GETTING STARTED
WITH
ACCESS CONTROL LISTS

➢ ACCESS CONTROL LISTS (ACL'S):

- In Linux, most of the operating systems has a standard set of file permissions. Aside from these, it also has a more refined set of permissions implemented through ACL's.
- Files and Directories have permission sets for the **Owner, Group** and **Others** for the system. However, these permission **sets have Limitations.**
- Different permissions can be configured for **different users and Groups.**
- There are two types**:**
  - **ACCESS ACLs** **:** ACL for specific file or directory.
  - **DEFAULT ACLs** **:** A default ACL for directory [optional].

TOOLS:

- **SETFACL** **:** Sets ACLs for files and directories.
- **GETFACL** **:** To verifying ACLS

SYNTAX: #setfacl -m <rules> <files>

→ **Viewing the current ACL:**

#getfacl /cloud-data

→ **Setting up an ACL for the user ram:**

#setfacl -m u:ram:r /cloud-data

#getfacl /cloud-data

→ **Switch the user ram and test the permissions:**

#su – ram

$cd /cloud-data

Permission denied because no execute permissions.

$exit

→ **To setting multiple users:**

#setfacl -m u:ram:r,u:raju:rx /cloud-data

#getfacl /cloud-data

→ **To remove an acl for the user:**

#setfacl -x u:raju /cloud-data

→ **If you have multiple ACL setup on a single file, you can remove them all with -b option instead of removing them one by one:**

#setfacl -b /cloud-data

#getfacl /cloud-data

→ **Setting up an ACL for the group sports:**

#setfacl -m g:sports:rw /cloud-data

#getfacl /cloud-data

→ **Setting up an ACL for the multiple groups:**

#setfacl -m g:sports:rw,g:cloud-team /cloud-data

#getfacl /cloud-data