LSST IAM Group Naming Convention

~~ITRFC-12~~ - LSST IaM Group Naming Convention IMPLEMENTED

Note: this document has been updated for clarification and to ensure consistency with LPM-261. For example, previous instances required a "data release" tag in the group name which has since been removed since LPM-261 confers and revokes data rights as all or nothing and does not assign data rights at a granular level.

User Groups

LSST can enforce data access rights through group membership. Furthermore, LSST intends to enforce User-Generated data access rights through group membership. Since we intend on using LSST groups membership to determine data access rights and access to other LSST resources and services, a group naming convention must be established. Groups must adhere to the following format:

lsst_<data-level>_[<identifier>|<UG>_<identifier>]

<data-level> this optional prefix maps to the information classification policy as defined in LPM-122. This identifier cannot be an arbitrary string and must use one of the designated names as set forth in LPM-122. If this prefix is absent then “shareable” is assumed unless a convention supersedes this, see examples below.

<identifier> this optional prefix is an arbitrary field that can be used to designate the context in which the group grants resource access or data access rights. Also, it can be used to designate a group in which membership is denied access to a specific service, resource or Data Release. For example: “comcluster” might be used to designate those with access to the commissioning cluster where “notebookBL” might be used to designate those denied access to the notebook Aspect in the science platform. In terms of LSST’s security policy this prefix shouldn’t be used if a general case is sufficient for access.

<UG> this prefix, using the string “UG”, designates a User-Generated data access rights group. In this context, the <identifier> string is used to name the specific UG data access rights group. This string must be present if the “UG” prefix is used.

When new groups are created that share a prefix, the requirement is that any defined group “lsst_N” is a superset of any subgroups, i.e. “lsst_N_1”, “lsst_N_2”. This requirement is made with the understanding that LDAP does not have a notion of subgroups and cannot enforce this requirement. It is expected to be enforced through LSST’s identity management auditing process.

Note: the above scheme allows for a group name of "lsst". This is an alias of "lsst_users". Also, if optional prefixes are not present then the underscores are not needed.

Data Levels

LSST's information classification policy, LPM-122, defines the following information categories that are used to designate the "data-level". These categories are listed in order of increasing sensitivity.

- Shareable - Information that is not confidential and can be made public without any adverse implications. ***data-level tag name: share***
- Internal - Access to and use of this information is broadly accessible to project staff and others authorized by project management. ***data-level tag name: internal***
- Protected User - Scientific data and operational metadata reserved for authorized data consumers. ***data-level tag name: protu***

The following information categories must not have groups created at their respective "data-level" without prior LSST project and ISO approval:

- Sensitive - Limited access only. Access should not be granted to broad groups of people.
- Highly Sensitive - Information associated with regulatory or contractual burdens that require specific compliance planning or controls.

Examples

Users can have a group automatically created upon account creation. This group serves as a namespace over which they have control. For example, the user `jbasney`, would have the group `lsst_jbasney`. The user `jbasney` could then create and manage (i.e. determine membership of) a group called `lsst_jbasney_galaxyXYZ`. This group could then be used to control access to user generated data products. Note that technically the <data-level> is implying "shareable" as the information classification but if this group is being used to control access to user generated data products then the <data-level> is "protected user".

Access groups can be created, for example `lsst_portal`, that a typical LSST user would be added to during account creation and the data rights access workflow.

During account creation, users must go through an automated (or potentially manual) process to determine their data access rights. This process will automatically add users to preexisting groups that grant them access to non-public LSST data. For example, the user `jbasney` has been determined to be a US Astronomer and thus is granted access to `lsst_protu.`

Staff Groups

For internal LSST staff, default groups hall be created with the prefix of:

lsst_internal_<identifier>

It is assumed that any member of these groups have broad access to LSST data classified as “internal” or lower as detailed in LPM-122.

For internal LSST staff that require admin privileges, default groups shall be created with the prefix of:

lsst_admin_<identifier>

It is assumed that any member of these groups have broad access to LSST data classified as “highly sensitive” or lower as detailed in LPM-122. ***Obviously this means LSST staff in these groups have access to any data due to the ability to escalate their privileges. Membership in these groups needs to be carefully planned.***

For both of these group prefixes:

<identifier> an arbitrary field used to designate the context in which the group grants service or resource access. Also, it can be used to designate a group in which membership is denied access to a specific service or resource. In terms of LSST’s security policy this prefix shouldn’t be used if a general case is sufficient for access.

Default Groups and Hierarchy

lsst_users - All LSST users placed in this group. See https://confluence.lsstcorp.org/display/LAAIM/Granting%2BData%2BAccess%2BRights and https://docs.google.com/document/d/1AKjIiYiBr7tenl5ZlNGypc2n8xqWK2SSmTDUCMJjxvQ/edit

lsst_staff - All LSST staff, equivalent to lsst_internal_staff. This group has broad access to LSST data classified as “internal” or lower as detailed in LPM-122.

lsst_admin - All LSST staff requiring administrative privileges on any particular service or resource. In general, this group should not be used. Instead, specify specific groups according the “lsst_admin_” prefix scheme specified above. This group provides a quick way to list all accounts requiring admin privileges and can also be used to quickly revoke those privileges.

lsst_disabled - LSST disabled accounts. Users or staff that need to be disabled quickly can be added to this group. This is normally used for security issues and/or for users no longer part of the project.

