# File permissions in Linux

## Project description

[Describe what I accomplish through Linux commands.]

In this project, I’ll demonstrate how to examine and manage file permissions and how to configure user authorization. As a security analyst, setting appropriate access permissions is critical to protecting sensitive information and maintaining the overall security of a system.

In the /home/researcher2/projects directory, there are five files with the following

names and permissions:

● project\_k.txt

○ User = read, write,

○ Group = read, write

○ Other = read, write

● project\_m.txt

○ User = read, write

○ Group = read

○ Other = none

● project\_r.txt

○ User= read, write

○ Group = read, write

○ Other = read

● project\_t.txt

○ User = read, write

○ Group = read, write

○ Other = read

● .project\_x.txt

○ User = read, write

○ Group = write

○ Other = none

There is also one subdirectory inside the projects directory named drafts. The

permissions on drafts are:

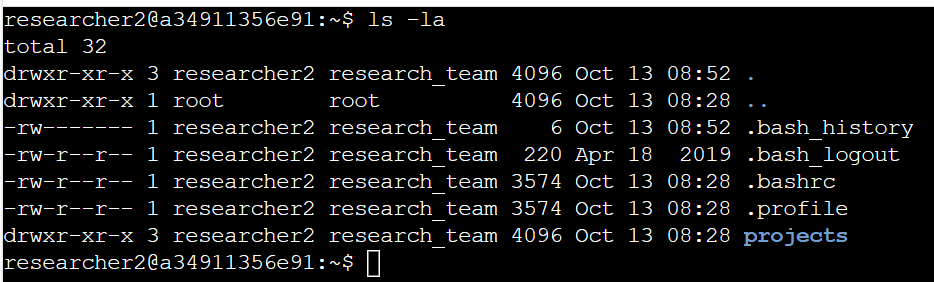
● User = read, write, execute

● Group = execute

● Other = none

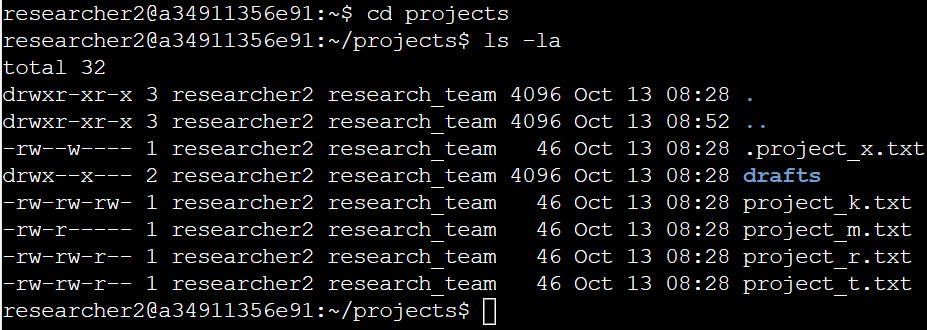
## Check file and directory details

The following code demonstrates how I check file and directory details using the ls -la Linux command in Bash. Using the modifier -la shows the detail listing of files and directories which includes hidden files.



The output of the code shows the file and directory details in researcher 2.The 10-character string in the first column represents the permissions set on each file or directory. Hidden files are indicated with a full stop in front of the file name.

I use the cd command to enter into the projects directory. Followed by ls -la to show the file and directory details of projects.



From the command output, the output shows all the permissions of files and directories, 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 others.

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

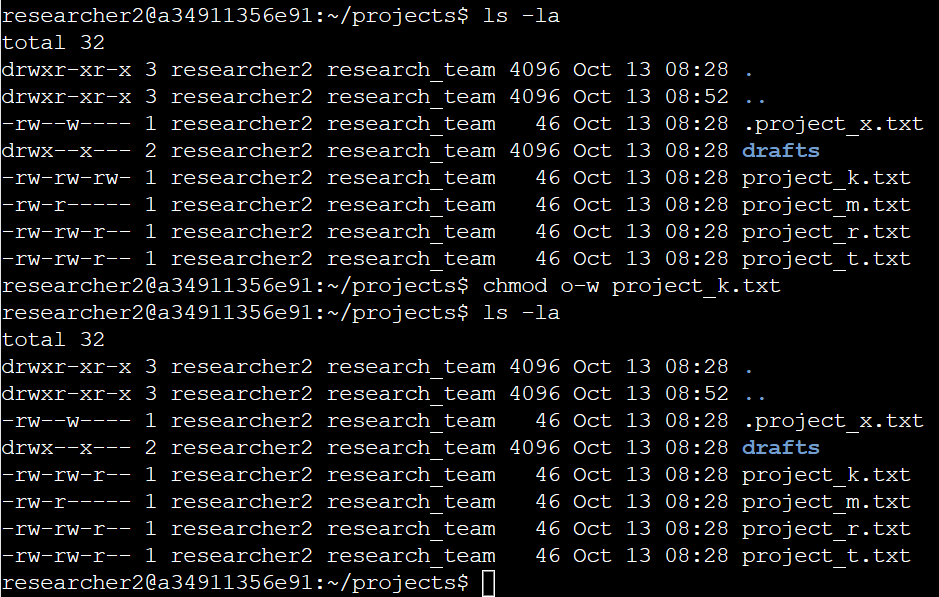
group have write permissions. No one has execute permissions for project\_t.txt.

