



Group in Action

Access Management Strategies for Higher Education and Research

Lafayette Reference Groups

Bill Thompson, CISSP, CSSLP, GSLC

thompsow@lafayette.edu

Director Digital Infrastructure

Lafayette College

TIER Folder and Group Design

- **etc:** - Grouper configuration, administrative access control groups, and loader jobs
- **basis:** - groups used exclusively by the IAM team to build reference groups
- **ref:** - reference groups, institutional meaningful cohorts - “truth”
- **bundle:** - sets of reference groups used in policy for many services
- **app:** - enterprise applications access control policy - specific policy for a service
- **org:** - delegated authority, ad-hoc groups, org “owned” apps or reference groups
- **test:** - test folder for system verification

TIER Folder and Group Design

Basis Groups - Systems of record codes (hidden away from access policy)

- **basis:hris:{employee_codes}**
- **basis:sis:{student_codes}**

Reference Groups - Institutionally meaningful cohorts – “truth” (aka subject attributes)

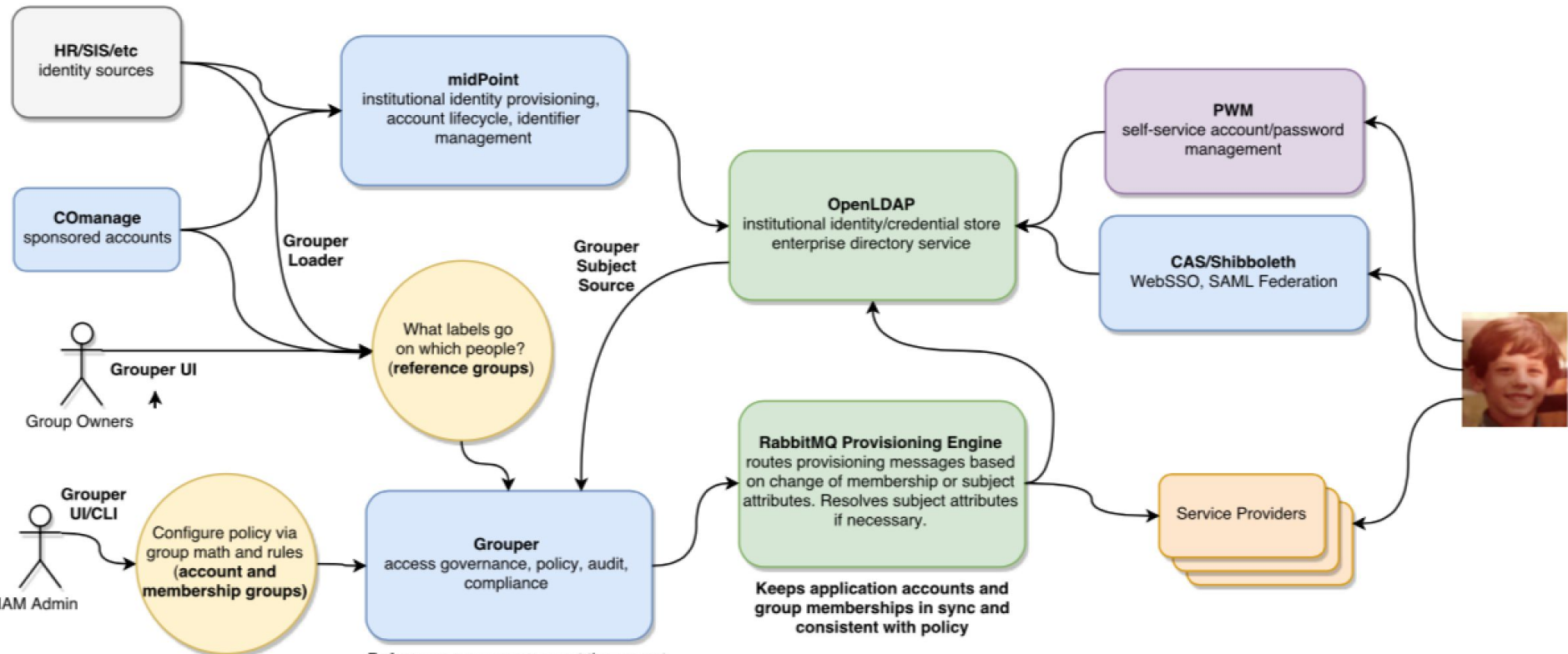
- **ref:role:** - institutional scope roles (e.g. president, provost, chaplain...)
- **ref:employee:** - types of employees (faculty, staff, part-time, full-time...)
- **ref:student:** - types of students

