

You are a system administrator managing a shared directory /projects on a Linux server used by different teams in your organization. The directory contains subdirectories for different projects, and each project directory needs specific access permissions for different users and groups.

****Requirements:****

1. ****Project Managers**** (group proj_managers) should have read, write, and execute permissions on all project directories.

Sudo setfacl -m g:project_manager:rwX /projects

2. ****Developers**** (group developers) should have read and execute permissions on all project directories, but they should not be able to delete or modify any files.

Sudo setfacl -m g:developers:rx /projects

3. ****QA Engineers**** (group qa_engineers) should have read-only access to the project_alpha directory but no access to other project directories.

Sudo setfacl -m g:qaengineers:r /projects/project_alpha

4. User alice (a senior developer) should have read, write, and execute permissions on the project_beta directory only.

Sudo setfacl -m u:alice:rwX /projects/project_beta

5. Ensure that default ACLs are set so that any new files or subdirectories created within /projects inherit the correct permissions.

Sudo setfacl -d -m g:project_manager:rwX /projects

Like that for all

****Tasks:****

****Example Subdirectories in /projects:****

Sudo mkdir /projects

Sudo mkdir -p /projects/projects_alpha /projects/projects_beta /projects/projects_gamma

/projects/project_alpha

/projects/project_beta

/projects/project_gamma