# 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 took the following steps:

## Check file and directory details

The following code shows how I used Linux commands to determine the existing permissions for a specific directory in the file system.



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

I 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. The first character indicates the file type, followed by three characters for the permissions for the owner, three characters for the permissions for the group, and three characters for the permissions for others.

## Describe the permissions string

The 10-character string can be interpreted to determine who has access to the file and what permissions they have. The characters and their meanings are as follows:

* The first character indicates the file type. A d means the file is a directory, and a hyphen (-) means the file is a regular file.
* The next three characters indicate the read, write, and execute permissions for the file's owner. A r means the owner has read permissions, a w means the owner has write permissions, and an x means the owner has execute permissions. A hyphen (-) means the owner does not have any permissions.
* The next three characters indicate the read, write, and execute permissions for the file's group. The meanings are the same as for the owner's permissions.
* The last three characters indicate the read, write, and execute permissions for everyone else on the system. The meanings are the same as for the owner's and group's permissions.

For example, the file permissions for project\_t.txt are -rw-rw-r--. The first character is a hyphen (-), so project\_t.txt is a regular file. The second, fifth, and eighth characters are all r, so the owner, group, and everyone else all have read permissions. The third and sixth characters are both w, so only the owner and group have write permissions. No one has execute permissions for project\_t.txt.

## 

## 

## Change file permissions

I have been instructed to remove write access for other from all files. I reviewed the file permissions for project\_k.txt and found that other has write access. I will remove write access for other to comply with my instructions. The following code snippet illustrates how I used Linux commands to achieve this task:



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 recently archived the file project\_x.txt. They do not want anyone to have write access to this file, but the user and group should have read access. I used the following Linux commands to change the permissions for this file:



The first two lines of the screenshot show the commands that I ran, and the other lines show the output of the second command. I know the file .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.

## Change directory permissions

My organization only wants the user researcher2 to have access to the directory drafts and its contents. This means that no one other than researcher2 should have execute permissions for the directory or its contents. I used the following Linux commands to change the 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. I had previously determined that the group had execute permissions for the directory drafts. To ensure that only the researcher2 user has execute permissions, I ran the command chmod o-x drafts to remove the x (execute) permission from the other user. 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 that my organization wanted for files and directories in the projects directory. The first step in this was to use the ls -la command 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, following the organization's guidelines.