Access Policy Groups - digital policy based on subject attributes

- **app:vpn:vpn_allow** - allow policy for vpn access

Bundle Groups - Sets of reference groups (cohorts) used to drive access policy

- **bundle:employee_services** - cohorts that get employee-like access



Account and membership groups represent authorization policy. Effective membership configured via group math or rules generates change notifications.

Reference groups represent the current state of membership for all subjects as known to the enterprise. They are used to configure access management policy and provide the means for automated provisioning of groups and accounts as well as audit and compliance.

ref

- + alumni
- + dept
- + employee
- + engineering
- + etc
- + ex_officio
- + Faculty Governance
- + personas
- + Projects
- + shared_accounts
- + sponsored
- + student
- + trustees
- deactivated
- deceased
- disabled

student

- + majors
- + status_change
- class2016
- class2017
- class2018
- class2019
- class2020
- class2021
- class2022
- early_onboarded
- exchange_students
- freshman_class
- grads_prev_curr_year
- incoming_class
- junior_class

employee

- + ad_hoc_employees
- + new_hires
- + tenure
- active_positions
- admin_ft
- admin_pt
- athletic_interns
- emeriti
- employee
- exempt_ft
- exempt_pt_w_positions
- faculty
- faculty_ft

Home > Root > ref > student > early_onboarded

early_onboarded

Students who were onboarded ahead of their official first day as a student. E.g. part time students that need online access prior to the first day of classes. A generalized case of "incoming_class". Subjects added to this group should be given a definite end date (i.e. a date sometime after the start of term when reference groups driven from institutional data take over).

Home > Root > ref > student > on_track_grad

on_track_grad

Students on track to graduate in the current school year. Ref: Banner.

[Home](#) > [Root](#) > [ref](#) > [employee](#) > [new_hires](#) > [recent_hire](#)

recent_hire

Recently hired employee. Data may not yet have been entered in Banner, yet. Subjects added to this group are automatically given an end date 28 days (4 weeks) after being added. Unless you have a specific reason, it is probably best to NOT add a subject directly to this group, but instead to `recent_non_faculty_hires` OR `recent_faculty_hires`. Members of those groups are automatically made indirect members of this group.

[Home](#) > [Root](#) > [ref](#) > [employee](#) > [temps_w_positions](#)

temps_w_positions

Temporary employees (code "NP") with active positions.

More ▾

ex_officio

Offices that confer permissions.

More ▾

Folder contents

Privileges

Filter for:

Apply filter

Reset

Name ▾

^ Up one folder

dean

chaplains

Clerk of the Faculty

College Chaplin

Director of Engineering

General Counsel

President of Student Government

President of the College

provost

engineering

More ▾

Folder contents

Privileges

Filter for:

Apply filter

Reset

Name ▾

^ Up one folder

basis

CEE

CHBE

ECE

EGRS

ENGU

ES101

etc

ME

Engineering Full-Time Faculty


  basis

 active_positions

 exempt_pt

 expelled_intake

 extended_loa_students

 loa_4_years

Home > Root > basis > loa_4_years

loa_4_years

Students that have taken a leave of absence within 4 years of the current date.



Thanks!

Bill Thompson, CISSP, CSSLP, GSLC
thompso@lafayette.edu
Director Digital Infrastructure
Lafayette College