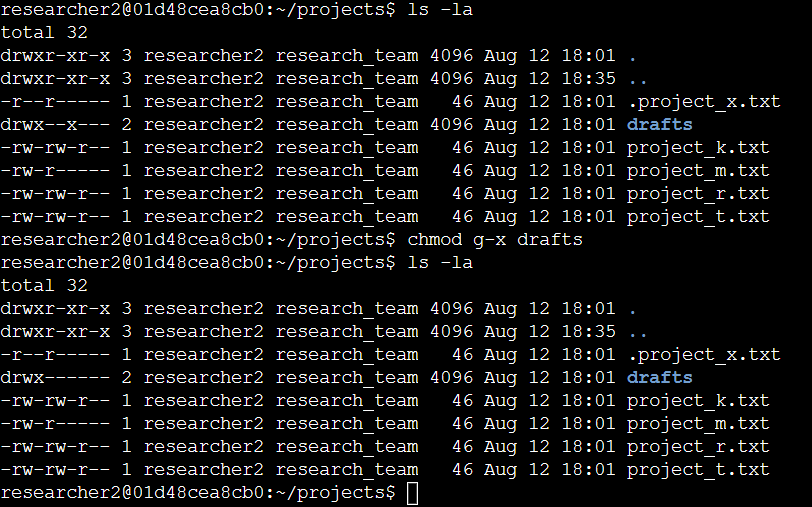
The first character of the permissions string indicates whether the subject is a directory or not, hence the ‘d’. The next three groups of three indicate the permissions for the user, group, and others. The first character r, dictates read permissions, the second w, write permissions, and the final x, execute permissions.

## Change file permissions and hidden file permissions

In this example, the organization required that no file gave others the permission to write. The chmod command was used to remove those permissions from the only file that gave other write permissions, project\_k.txt. The organization also archived .project\_x.txt, which is why it was hidden. This project was meant to give no party write permissions, but give the user and group read permissions. The chmod command was used twice more to remove and grant these permission changes.



## Change directory permissions



In this case, only the user, researcher2 was made to have permissions to the directory drafts, as it belonged to them. The chmod command was used to remove the permissions of group and other while maintaining the permissions of the user, researcher2.

## Summary

To begin, all files in the projects directory were made to refuse write permissions to the other category. Next, the file .project\_x.txt was hidden because it was archived. Since it was archived, the file was made to refuse all write permissions, but allowed the user and group to read it. Finally, the drafts directory was made to be accessible only to the user who it belonged to, researcher2.