## 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:



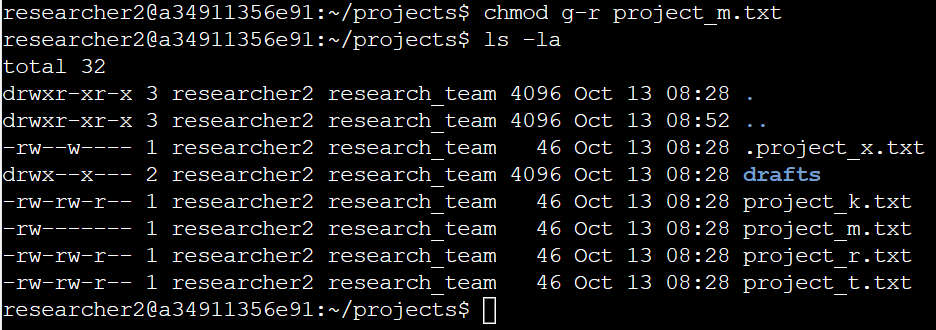
The first line of the screenshot shows that I used ls -la to show the permissions of the files and directories, including hidden files.

The second command I used is the chmod o-w project\_k.txt .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. After this, I used ls -la to review the updates I made.

## Change file permissions on a hidden file

The research team at my organization recently determined that they do not want the anyone except the user to have permission to project\_m.txt.

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

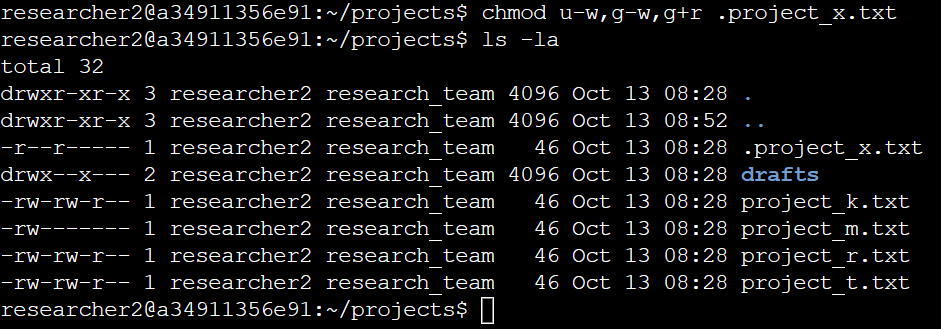


The first command I used is the chmod g-r project\_m.txt to remove the group permission of read.

The second command ls -la to review the updates I made.

The research team at my organization discovered that there is a hidden file with incorrect permission setting set. The file .project\_x.txt is a hidden file that has been archived and should not be written to by anyone. (The user and group should still be able to read this file.)

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



The first command I used is the chmod u-w,g-w,g+r project\_x.txt to perform the following

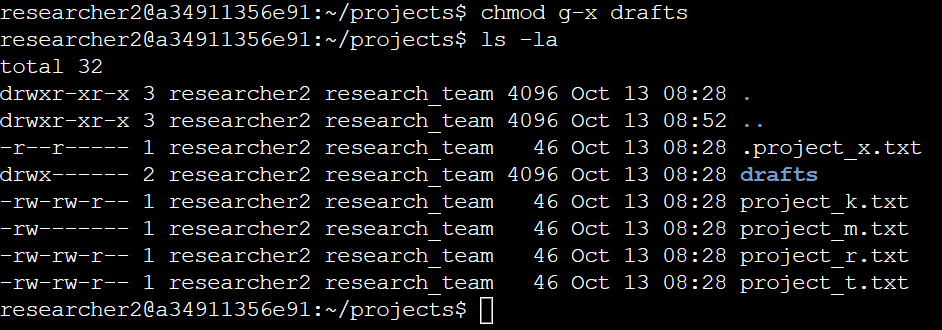
1. Remove user write permissions
2. Remove group write permissions
3. Add group read permission

The second command ls -la to review the updates I made.

## Change directory permissions

The research team at my organization requires me to change the permissions of the directory called drafts. They also determined that only the researcher2 user should be allowed to access the drafts directory and its contents. (This means that only researcher2 should have execute privileges.)

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



The first command I used is the chmod g-x draft to perform the change in permissions for group.

The second command ls -la to review the updates I made.

## 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.