# File permissions in Linux

## Project description

## The research team at my organization requires that the file permissions for certain files and directories within the projects directory be updated. The current permissions do not reflect the appropriate level of authorization. Updating these permissions will help to secure the system. To complete this task, I performed the following steps:

## Check file and directory details

The screenshot shows the command I used to list the contents of the projects directory, and the output of the command.

Used the ls command with the -la option to list all contents of the projects directory, including hidden files.

The output of the command shows that there is one directory named drafts, one hidden file named .project\_x.txt, and five other project files. The permissions for each file or directory are shown in the first column.

The 10-character string in the first column represents the permissions set on each file or directory.

## Describe the permissions string

## **1st character** indicates the file type. A d means the file is a directory, and a hyphen (-) means the file is a regular file.

## **2nd - 4th character** indicate the read, write, and execute permissions for the file's user. A r means the user has read permissions, a w means the user has write permissions, and an x means the user has execute permissions. A hyphen (-) means the user does not have any permissions.

## **5th – 7th character** indicate the read, write, and execute permissions for the file's group. The meanings are the same as for the owner's permissions.

## **8th – 10th character** indicate the read, write, and execute permissions for other on the system. The meanings are the same as for the user’s and group's permissions.

## Screenshot of the command line with the commands for this task and their outputChange file permissions

The first two lines of the screenshot show the commands that I ran, and the other lines show the output of the second command. The chmod command is used to change the permissions on files and directories. The first argument to the chmod command specifies the permissions that should be changed, and the second argument specifies the file or directory that the permissions should be changed for. In this example, I ran the command chmod o-w project\_k.txt to remove write permissions from other for the file project\_k.txt. I then ran the command ls -la to review the changes that I had made.

## Change file permissions on a hidden file

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



.project\_x.txt is a hidden file because it begins with a period (.). I removed write permissions from the user and group, and added read permissions to the group.

## Change directory permissions

My organization wants the researcher2 user to have access to the drafts dir and its contents.

This means no one other than researcher2 should have execute permissions.

I previously determined that the group had execute permissions, so I used chmod 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 dir in the projects dir. The first step in this was using ls -al to check the permissions for the dir including hidden files. This informed my decisions in the following steps. I then used the chmod command multiple times to change the permissions on files and dir.