Chapter - 5
ACCESS CONTROL LIST (ACL)

####ACCESS CONTROL LIST :
To Configure different set of file permissions for different users on a single source (file/directory).
ACL's are implemented on ACL enabled partition's. ACL's can applied on (1) users (2) groups.
If we apply for a user in both user level and group level then for him user level will be applied.

####ACL IMPLEMENTATION :
Create a new partition : # fdisk /dev/hda
To update the kernel without restarting : # partprobe
format the partition with ext3 file system : # mkfs.ext3 /dev/hda7
Create the mount point : # mkdir/acl
mount the partition with ACL option : # mount -O acl /dev/hda7/acl
Assign the full permission : # chmod 777 /acl

####CREATE THE SOURCE AT ACL ENABLED PARTITION LOCATION
cd /acl
cat > test

####CREATE THE USERS AND GROUP
useradd userl # useradd user2 # useradd user3
groupadd sales
useradd -g sales s1
useradd -g sales s2

####TO ASSIGN THE PERMISSIONS AT USER LEVEL
setfacl -m u:user:r /acl/test

####TO ASSIGN THE PERMISSIONS AT GROUP LEVEL
setfacl -m g:sales:r /acl/test
setfacl -m u:uers2:rw,u:user3:-/acl/test

####TO SEE THE ACL PERMISSIONS ON RESOURCE /ACL/TEST
getfacl /acl/test

####TO REMOVE THE USERS FROM THE LIST
To remove user 'user2', group 'sales' from the list
setfacl -x u:user2:,g:sales: /acl/test

Note :
We can assign the ACL permissions on existing partitions also by using remount option with ACL feature.
mount -O remount, acl <mount-point> (or) <partition>
ex : #mount -O remount, acl /dev/hda7