File permissions in Linux

Project description

The research team at our organization required an update to the file permissions for specific files and directories within the projects directory, as the current permissions were inadequate in reflecting the appropriate level of authorization. This action was crucial for maintaining system security.

Check file and directory details

I utilized Linux commands to inspect the existing permissions of a specific directory in the file system. By employing the ls -la command, I obtained a detailed listing of the contents within the projects directory, including hidden files. The output revealed one directory named "drafts," a hidden file named ".project_x.txt," and five other project files, with the 10-character string in the first column representing their permissions.

Describe the permissions string

- The 1st character represents the file type: 'd' for directory, '-' for a regular file.
- Characters 2nd to 4th indicate user permissions: 'r' for read, 'w' for write, 'x' for execute.
- Characters 5th to 7th indicate group permissions.
- Characters 8th to 10th indicate permissions for others.

For example, in "-rw-rw-r--", the file is not a directory. Users, groups, and others have read permissions ('r'). Users and groups have write permissions ('w'). No one has execute permissions.

Change file permissions

I modified the file permissions to revoke write access for 'other' on project_k.txt. I achieved this using the 'chmod' command in Linux. The command syntax involved specifying the permissions to be changed followed by the file name. Subsequently, I verified the changes using the 'ls -la' command.

Change file permissions on a hidden file

To secure project_x.txt, the research team revoked write access for all users except the user and group, who retained read access. Using commands, I modified the permissions accordingly.

Initially, I recognized .project_x.txt as a hidden file. Then, I removed write permissions for the user and group ('u-w' and 'g-w'), while adding read permissions for the group ('g+r').

Change directory permissions

To grant exclusive access to the drafts directory and its contents for the researcher2 user, I adjusted permissions using commands. By inspecting the permission listing, I confirmed that only researcher2 possessed execute permissions for the drafts directory, while the group also had access. I utilized the 'chmod' command to revoke execute permissions for the group, ensuring that only researcher2 retained this privilege.

Summary

I adjusted permissions for files and directories within the projects directory to align with the organization's authorization requirements. Initially, I assessed the existing permissions using 'ls -la'. Subsequently, I iteratively utilized the 'chmod' command to modify permissions based on the observed settings and organizational preferences.