# File permissions in Linux

## Project description

The task is to examine existing permissions on the file system. The project includes determining if the permissions match the authorization that should be given. If they do not match, I am required to modify the permissions to authorize the appropriate users and remove any unauthorized access.

I have done multiple Linux command prompts to complete the task

* Check permissions for files in a directory.
* Check for incorrect file permissions and change permissions as needed.
* Remove unauthorized access to a directory.

## Check file and directory details

The following code demonstrates how I used Linux commands to determine the existing

permissions set for a specific directory in the file system.A screenshot of a computer program

Description automatically generated

## 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

Using chmod command followed by the argument that contain users, groups, or other users permission and adding the math symbols separated by , and no space in order to complete the step followed by the file name.

Check my lab work applying this command:

A screenshot of a computer program

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:

dA screenshot of a computer

Description automatically generated

The first two lines of the screenshot display the commands I entered, and the other lines

display the output of the second command. I know .project\_x.txt is a hidden file because

it starts with a period (.). In this example, I removed write permissions from the user and

group, and added read permissions to the group. I removed write permissions from the user

with u-w. Then, I removed write permissions from the group with g-w, and added read

permissions to the group with g+r.

## Change directory permissions

You have to be in the father directory to apply the permissions to the child directory, see me in the pictures applying the steps using linux

Screenshot of a computer screen

Description automatically generated

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.