Managing L3 Data Access

This page describes a draft process for managing access to Level 3 (L3) Data, which is derived data produced by one or more collaborating LSST users, who control access to their L3 data in the LSST Data Management (DM) environment. This page (focused on L3 data access) is a companion to the Granting Data Access Rights page (focused on L2 data access).

It will be common for collaborating LSST users to keep their L3 data private from both the public and from other LSST users prior to publication, both to avoid having their results "scooped" by rival researchers and to avoid having pre-publication results misinterpreted or relied on by other researchers prior to validation.

One of the capabilities granted to LSST users with Data Access Rights is the ability to "create Level 3 Data Products (subject to availability of storage allocation) and grant access to all, some, or no other users with data rights (or to named groups of users with data rights)."

The LSST IAM Design involves 3 key components in access control:

- User/Group Manager: This component implements the logic and workflows to determine who has L2 Data Access Rights and who is involved in L3 collaborations. These workflows set/unset User Attributes (i.e., group memberships).
- User Attributes: This component receives information from the User/Group Manager and publishes the resulting User Attributes via a standard LDAP interface.
- Service Level Authorization: Services implement authorization (access control) based on access control lists (ACLs) or database GRANT statements or other service-specific methods, based on the User Attributes. For example, the ACL for WebDAV access to L2 data will allow any user in the "L2 Data Access Rights" group, and the ACL for access to the L3 data produced by the "ABC Quasar" collaboration will allow any user in the "ABC Quasar" group. Service level interfaces will allow data owners to modify ACLs according to service level policies (e.g., a member of the "ABC Quasar" group may have the ability to modify the ACL on some of the group's L3 data to allow read access by other LSST users).

Managing an L3 Group:

- Via ORACLE: Quoting the Data Access White Paper (Doc-5373), "Users (typically in institutional or collaborative groups) can write proposals to the Observatory Resource Allocation Committee for Level Elevation (ORACLE) for the available fraction of the resources in the higher Service Level."
  - The ORACLE process will need to define/maintain a group indicating the users (group members) who can use the resource allocation. It's natural to also create an associated L3 data workspace private to that group.
- Via User/Group Manager:
  - Any user with Data Access Rights can click "Create L3 Data Product Group" in the User/Group Manager web interface to create an L3 group and define its initial members. That user will be the initial owner of the group.
  - Users who own L3 groups will also see a "Manage My L3 Data Product Group(s)" button/link that allows them to add/remove members and add owners / transfer ownership.
  - Users with Data Access Rights will see a "Manage My L3 Data Product Group Memberships" button/link that allows them to request to join L3 groups or leave L3 groups they are currently a member of.

MariaDB example:

```sql
CREATE ROLE L2DataAccessRights;
GRANT L2DataAccessRights TO 'tfleury'@'%', 'jbasney'@'%';
SET DEFAULT ROLE L2DataAccessRights FOR 'tfleury'@'%;'
SET DEFAULT ROLE L2DataAccessRights FOR 'jbasney'@'%;';

CREATE ROLE L3ProjectAMember;
GRANT L3ProjectAMember TO 'tfleury'@'%', 'jbasney'@'%;'

CREATE ROLE L3ProjectBMember;
GRANT L3ProjectBMember TO 'jbasney'@'%';

GRANT SELECT, ALTER, INSERT, UPDATE ON lsst.L3ProjectA to L3ProjectAMember;
GRANT SELECT, ALTER, INSERT, UPDATE ON lsst.L3ProjectB to L3ProjectBMember;

GRANT L2DataAccessRights TO L3ProjectAMember;
GRANT L2DataAccessRights TO L3ProjectBMember;
```