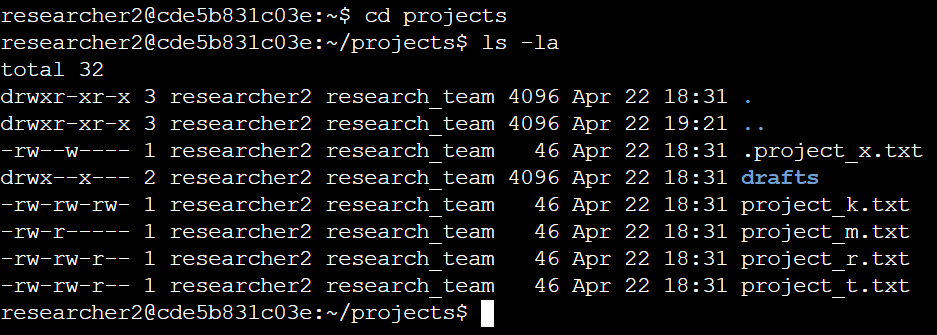
# File permissions in Linux

## Project description

This organization’s research team needs to have their file permissions updated for certain files and directories within the projects directory. The permissions before the project didn’t have the level of authorization that should be given. By using Linux commands, I was able to efficiently check and update these permissions to help keep their system secure and up to date.

## Check file and directory details



The 1st line in the screenshot was entered to move to the projects directory. By using cd projects I was able to access the specified directory. The 2nd line displays the command I entered, while the rest displays the output by listing all of the contents of the projects directory. I then used ls along with -la option to display a detailed list of the file contents while also returning hidden files. The output shows that there is one directory named drafts, one hidden file named .project\_x.txt, and five other project files.

## Describe the permissions string

The 10-character string at the beginning of each file listing represents the permissions set on each file or directory.

The first character in the column is either a d or -, which indicates the file type. If it’s a d, it’s a directory. If it’s a - it’s a regular file.

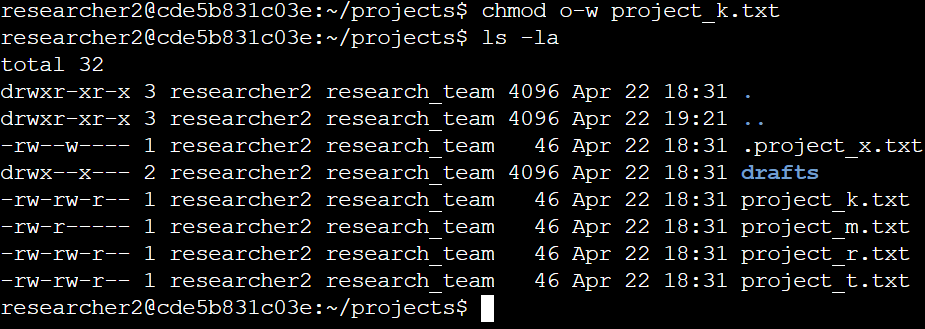
The 2nd-4th characters show the read (r), write (w), and execute (x) permissions for the user. When one of these characters is a - instead, it indicates that this permission is not granted to the user.

The 5th-7th characters act much like the 2nd-4th, indicating the read (r), write (w), and execute (x) permissions for the group instead. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted for the group.

The 8th-10th characters operate much like the previous 2 sections, but function towards the permissions for other, which consists of all other users on the system apart from the user and the group.

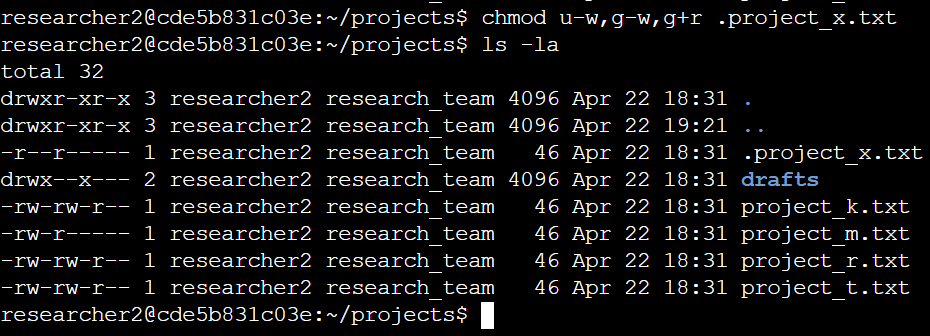
the file permissions for project\_k.txt are -rw-rw-rw-. Since the first character is a hyphen (-), this indicates that project\_k.txt is a file, not a directory. The 2nd, 5th, and 8th characters are all r, which indicates that user, group, and other all have read permissions. The 3rd, 6th, and 9th characters are w, which means that the user, group, and other also all have write permissions. However, no one has execute permissions for project\_k.txt because none of them have x within their code.

## Change file permissions



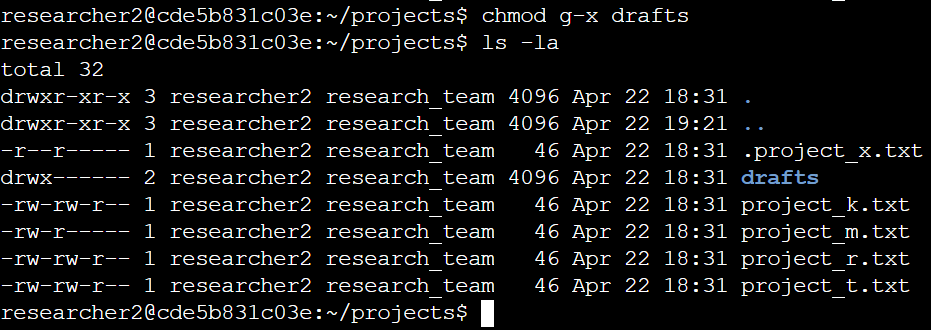
It was decided that other shouldn't have write access to any of their files. To make this happen, I edited the file permissions referencing the permissions prior to the change and saw that project\_k.txt still had write access in other and must be removed. The 1st line of code are the commands I entered to change the access rules. The chmod command changes the permissions on files and directories. The 1st argument o-w explains that other should remove the write access, and the 2nd argument specifies the file or directory to use the first argument for, in this case, used for the project\_k.txt file. The 2nd line was used to show the output of the rules after the change, so I used ls -la to review the updates I made.

## Change file permissions on a hidden file



Because the research team archived project\_x.txt, they did not want anyone to have write access to this project, but still wanted the user and group to have read access. 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 .. Here, I used the chmod command to remove write permissions from the user and group using u-w and g-w respectively, and added read permissions to the group by using g+r. The 2nd line was used to show the output of the rules after the change, so I used ls -la to review the updates I made.

## Change directory permissions



The organization only wanted the researcher2 user to have access to the drafts directory and its contents, meaning that only researcher2 user should have execute permissions. The output here displays the permission listing for several files and directories. Showed that the group had execute permissions, so I used the chmod command and g-x to remove them.Line 4 is the directory (drafts) with restricted permissions. Because researcher2 user already had execute permissions, they did not need to be added.

## Summary

I needed to change various permissions for the organization to stay up to date with the rulings they wanted for files and directories within the projects directory. I 1st used ls -la to check the permissions for the directory. This showed me what the current permissions were to see what needed to be changed based on their request. I then used the chmod command multiple times to change the permissions on files and directories. By specifying what changes we wanted such as o-w to remove write permissions from other, or project\_k.txt to specify where to remove the access from, these were steps needed to ensure that the organization's files stay up to date and secure.