. How does the operating system decide what permissions to apply when a user creates a new file?

Step 1:

File access control (FAC) in operating systems restricts access to sensitive files that are necessary for computer operations. Learn more about the function of FAC and how it operates, including how to create permissions and understand the many types of permissions and combined permissions.

Step 2:

The file access control feature of the operating system can be used to safeguard important computer files. We'll look at how an operating system can restrict access to files and directories or grant it in this lesson.

By modifying the permissions for files and directories, operating systems regulate file access. Access to particular files and directories can be granted or denied by setting permissions. When permission is granted, you have full access to the file or directory and can do whatever with it. When access to a file or directory is disallowed, you cannot access it.

By modifying the permissions for files and directories, operating systems regulate file access. Access to particular files and directories can be granted or denied by setting permissions. When permission is granted, you have full access to the file or directory and can do whatever with it.

2. Explain how the four basic access rights of files and directories interact.

Step 1:

Access permissions fall into four categories (system, owner, group, and world) (Read, Write, Execute and Delete). Since World includes Group and Group, in turn, includes Owner, the categories are not mutually exclusive.

Step 2:

A file or directory can be opened and read with the read command.

A user may open a file or directory, make changes, and then save those changes using the write command.

The user can remove the file or directory by using delete.

An executable file can be run using the function execute. Some files can launch an application on your computer; these files typically end in.exe or.com.

3. What does it mean to have “Execute” access to a file?

Step 1:

A computer programme is started to operate when it is "executed," which also implies that the programme is being started.

Step 2:

A file can be executed with the execute permission. For executable programmes to be run by the operating system, this permission needs to be set.

execute (x) If a file has the "execute" permission set, it can be used to run programmes. When applied to directories, the execute permission enables you to navigate to the directory (i.e., cd into it) and access any of its files. (Files that are not programmes shouldn't be given the execute permission.)