

File permissions in Linux

Project description

By using these Linux commands, I'm able to check where I am in the system and what files I'm working with. The `pwd` command shows my current location, which helps me keep track of where I'm navigating. Then, when I use `ls`, `ls -l`, and `ls -la`, I can see all the files in the directory, including hidden ones, along with important details like their permissions, who owns them, and when they were last changed. After seeing the current file setup, I start adjusting permissions. For example, `chmod o-w project_k.txt` takes away write access from others, which stops anyone outside the user and group from changing the file. `chmod g-r project_m.txt` blocks the group from being able to read that file, adding more privacy. Then with `chmod u-w,g-w,g+r .project_x.txt`, I remove write access from both the user and the group but still let the group read it, which helps me control what actions different users can take. Finally, using `chmod g-x drafts` stops group members from entering the drafts directory by removing their execute permission. Overall, these commands help me understand the structure of my files and give me control over who can see or change them.

Check file and directory details

This command shows a **detailed list** of all files in the current directory, including hidden files (like `.project_x.txt`) along with their **permissions, owner, group, size, and timestamps**. The first 10 characters in each line of the output represent the **file type and permissions**.

-
- `project_k.txt` → `-rw-rw-rw-`
 - `project_m.txt` → `-rw-r-----`
 - `project_r.txt` → `-rw-rw-r--`
 - `project_t.txt` → `-rw-rw-r--`
 - `.project_x.txt` → `-rw--w----`
 - `drafts` (directory) → `drwx--x---`

Describe the permissions string

The 10 character string `-rw-rw-r--` represents the file type and permission settings for `project_k.txt`. The first character (`-`) shows that this is a regular file (not a directory). The next three characters (`rw-`) show that the **user** (owner) has **read and write** permissions. The following three characters (`rw-`) show that the **group** also has **read and write** permissions. The last three characters (`r--`) indicate that **others** (anyone else) have **read only** access. This string helps identify who can read, write, or execute the file.

Change file permissions

This command removes write permission from "others" for the file `project_k.txt`. Before running this command, the permissions were `-rw-rw-rw-`, meaning the user, group, and others all had read and write access. After the command is executed, the permissions change to `-rw-rw-r--`, which means only the user and group can write to the file, while others can now only read it. This helps limit who can make changes to the file and adds an extra layer of control.

Change file permissions on a hidden file

```
chmod u=r,g=r,o= .project_x.txt
```

This command sets the permissions on `.project_x.txt` so that the **user** and **group** can **read** the file, and **others** have **no permissions at all**. The previous permissions were `-rw--w----`, which allowed the user to read and write, the group to write, and no access for others. After running the command, the new permissions become: `-r--r-----`

Change directory permissions

```
chmod g-x,o-x drafts
```

This command **removes the execute permission** from the **group** and from **others**, which stops anyone except the user from being able to **enter or access** the `drafts` directory. You're not adding or replacing anything — you're just taking away `x` (execute) from group (`g`) and others (`o`).

Before the command, the permissions were: `drwx--x---`

After the command, the permissions are: `drwx-----`

This means **only researcher2** (the user) can open and work with the contents of `drafts`, and no one else can even access the directory.

Summary

In this scenario, I managed the file and directory permissions within the `/home/researcher2/projects` directory to ensure proper access control. I checked the current permissions, updated files like `.project_x.txt` to restrict write access while allowing read access, and secured the `drafts` directory so only the user, researcher2, can access it. These changes help protect sensitive files and directories, keeping the research data safe and private.