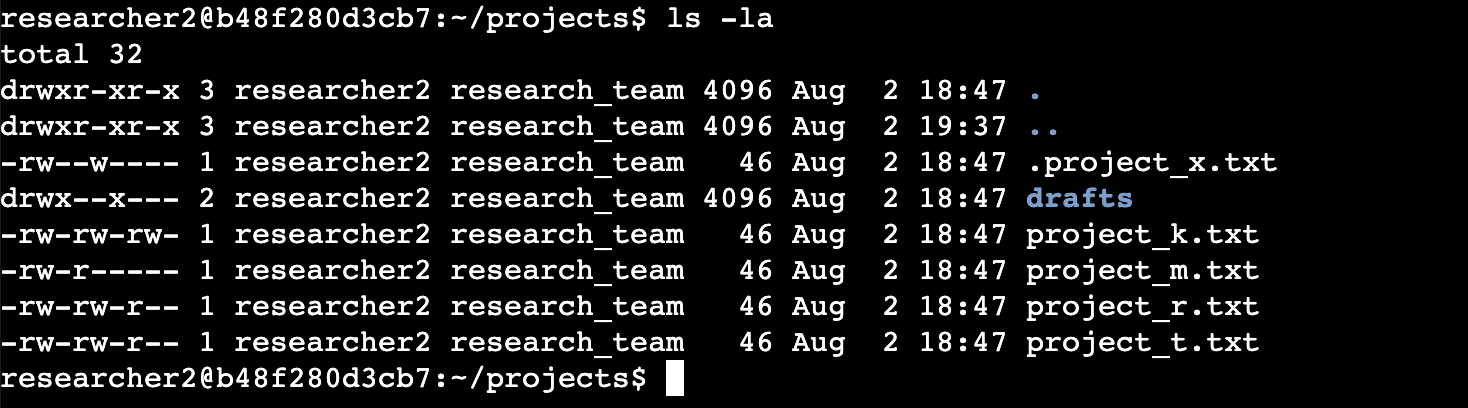
# File permissions in Linux

## Project description

The research team needs to update the file permissions of certain files and directories within the “projects” directory. To complete this, I performed the following:

## Check file and directory details

Determine current permissions in the directory.



## Describe the permission string

## The 10-character string represents the file permissions for a file or directory in Linux. Each character in the string corresponds to a specific permission category:

## **1st Character:** This character is either a "d" or a hyphen ("-"). A "d" indicates that the entry is a directory, while a hyphen ("-") signifies a regular file.

## **2nd-4th Characters:** These characters represent the permissions for the user (owner) of the file. The first character can be "r" for read access, "w" for write access, or a hyphen ("-") if the permission is not granted. The second character represents the group's permissions, and the third character represents others' permissions.

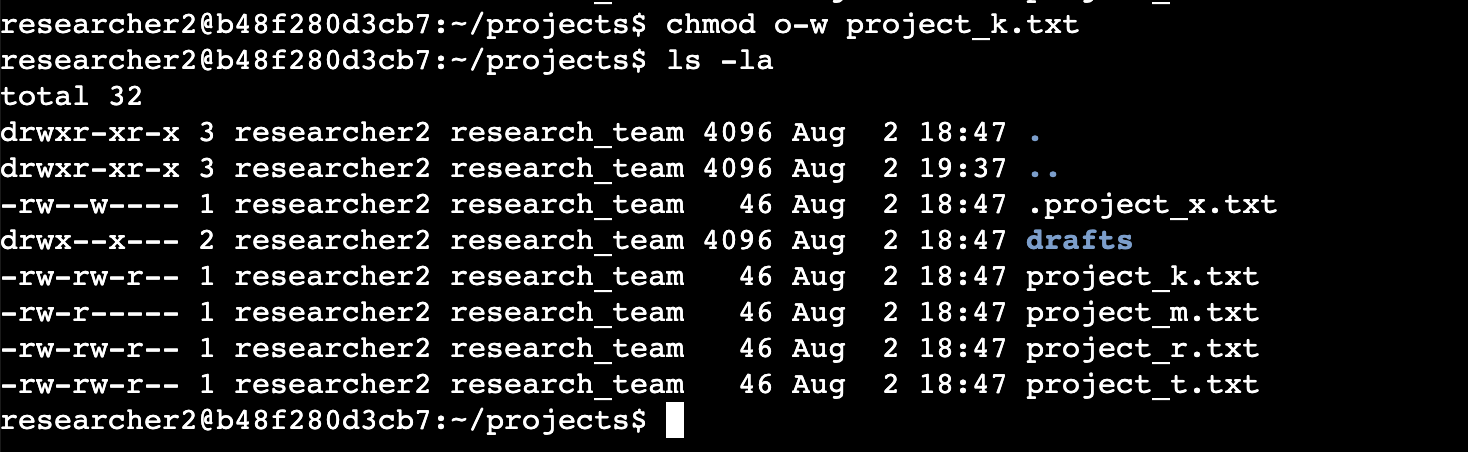
## **5th-7th Characters:** These characters represent the permissions for the group that the file belongs to, in the same manner as the user permissions. The first character represents the group's read access, the second character represents write access, and the third character represents execute access.

