Grouper Intro and Case Studies
IAM Online
July 13, 2016 – 2 pm EDT

Chris Hyzer, University of Pennsylvania
Bert Bee-Lindgren, Georgia Tech
John Bryson, Georgia Tech
Dusty Edenfield, Georgia Tech

Carl Waldbieser, Lafayette College
Madan Dorairaj, NYU
Julio Macavilca, NYU
Jeff Pasch, NYU
IAM Online
Grouper
Intro
Internet2 TIER

- Trust and Identity in Education and Research
- Enrich existing Internet2 middleware
- Add new technology to address community’s needs
- Common high level project management
- Sustainable funding model
- Improve TIER collaboration
- TIER software and projects:
  - Grouper, Shibboleth, COmanage, APIs, packaging, instrumentation, security, etc
The Grouper Story

- Open source, community-driven project of the Internet2 Middleware Initiative
  - Initial release v0.5 in December 2004
What is Grouper?

- Central authorization
- Groups
- Permissions
- Provisioning
- Auditing
- Delegation and distributed management
Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify and make consistent by using the same group or role in many places

**Physics 101 Course Group**

- Email Group
- Wiki Access
- Lab Reservations
Additional benefits of access management

- Empower the right people to manage access. Take central IT out of the loop.
- See who can access what, with a report rather than a fire drill
- Easier deprovisioning when affiliations change
Access management stages: authorization > authentication

Enrich & centralize access management with groups determined from systems of record

- Courses, financial accounts, departments
- Define service-specific access policies in the centralized access management system

Math Faculty Group

can access

Math Faculty Resources
Access management stages: authorization > authentication

Get central IT out of the loop

- Distributed management
- Exceptions
- Departmental applications
The Grouper Story

Grouper v2.X in 2011 expanded beyond groups

- Roles & permissions

- Rules

  - If removed from group A
  - Then remove from group B
* PSP connectors may be needed
Get started and contribute back

- Grouper training videos  
  https://spaces.internet2.edu/display/groupertrain/Grouper+Training

- Grouper Community Contributions on the wiki:  
  https://spaces.internet2.edu/display/Grouper/Community+Contributions

- Contact Emily Eisbruch at emily@internet2.edu for help getting access to the wiki to add your story
Upcoming events

- 2016 Internet2 Technology Exchange, Miami, September 25-29
  - Price goes up $75 tomorrow!
- Grouper BOF at Tech Ex on Tues afternoon Sept 27
- Grouper Provisioning: Locally & Cloud at TechEx on Monday, Sept 26, 1:10pm
Georgia Tech
Grouper & Door Controls
IAM Online
July 13, 2016
Door Controls: Before

Enterprise Data

Single Department

Vendor1

Rules

Manual Changes
No Cleanup

Auto

Vendor2

Rules

Manual Changes
List Imports
No Cleanup

Auto

Vendor3
Door Controls: Vision

Enterprise Data → Loader → Grouper → PSPNG → Person Registry LDAP → Integration

Door Management UI → Grouper Web Services → Grouper & BuzzApi (soa)

Rules (Loaded Groups) + Manual (Temporary & Conditional)

Door Control (Vendor 4)
- GroupMembers → Door Schedule
- ...
Status: Mid Implementation
First Buildings

- First Georgia Tech Grouper
  - Done: Installed, OracleDB, Subject Sources, WS/SoA
- In Process
  - Grouper: Loader, PSPNG (to Entitlements)
  - Door hardware installation
  - Door-control integration
  - Group organization
  - Door Control Application
- Soon:
  - HA Servers, Redundant Oracle, Load Balancers
Grouper: Interesting Bits (1)

Subjects

● Many people have Buzzcards but no computer accounts
● Some Buzzcards are Loaned/Shared
● Solution: Person Subjects in Grouper
  ● (And Account Subjects)
  ● Loaded Groups: Both Person & Account Subjects
  ● Use Group Math (Intersection) to filter to desired subject type
  ● Use Attributes/Hooks to prevent manual mistakes
Grouper: Interesting Bits (2)

- Manual Group Memberships & Cleanup
  - Temporary
  - Conditional
    - George can get into Margaret’s Lab while George remains an employee
      - Might be 1 week or 1 decade
    - Anticipated Solution:
      - Membership Attribute
      - Hook that looks to see if group being removed is a condition of another membership
Scriptable Grouper

IAM Online
July 13, 2016
Lafayette College
Three Main Stems

- **orgs** mirrors an org-chart.
- **refs** are reference groups that are either data-driven or maintained directly in Grouper.
- **apps** are where application specific policies are composed and exported to provisioners.
How to Get Work Done

- The New UI
- The Admin/Lite UI
- The Grouper API
The New UI

- Excels at routine tasks.
- Grant/deny permission to individual subjects.
- Add small-moderate lists of subjects to groups.
- Remove all members from a group.
- Create new groups, stems, etc.
- Tweak permissions.
The Grouper API

- Excels at tasks requiring precision and automation.
- Remove a large number of specific subjects from a group.
- Create uniform stem/group/permission structures.
- Add/remove rules to a group.
- Set up a Grouper Loader job.
The Grouper Shell

- Typical way for a system administrator to work with the Grouper API is via the Grouper Shell (GSH).

- GSH is feature-poor compared to modern shells.
  - No readline. Arrow keys do not work.
  - No command history.
  - Not really suitable as an interactive shell.

- Useful for executing batch scripts.
Why is Interactivity Important?

