# File permissions in Linux

## Project description

I mainly work with my organization's research team. Part of my job is to ensure users on the team are authorized with the appropriate permissions. This helps keep the system secure.

My task is to examine existing permissions on the file system and determine if the permissions match the authorization that should be given. If they do not match, I’ll need to modify the permissions to authorize the appropriate users and remove any unauthorized access.

## Check file and directory details

1. Check the permissions set for files and subdirectories in the projects directory, without hidden files.A screenshot of a computer

   Description automatically generated

This command shows the permissions in a directory, but only for regular files; it does not include hidden files.

1. Check the permissions set for files and subdirectories in the projects directory, including hidden files.

A screenshot of a computer program

Description automatically generated

The first line of the screenshot displays the command I entered, and the other lines display the output. The code lists all contents of the projects directory. I used the ls command with the -la option to display a detailed listing of the file contents that also returned hidden files. The output of my command indicates that there is one directory named drafts, one hidden file named .project\_x.txt, and five other project files. The 10-character string in the first column represents the permissions set on each file or directory.

This command shows the permissions in a directory, including hidden files.

## 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.



For example, the file permissions for project\_t.txt are -rw-rw-r--. Since the first character is a hyphen (-), this indicates that project\_t.txt is a file, not a directory. The second, fifth, 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 execute permissions for project\_t.txt.

## Change file permissions

The organization determined that other 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.



The following code demonstrates how I used Linux commands to do this. The chmod command changes the permissions on files and directories. The first argument indicates what permissions should be changed, and the second argument specifies the file or directory. In this example, I removed write permissions from other for the project\_k.txt file.



Then, I used ls -la to review the updates I made.

A screen shot of a computer

Description automatically generated

## Change file permissions on a hidden file

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

The following code demonstrates how I used Linux commands to change the permissions:



I know .project\_x.txt is a hidden file because it starts with a period (.). In this example, I assigned just read permissions to the user and group. I assigned just read permissions to the user with u=r. Then, I assigned just read permissions to the user with g=r.

Then, I used ls -la to review the updates I made.

A screen shot of a computer

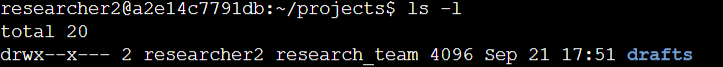
Description automatically generated



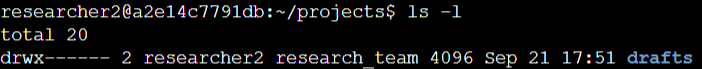
## Change directory permissions

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 following code demonstrates how I used Linux commands to change the permissions:







The first two lines of the screenshot display the commands I entered, and the other lines display the output of the second command. I 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.