## **8th-10th Characters:** These characters indicate the permissions for all other users on the system (excluding the user and the group). The first character represents read access, the second character represents write access, and the third character represents execute access.

## For example, a permissions string like "-rw-rw-r--" indicates that it is a regular file, the user has read and write permissions, the group has read and write permissions, the group has read and write permissions, and others have only read permission.

## Change file permissions

The organization does not allow other to have write access to any files. So we need to change that.



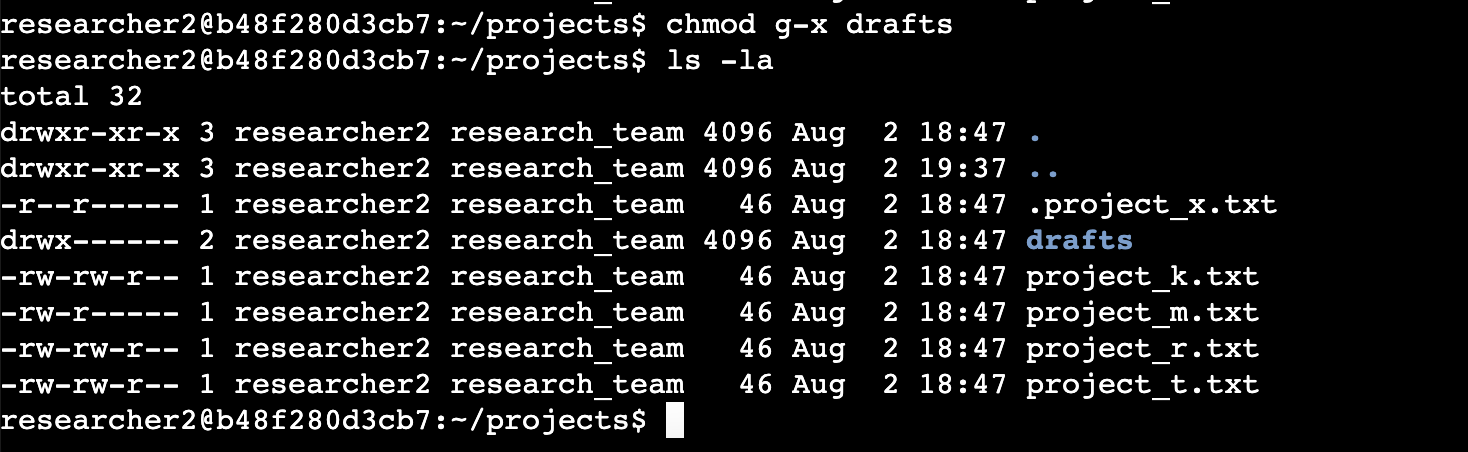
## Change file permissions on a hidden file

## 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

The files and directories in the projects directory belong to the researcher2 user. 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.