File permissions in Linux

Project description

In this project, I utilized Linux commands to manage file permissions in order to ensure proper authorization and enhance system security. By examining and modifying file permissions, I aimed to align the access privileges of users within the organization's research team with the required level of authorization.

Check file and directory details

To check the file and directory details, you can use the following command:
ls -la /home/researcher2/projects

Describe the permissions string

The permissions string consists of ten characters. Each character represents a specific permission or attribute for the file or directory. The first character represents the file type (e.g., "-" for a regular file, "d" for a directory). The subsequent characters are divided into groups of three, representing the permissions for the user, group, and others, respectively. Each group consists of three characters: "r" for read, "w" for write, and "x" for execute. For example, the permission string "rw-r--r--" indicates that the user has read and write permissions, while the group and others have only read permissions

Change file permissions

To modify the permissions of a file, you can use the chmod command. For example, to remove write access for others on the file "example.txt," you can execute the following command:

chmod o-w /home/researcher2/projects/example.txt

Change file permissions on a hidden file

To modify the permissions of a hidden file such as ".project_x.txt," you can use the chmod command. For example, to make the file readable by the user and group, and not writable by anyone, you can execute the following command:

chmod ug=r,o= /home/researcher2/projects/.project_x.txt

Change directory permissions

To modify the permissions of a directory, you can use the chmod command. For example, to restrict access to the "drafts" directory to only the user, you can execute the following command:

chmod 700 /home/researcher2/projects/drafts

Summary

Through the use of Linux commands, you can manage file permissions effectively. By examining and modifying the permissions, you can ensure the appropriate level of authorization and enhance system security.