

Open Apereo 2016

100% Open for Education

Grouper in Action

Access Policy and Reference Groups @ Lafayette College

Bill Thompson, CISSP
Director Digital Infrastructure
Lafayette College



Policy and Governance

PRESIDENT
PROVOST



REGISTRAR



HUMAN
RESOURCES



FACULTY
AFFAIRS



CIO



...

Establish identity

Determine policy

Source Systems

HR

faculty, staff

SA

student,
postdoc

Finance

PI, approver

Courses

instructor,
enrolled

...

Manage Identity

Persons

Accounts

Organizations

Groups

Privileges

Authenticate
Authorize
Provide
Federate

Reflect
& Join

Systems and Services

Business
systems

Network
services

Library

...

Federated
partners

Enrich identity

SCHOOLS
DEPARTMENTS

PROJECTS

PROGRAMS

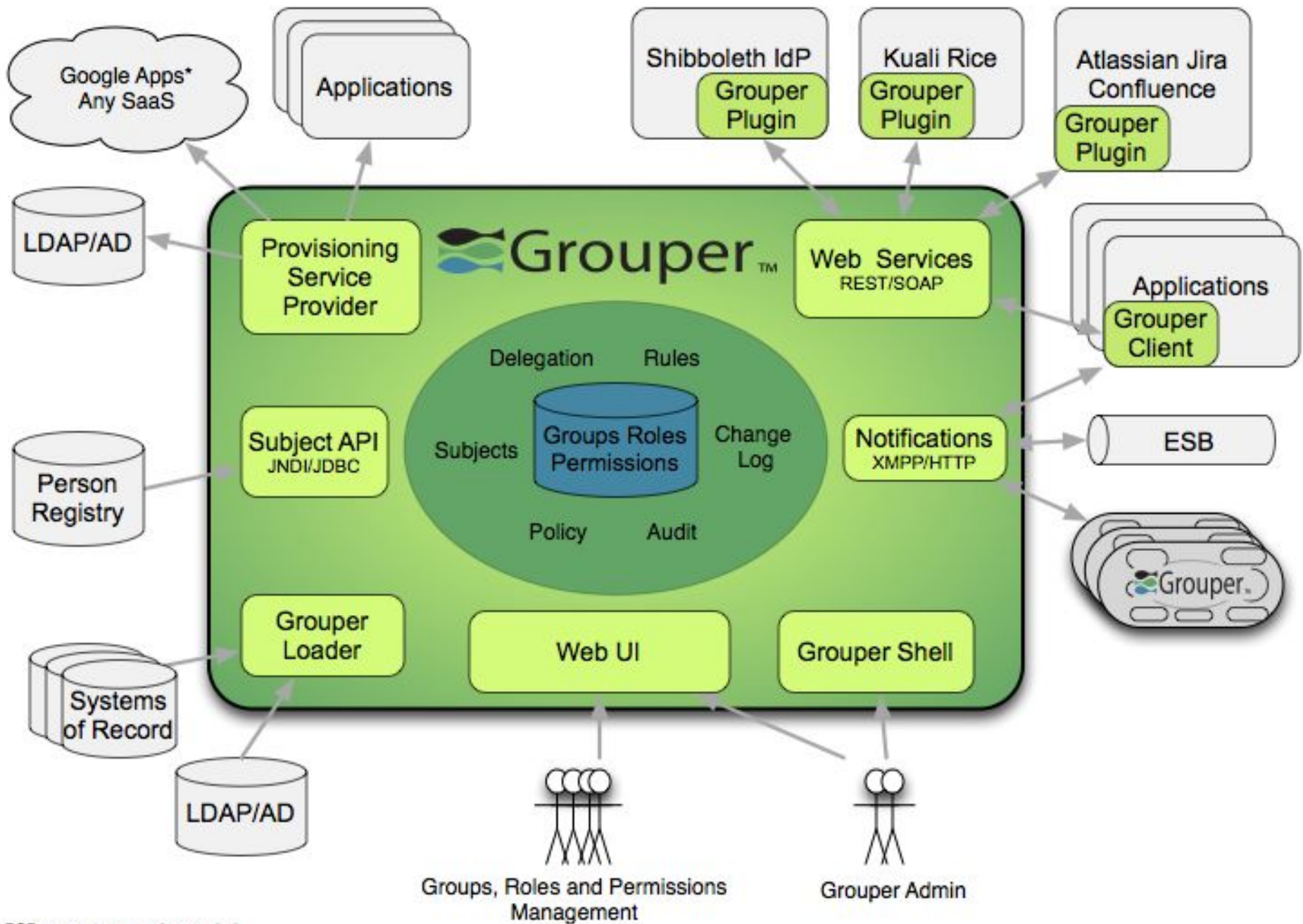
Manage Groups

Apply policy

TEAMS

USERS

Manage Privileges



* PSP connectors may be needed

Reference Groups

ref

- role
 - banner
 - class_years
 - contractors
 - ex_officio
 - interns
 - legacy
 - new_hires
 - personas
 - alum
 - alum_no_degree
 - december_grads_2015
 - disabled
 - employee
 - faculty
 - incoming_class
 - lafayette_members
 - on_track_grad
 - outgoing_class
 - student
 - vendors

