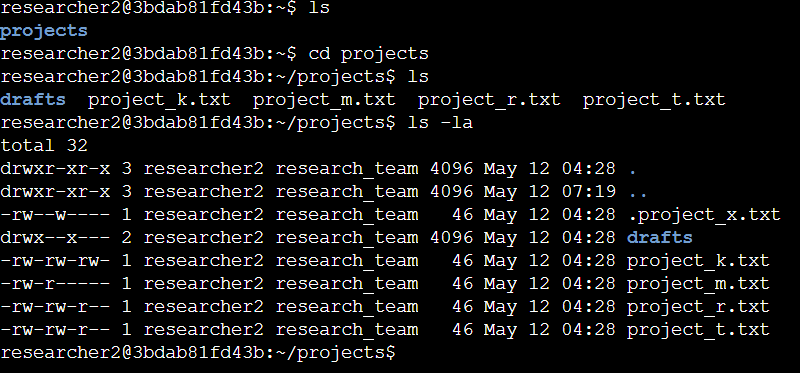
# File permissions in Linux

## Project description

The research team at my organisation needs to update the files permissions for certain files and directories within the “projects” directory.The permissions do not currently reflect the level of authorization that should be give.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

I used the command line “ls” to check and list the contents of the directory I am currently in then I proceeded to use “cd projects” so that I could enter the “projects” directory. I then used “ls” to check the “projects” subdirectories. Then I used “ls -la” command so that i could determine all the existing permissions including all the hidden files permissions.

## Describe the permissions string

The 10-character string can be deconstructed to determine who is authorized to access the

le 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 others. 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

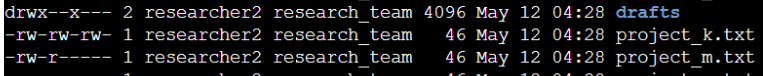
indicates that this permission is not granted for others.

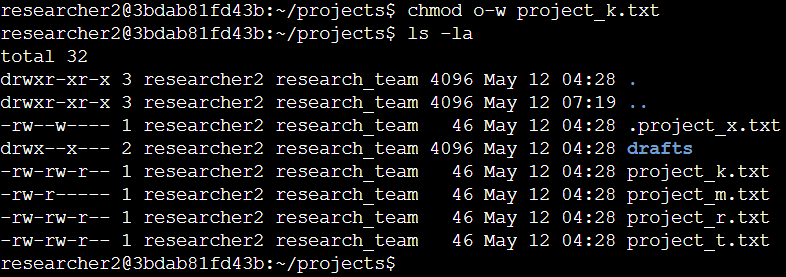
For example, the

le permissions for project\_t.txt are -rw-rw-r--. Since the first character is a hyphen (-), this indicates that project\_t.txt is a le, not a directory. The second, h, 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 executed permissions for project\_t.txt.

## Change file permissions

The organization determined that other (o) shouldn't have write access to any of their files. To comply with this, I referred to the file permissions that I previously returned. I determined project\_k.txt must have the write access removed for other.

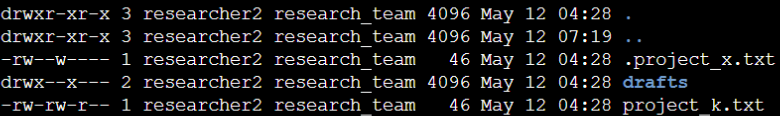




In the second screenshot I used the chmod command to change the permissions on files and directories. The first argument (o-w) indicates what permissions should be changed, and the second argument (project\_k.txt)specifies the file or directory.I removed write permissions from other for the project\_k.txt file. After this, I used ls -la to review the updates I made, and it show that the write permission was removed.

## Change file permissions on a hidden file

The research team at my organization archived project\_x.txt. They do not want anyone to have write(w) access to this project, but the user(u) and group(g) should have read(r) access.



I know .project\_x.txt is a hidden file because it starts with a period (.). The second screenshot shows that I removed write(w) permissions from the user(u) with with u-w and then I removed write permissions from the group group(g) with g-w, and added read(r) permissions to the group(g) with g+r.



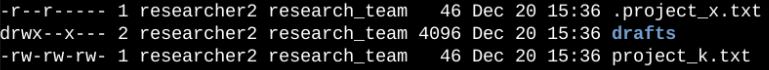
(continue to next page)

## 

## Change directory permissions

My organization only wants the researcher2 user to have access to the drafts directory and its contents. This means that no one other than researcher2 should have execute permissions.





The second screenshot shows the permission listing for the different files and directories. Line 1 indicates the current directory (projects[indicated by . ]), and line 2 indicates the parent directory (home[indicated by .. ]). Line 3 indicates a regular file titled .project\_x.txt. Line 4 is the directory (drafts) with restricted permissions. Here you can see that only researcher2 has execute permissions. It was previously determined that the group had execute permissions, so I used the chmod command to remove them. The researcher2 user already had execute permissions, so they did not need to be added.

## 

## 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.