RBAC module

Arun Olappamanna Vasudevan

Architecture

File	Mapping		Remarks
gebh_role_id	Role name	Role id	1 to 1
gebh_user_role	User id	Role id(s)	1 to many
gebh_policy	Role id	Inode no(s)	1 to many, used by kernel module
gebh_active_role	User id	Role id	1 to 1, used by kernel module

LSM hooks used

- gebh_inode_create
- gebh_inode_unlink
- gebh_inode_mkdir
- gebh_inode_rmdir
- gebh_inode_rename

Limitation in mkdir

- Desired behavior: When user creates directory, user gets permission to access it

mkdir -> gebh_inode_mkdir -> inode is created

We don’t have inode number of newly created dir in gebh_inode_mkdir