ref

- role
 - banner
 - class_years
 - first_class
 - lvaic
 - part_time
 - transfers
 - class2015
 - class2019
 - class2020
 - contractors
 - ex_officio
 - chaplain
 - clerk_faculty
 - dean_of_curriculum_a
 - dean_of_faculty
 - president
 - pres_stu_gov
 - provost
 - interns
 - legacy
 - new_hires
 - personas
 - alum
 - alum_no_degree

org

- academic
 - compsci
- admin
 - communications_division
 - digital_communication
 - dining_services
 - dining_services_staff
- its
 - di
 - edms
 - itech
 - web
 - admin
 - di
 - edms
 - itech
 - its_staff
 - usg
 - webdev

- + arts_env
- + cognos
- + crashplan
- + DHCP Admins
- + file_services
- + HR Mail Lists
- + ITS-Library Wiki Access
- + keyserver
- + Lab Manager
- + mediaspace
- + moodle
- + noli
- + papercut
- + portal
- + provost_archive
- + rt
- + splunk
- + trustee_archive
- + vpn

exports

More ▾

Folder contents

Privileges

Filter for:

Ap

Name ▾

^ Up one folder

adv_annual_fund

adv_executive

adv_major_gifts

adv_tools_bi_analytics_explorer

adv_tools_bi_analytics_user

bi_administrator_edms

student_include

Student includes.

More ▾

Members

Privileges

More ▾

The following table lists all entities wh

Filter for:

Remove selected members

Entity name ▾

 cos_students

 fall2015_grads

 first_class

 incoming_class

 lvaic

 part_time

 student

cos_students

Students that are in a COS state may not quite meet the definition of "student" invented for the portal. ITS policy seems to be to continue services for these accounts unless the Office of Advising indicates the account should be termed. Recently reinstated students may also need student access to the portal prior to taking classes. Those accounts should be added to this group with a definite end date (e.g. start of next semester) in mind.

More ▾

Members

Privileges

More ▾

The following table lists all groups in which this group is a member.

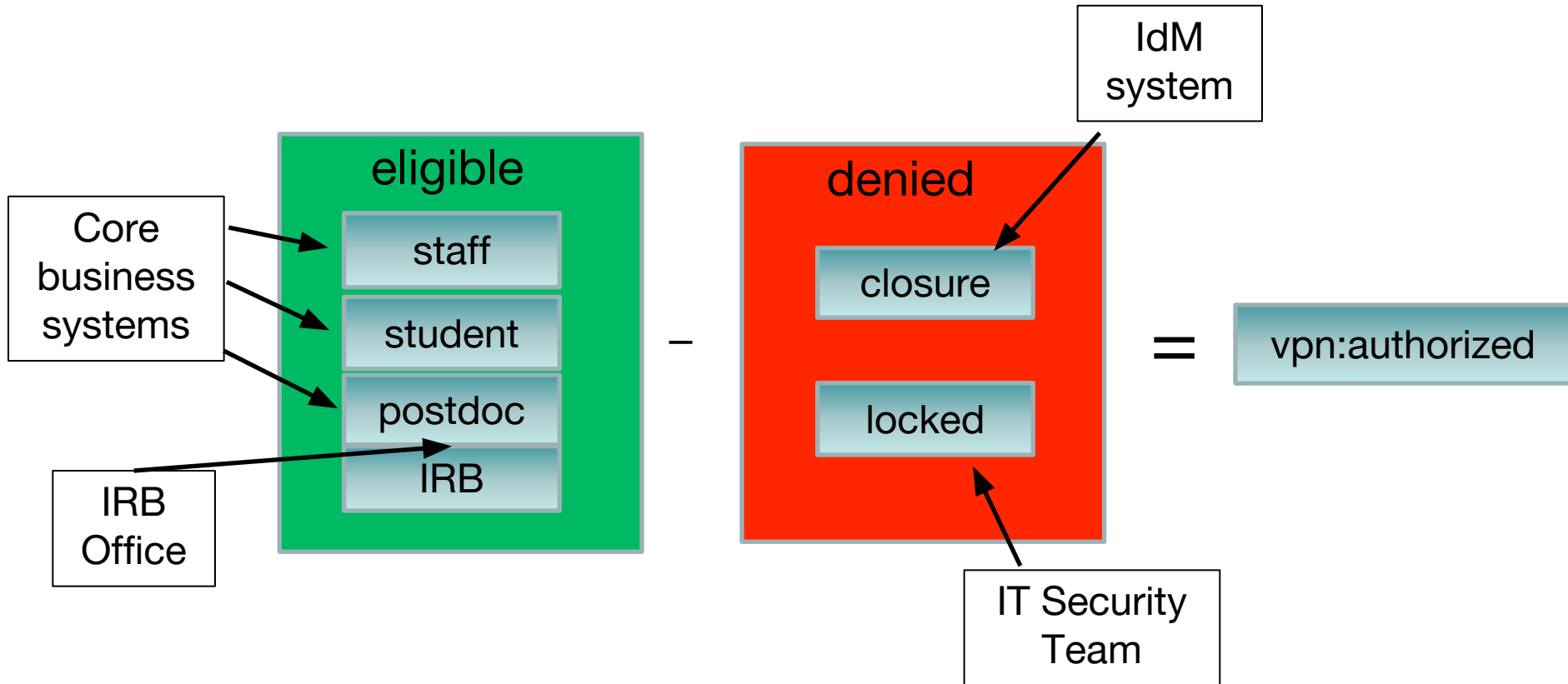
Filter for:

Remove from selected groups

Folder Group Membership

lc : app : portal  student_include Direct

Distributed Authorization Management



Different groups, different authorities
VPN only uses “vpn:authorized”

  vpn_roles

 exceptions

 exceptions_exclude


 exceptions_include

 netadmins

 netadmins_exclude

 netadmins_include

 vpn

 vpn_exclude

 vpn_include

vpn_include

VPN net inclusions.

More ▾

Members

Privileges

More ▾

The following table lists all entities wh

Filter for:

Remove selected members

Entity name ▾

 admin_ft

 admin_pt

 admissions_contractor

 chaplain

 consultants

 contractor_as_facstaff

 contractor_min_vpn

 contractor_wifi

 ECE access

 edms_consultants

 emeriti

 emeriti

 Engineering projects

 exempt_ft

 exempt_pt

 faculty_ft

 faculty_personas

 faculty_pt

 Geology Field Book app

 interns

 LIDAR Cloud Display web:

 moodle_archive

 nonexempt_ft

 nonexempt_pt

 pres_request

 recent_hire

 staff_personas

 TheLaf Editors

 union_ft

 union_pt

 VCR rebuild project

 You cannot VIEW group: 1d77d04...

 vendors

 vip

 vpn_emp_no_ref

 vpn_rosenbau

 vpn_watkinma

 vpn_woolleyj

vpn_include

Trace membership for ALMA Architecture LLC

ALMA Architecture LLC is a member of the *vpn_include* group by the following paths:

ALMA Architecture LLC is a **direct member** of

↳ [lc:app:vpn:policies:contractor_as_facstaff](#)

↳ which is a **direct member** of

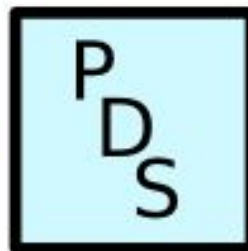
↳ [lc:app:vpn:vpn_include](#)