- Allows exploring the Grouper API
- Instant feedback
- Allows ad hoc solutions to be built up incrementally.
Grouper Shell Wrappers

- Started as groovysh4grouper
- Added Jython and Clojure scripting languages
- Basic idea is to leverage modern scripting tools and shells to host the Grouper API.
- Provides readline, introspection, instant feedback, familiar environments.
Unintended Benefits

- A scriptable Grouper allowed Lafayette College to try out some interesting ideas.
- The Grouper Provisioning Service Provider (PSP) seemed too complicated for a pilot deployment.
- A simple change log consumer existed in the Grouper API.
- Scripting the change log consumer and standing up a very basic provisioner was simple.
Lafayette College – Grouper Pilot Provisioning Architecture
Architectural Needs
Change Over Time

- Desire to provision multiple targets.
- Grouper project already discussing message queues.
- Scripted changelogger and provisioners could be quickly changed to meet these goals.
Lafayette College – Grouper Pilot Provisioning Architecture V2
Looking toward integration with cloud providers.

2 types of provisioners:

- **membership provisioners** only care about a subject's membership.

- **account provisioners** care about subjects' attributes.
Account Provisioners

- Receive notifications from multiple event sources:
  - Grouper change log consumer
  - Entity Change Notifier (does not exist-- yet!)
Lafayette College – Grouper Pilot Provisioning Architecture V3
Grouper in Action at NYU

Jeff Pasch  
LMS Product Director

Madan Dorairaj  
Solutions Architect

Julio Macavilca  
Senior Application Developer, Identity Services
Current State

Grouper manages high level institutional groups

- Using loader jobs based on queries of identity registry database
- Affiliation, Division, former, recent, current
  - E.g. Former Student, Stern School of Business
  - E.g. Recent Faculty, NYU Abu Dhabi
  - E.g. Current Administrator, NYU IT

Grouper provides APIs to consume groups data

- Using loader jobs based on queries of identity registry database

Grouper syncs groups information to LDAP Groups

- Another way of providing groups information: using isMemberOf Attributes
  - E.g. In use by VPN service to require MFA for IT staff
Planned enhancements for Fall 2016

Self service groups management that support following functions

- Create and Manage Groups
- Search and View Groups
- Join and Unjoin Groups

Integration with end user applications

- Starting Linux Groups, possibly utilizing LDAP POSIX groups
- Extending the integration to File Management Systems
- Published APIs and Methods to consume Groups information by end-user applications
Sakai, Grouper, and Google
Keeping Memberships in Sync is the Key

Ability to create a Google Group based on membership of a Sakai course site and keep memberships in sync.
Workflow

Sakai

Sakai Groups Sync Process

Sakai groups table

Google Groups

Google Groups Change Log Consumer

Grouper

Grouper Loader

runs every min
	runs 2x every min
Google API Manager

Create a new project

- Create service account
  - Service account ID
  - Client ID key
- Project owner email
- Domain

Client ID scopes needed to be granted:

- admin.directory.user, admin.directory.group, apps.groups.settings
- OR custom role: read/create/update users and read/create/update/delete groups.
Adding the Google Provisioner

Download or clone from repo:
https://github.com/Internet2/grouper/tree/master/grouper-misc/googleapps-grouper-provisioner

With Maven, build the module and pull dependencies

Move the module (google-apps-provisioner-1.X.X-SNAPSHOT.jar) and the dependency jars to GROUPER_HOME/lib/custom directory
Grouper configurations

Loader job runs twice a minute looking for diffs

Update the Grouper Registry

Marking the groups

GoogleProvisioningHook.include.regex.1=^app.*classes.*.*(?<!_grouperupdaters)$

GoogleProvisioningHook.attributeDefName=etc:attribute:googleProvisioner:syncToGoogleNYUGoogleConsumer

Let’s provision

changeLog.consumer.NYUGoogleConsumer.quartzCron = 35 * * * * ?

Apply the default group settings

whoCanJoin=INVITED_CAN_JOIN
whoCanViewMembership=ALL_MEMBERS_CAN_VIEW
whoCanManage = update
handleDeletedGroup = archive
...
Syncing

Classes authoritative

- Will overwrite changes done to the Google side

Limit which Google Groups to compare during nightly full syncs

- changeLog.consumer.NYUGoogleConsumer.googleGroupFilter=^.*-(fa|ja|sp|su|wi)?([0-9]{2})-([0-9a-f]{4})$

Daily full syncs

- googleAppFullSync NYUGoogleConsumer --dry-run
Sakai data and loader job

Groups: group_name | group_description
apps:classes:sp16:04cb:catching-grouper-101 | lures and baits

Memberships: group_name | subject_id
apps:classes:sp16:04cb:catching-grouper-101 | ab123
apps:classes:sp16:04cb:catching-grouper-101 | cd456

Managers: group_name | subject_id
apps:classes:sp16:04cb:catching-grouper-101 | ef789
catching-grouper-101-sp16-04cb@nyu.edu
Monitoring

Full sync
Loader job
Google provisioning
Grouper daemon
Update Sakai with group status
Questions?
IAM Online Evaluation

Please complete a short evaluation of today’s presentation

August IAM Online
“Collaborative Infrastructure for Research
August 10, 2016

Kathleen Fitzpatrick – Modern Language Association
Scott Koranda – Laser Interferometer Gravity Observatory (LIGO)
Von Welch, Indiana University Center for Applied Cybersecurity Research
Christopher Whalen – National Institutes of Health
2016 Internet2 Technology Exchange

September 25-29, 2016
Miami, Florida

https://meetings.internet2.edu/2016-technology-exchange/

Base CAMP – for those new to the field
CAMP – Two tracks of case studies and solutions
Advance CAMP (ACAMP) – Unconference tackling community issues
InCommon Shibboleth Installation Workshop

October 27-28, 2016
California State University Office of the Chancellor
Long Beach, California

www.incommon.org/shibtraining