Abbreviations

In the case where LDAP, Linux, POSIX standards, etc. enforces character limits in group names, abbreviations may be used in a consistent fashion. For example: lsst_admin_* could be lsst_adm_*.

Historical Groups

The following defined groups are currently in existence at the NCSA. They do not necessarily conform to the naming conventions above. However, they are all assumed to be composed of internal LSST staff. Since many of these group names follow LSST’s organizational structure under its construction phase, it is assumed that most of these groups will no longer be needed when LSST moves into the operations phase. If possible, these groups should be renamed to follow the “lsst_internal_<identifier>” convention specified above. (see: https://docs.google.com/spreadsheets/d/14VE13S8fYWtE8bCa_K4AQ79TFak2DTAH-n9L4sB2rB4/edit#gid=0)

Old Group Name	Proposed New Name	Description
lsst_alertprod	lsst_int_dm_ap	LSST Alert Production team within DM (University of Washington)
lsst_aws_admin	lsst_int_aws_proj	Group for access to the AWS portal for LSST project usage.
lsst_aws_users	lsst_int_aws	LSST users of Illinois AWS services through NCSA IDP
lsst_cam_ccs_adm	lsst_adm_cam_ccs	LSST Camera Control Systems admins
lsst_daqadm	lsst_adm_cam_daq	LSST administrative developers for the DAQ Teststand
lsst_daq	lsst_int_cam_daq	Users of LSST DAQ system

lsst_data	lsst_int_dm_data	LSST Data Access and Database team within DM (SLAC)
lsst_datarelease	lsst_int_dm_release	LSST Data Release Production team within DM (Princeton)
lsst_disabled	lsst_disabled	LSST Disabled Users When users need to be disabled quickly, they can be added to this group. This can be used for security issues and/or for users no longer part of the project.
lsst_epo	lsst_int_epo	LSST Education & Public Outreach team (external to DM)
lsst_hwadmin	lsst_adm_vendor	LSST hardware administrators, e.g. support vendors
lsst_imsim	lsst_int_dm_imsim	Legacy LSST Image Simulation Group
lsst_infrastruct	lsst_int_dm_infr	LSST Infrastructure (NCSA) team within DM
lsst_int_bastion	lsst_int_bastion	Users who have access to lsst-bastion* server(s)
lsst_int_dbb_ats	lsst_int_dbb_ats	ATS (Auxiliary Telescope System / Spectrograph) users of the data backbone service.
lsst_int_kubernetes	lsst_int_kubernetes	Users who have access to log into Kubernetes
lsst_jupyter	lsst_int_jupyter	Initial group of test users for Jupyter Hub
lsst_leads	lsst_int_leads	Leaders of LSST
lsst_nebula	lsst_int_nebula	Users of the general LSST project in Nebula OpenStack
lsst_network	lsst_int_network	LSST International Communications (aka Long Haul Networks) and Base Site (NOAO)
lsst_ora_dba	lsst_int_ora_dba	Group for DBA and system admins of the LSST database enclave. for lsst-dev-ora*
lsst_processing	lsst_int_process	LSST Processing Control team within DM (NCSA)
lsst_security	lsst_int_ncsa_security	LSST Security (NCSA)
lsst_sqre	lsst_int_sqre	LSST SQuaRE - Science Quality and Reliability Engineering team within DM (LSST/AURA)
lsst_sui	lsst_int_sui	LSST Science User Interface and Tools team within DM (IPAC)
lsst_sysadm	lsst_adm_ncsa	LSST System Administration at NCSA rename from grp_lsst_admin
lsst_storage	lsst_int_ncsa_set	NCSA Storage team assigned to LSST
lsst_int_ncsa_irst	lsst_int_ncsa_irst	NCSA Incident Response and Security team assigned to LSST
lsst_networking	lsst_int_ncsa_nerd	NCSA Networking team assigned to LSST
lsst_sysadmin	lsst_int_ncsa_sysadmin	NCSA Systems Administration team assigned to LSST
lsst_its	lsst_int_ncsa_its	NCSA IT Services team assigned to LSST
lsst_int_ncsa_idds	lsst_int_ncsa_idds	NCSA Integrated Data and Database Services team assigned to LSST
lsst_tel_ocs_adm	lsst_adm_tel_ocs	LSST Observational Control System administrators
lsst_tel_tcs_adm	lsst_adm_tel_tcs	LSST Telescope Control System administrators
lsst_telescope	lsst_int_tele	LSST Telescope and Site team (external to DM)
lsst_users	lsst_staff	Active LSST ‘staff’ (pruned from historical lsst_users)

n/a	all_lsst	All LSST users (active and historical) - generated dynamically from join of all other 'lsst_*' groups
lsst_vsphere_mac	*delete*	Users of the LSST vSphere Mac VM environment