Group Provisioning Architecture



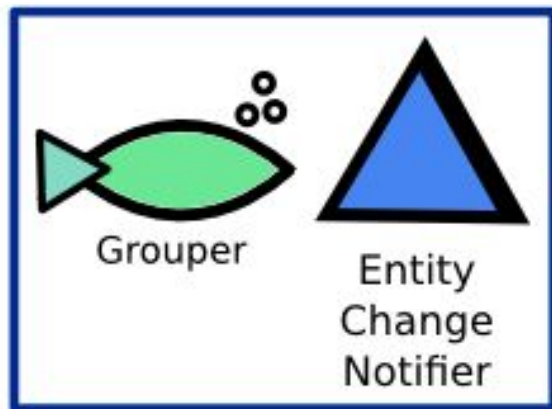
Grouper



Provisioner
Delivery
Service



Membership
Provisioners

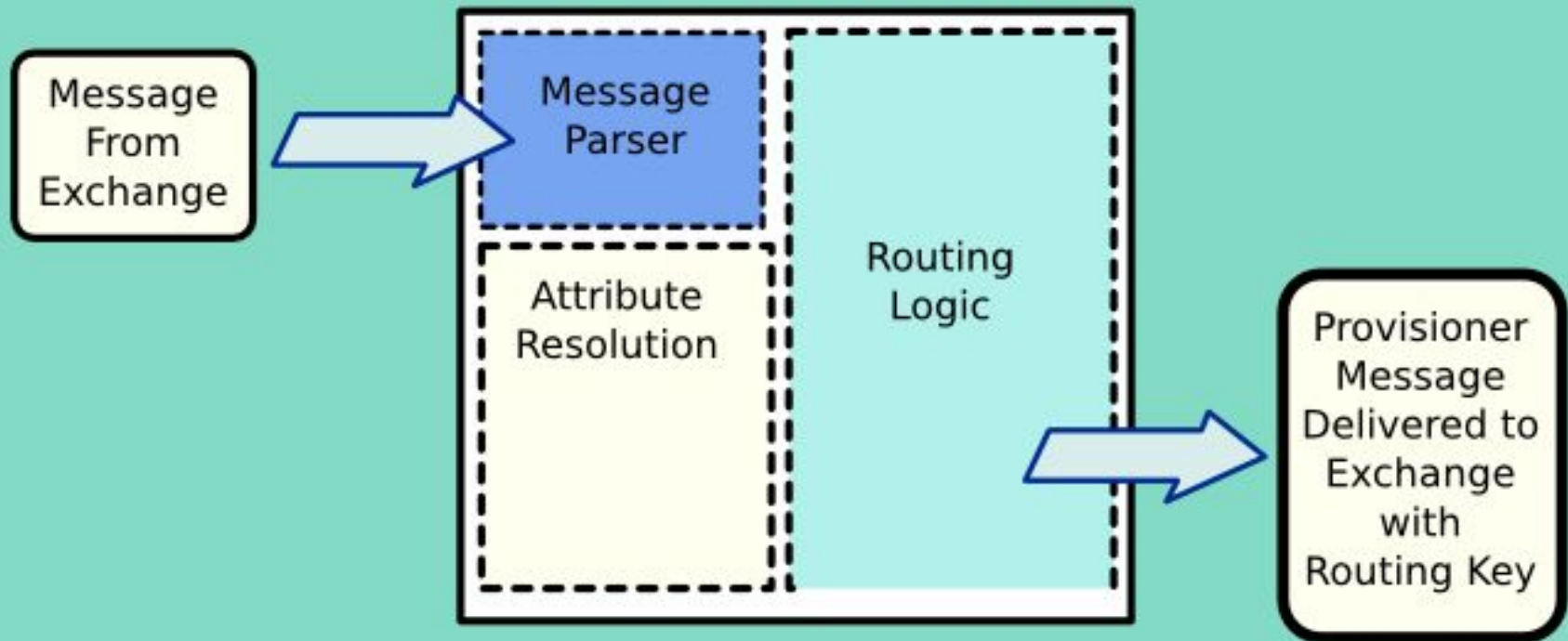


Provisioner
Delivery
Service



Account
Provisioners

Provisioner Delivery Service Architecture



Access Policy managed by Grouper, so far...

aams

Ad Astra

Bulkmail

Business Objects Enterprise

Chalk

CityRyde

Cmail

cnet

Confluence

Directory Administration

dmca

Facilities SIMS

gnetid

grouper

im

isx

IT Ecosystem

Lab School

LDAP

lists

Mail Forwarding

Mail Quarantine

Microsoft Exchange

modem pool

monitoring

myUChicago

Non-po

Onecard

online directory

password expiration

Service Now

sharepoint

shibboleth

statements portlet

SVN

tank

unifiedcomm

versions

virtualization

voip

vpn

web hosting

webproxy

webshare

webspace

wireless

Access Policy managed by Grouper, so far...at University of Chicago

aams

Ad Astra

Bulkmail

Business Objects Enterprise

Chalk

CityRyde

Cmail

cnet

Confluence

Directory Administration

dmca

Facilities SIMS

gnetid

grouper

im

isx

IT Ecosystem

Lab School

LDAP

lists

Mail Forwarding

Mail Quarantine

Microsoft Exchange

modem pool

monitoring

myUChicago

Non-po

Onecard

online directory

password expiration

Service Now

sharepoint

shibboleth

statements portlet

SVN

tank

unifiedcomm

versions

virtualization

voip

vpn

web hosting

webproxy

webshare

workspace

wireless

Access Policy Managed by Grouper so far...at Lafayette College

Arts_env

Cognos*

DHCP Admin

File Services

HR Mail Lists

ITS-Library Wiki

KeyServer

Lab Manager

Mediaspace

Moodle

Nolij

Portal*

Provost Archive*

Mediaspace

Moodle

Nolij*

Papercut*

Request Tracker RT

Splunk

Trustee Archive

VPN

OrgSync

CS Wiki*

LCA Wiki*

Gitlab*

Crashplan*

Reference Groups: 38

Loader Jobs: 17

(2 LDAP, 15 SQL)