

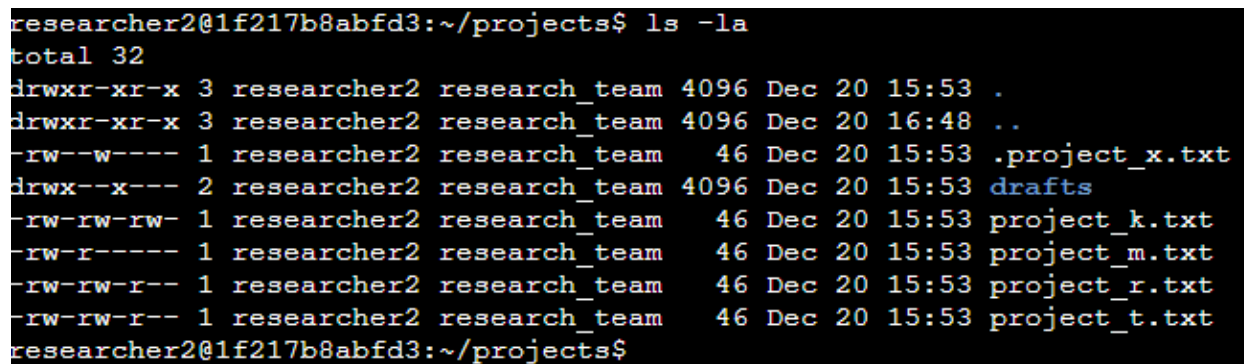
# File permissions in Linux

## Project description

My organization has set a goal to display and adjust all access rights for certain groups and users, in order to maintain security and reduce the risks associated with the leakage of certain information, using Linkus commands I perform actions that correct these access rights:

## Check file and directory details

In this image we can see what commands I used to identify permissions on certain files:



```
researcher2@1f217b8abfd3:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:53 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 16:48 ..
-rw--w---- 1 researcher2 research_team  46 Dec 20 15:53 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 20 15:53 drafts
-rw-rw-rw- 1 researcher2 research_team  46 Dec 20 15:53 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Dec 20 15:53 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 15:53 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 15:53 project_t.txt
researcher2@1f217b8abfd3:~/projects$
```

In the first line, I entered commands to check the permissions assigned to users, groups, and others. The `ls` command provides information about folders, while the `ls -l` command displays detailed information about permissions, indicated by specific letters. From the output, we can see one folder named "drafts" and several files in .txt format.

## Describe the permissions string

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

The organization does not allow others to have write access to any files. Looking at the current permissions, we can conclude that we need to change the permissions to the preogect\_k.txt file:

```
researcher2@6d1e64dded49:~/projects$ chmod o-w project_k.txt
researcher2@6d1e64dded49:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 16:18 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 17:01 ..
-r--r----- 1 researcher2 research_team  46 Dec 20 16:18 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 20 16:18 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 16:18 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Dec 20 16:18 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 16:18 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 16:18 project_t.txt
```

## 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. Therefore, i will change the permissions in this file this way:

```
researcher2@6d1e64dded49:~/projects$ chmod u=r,g=r,o= .project_x.txt
researcher2@6d1e64dded49:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 16:18 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 17:01 ..
-r--r----- 1 researcher2 research_team  46 Dec 20 16:18 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 20 16:18 drafts
-rw-rw-rw- 1 researcher2 research_team  46 Dec 20 16:18 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Dec 20 16:18 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 16:18 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Dec 20 16:18 project_t.txt
```

## Change directory permissions

By the same principle, we provide viewing, recording and execution only to the user who is authorized using all the same commands, and we can also write simply `chmod 700 drafts`, which will give the user full rights to the file, but will not grant rights to other users or groups

## 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.