Three Campus Case Studies: Managing Access with Grouper

IAM Online – March 13, 2013

Speakers:
Paul Donahue and Keith Hazelton, University of Wisconsin-Madison
Sébastien Gagné, University of Montreal
Rahul Doshi and Michael Gettes, Carnegie Mellon University

Moderator:
Tom Barton, University of Chicago

Thank you to InCommon Affiliates for helping to make IAM Online possible.
Value of access management

• The more information gathered in a central system that’s relevant to access policies, the
  – lower the cost and time to deliver a new service
  – more useful to people with delegated authority

• The more services integrated with a central system, the
  – more consistent is user access across services
  – simpler is user access management
  – easier to know who can access what

• These are easier to achieve with a central system that
  – is highly integrative
  – supports delegation
Do these values *really* play out?

- Three Universities using Grouper
  - One not yet in production
  - One with initial use case recently in production
  - One has a good start, now looking at next push

- Case study framework
  - Problem being addressed
  - Functional or technical requirements: can Grouper meet them?
  - Specifics: sizes/metrics, naming, operational architecture
  - Questions for *you* whose answers might help *them*
Grouper @ Carnegie Mellon University

Rahul Doshi & Michael Gettes
March, 2013
1. Why grouper
2. Grouper deployment statistics
3. Grouper UI changes
4. Grouper use cases
5. Naming and other challenges
6. Future plans
Why CMU Chose Grouper

- Replacement for homegrown legacy system insufficient for future of CMU
- Grouper benefits
  - Actively supported
  - Grouper Web Services API
  - Also supports roles and permission mgmt along with managing institutional and personal groups (future)
  - Great flexibility designing solutions for Apps (composite, nested, group permissions)
  - Easy to customize UI
Grouper deployment

• Went in production Feb 2013
  - Memberships: 668,242
  - Groups: 2,342
  - Distinct Userids: 35,402
  - Folders: 206

• Operational design
  - Two servers behind load-balancer
  - MySQL cluster with master-slave replication
  - Scheduling of grouper-loader daemon and grouper loader jobs
  - Essential Monitoring - https://spaces.internet2.edu/x/nYbd
UI Customization

Stock Grouper UI

Less is more!

No Grouper Icon:
Not one small enough and higher resolution
UI Customization (2)

Stock Grouper UI

Can search with a list:
user1, user2, user3
Grouper Use Case

- Example: Google apps provisioning with Google Apps Directory Sync tool
  - We use grouper to manage user provisioning with GADS
  - Composite of includes minus excludes
  - GA team controls the includes and excludes
    - Static group used to carefully manage de-prov
  - Groups used to control sub-orgs – services
  - isMemberOf is key to making GADS work
  - CMU has complex migration plans to GA – Grouper’s flexibility made the job much easier
Grouper deployment

• Grouper Stem Hierarchy
  – Apps : GoogleApps : andrew.cmu.edu
  – Campus : Physical Locations : byCollection
    – Campus:Pittsburgh:ComputingServices
    – Campus:Qatar:byBuilding:Building1
  – Community : Logical Org : byCollection
    – Community:Department:ComputingServices
    – Community:Students:byClass:{Freshman,Soph,…}
  – People : userid : personalGroups
  – Courses : {cmu course structure}
    – Access control rules are extremely conservative
Future plans

• Grouper integration with person reg (CPR)
• OIM (11) Integration, via ActiveMQ
• ActiveMQ integration for app notification
• Active Directory (multiple Domains)
• Groups to Ext. Apps (Box, Google, etc)
• When “Groups Solved” – Permissions
• Challenges
  – Real-time prov to ldap for large groups (PSP)
  – Need to integrate Zenoss / Google Analytics
UNIVERSITY OF MONTREAL
GROUPER CASE STUDY

MARCH 13, 2013
Who am I

• Sébastien Gagné, IT analyst, main Grouper developer
• Background in software engineering and Java development
Grouper: First Contact

- UofM is replacing its legacy systems
  - PeopleSoft was selected for HR and academics management
  - Oracle Identity Manager (OIM) was selected for managing user accounts
  - Grouper was suggested to manage groups
Why Grouper instead of OIM?

- Lifecycle management
  - While OIM can create and delete group with connectors, managing the lifecycle is more complicated
- Quick and simple to deploy
  - OIM is complicated to deploy and customize, while Grouper would give results faster
  - Grouper was in production 6 months after initial testing
- Easier access to required data sources
- Long term plan to provide a dedicated group management tool
- Active development and community with similar fields (see the Grouper mailing lists at: http://www.internet2.edu/grouper/lists.html)
- It’s open source
- It worked
Initial Grouper deployment

- Deployed in December 2012
- Automated course and program group
  - Automatically created and populated with students based on their enrollments;
  - Custom group loader using the Grouper API;
  - Provisioned to the central Active Directory repository;
  - Managed by delegated administrator, if required.
Deployement diagram
Deployement highlights

• Linux virtual servers
  – 4 Gb of RAM (could use a little more)
  – 4 Gb used disk space (applications only)

• Oracle databases
  – 13 000 groups, 400 000 memberships
  – 16 Gb of data

• High availability
  – Physical load balancers
  – Active-active where possible (Grouper UI)
  – Active-passive otherwise
    (Grouper Daemon, AcadLoader job)
Logical data flows

Academic SQL Database

- Contains student courses and programs enrollment information.
  - MAT1011:
    - StudentA
    - StudentB

Active Directory (subject source)

- Group membership
- LDAP

Existing Applications

Academic SQL Database

- JDBC calls

RSP

Subject API

AD groups with the same members as Grouper:
- CN=H13_MAT1011,OU=acad,OU=grouper,OU=People,DC=umontreal,DC=ca

Members =
- StudentA
- StudentB
- AssistantC

... and the other static groups, as well as functional groups not managed by Grouper

Course-group with ad-hoc members:
- acad.mat.cours.H13_MAT1011
  - StudentA
  - StudentB
  - AssistantC

... and other static groups:
- acad.mat.mat-admin
- acad.mat.Others:mat-conf

Grouper

Grouper Registry

Grouper UI

Add/delete ad-hoc members to group H13_MAT1011

User
Data flows - description

• **AcadLoader**: custom java application that uses the standard Grouper Java API.
  – Creates and maintain the base folder structure
  – Configures the delegation rules

• **Static groups in Grouper**: are used for delegation privileges and to contain configuration attributes

• **PSP (Provisioning Service Provider)**: Grouper made module for real-time and bulk provisioning

• **Existing applications and policies** are already using AD for group membership so they keep doing so
Results in Grouper

- **Root folder**
  - Department folder
    - Admin group
    - Courses
    - Programs
    - Others
      - Configuration group
Delegation model

• Rule based
  – Applied to the folder
  – Defined in the custom loader

• Department admins can:
  – Update members in Courses and Programs
  – Create and admin groups in Others
  – Update members in admins

• Everyone can view groups
Impressions

• The good
  – Active and responsive community
  – It’s open source
  – Simple to deploy

• The bad
  – Grouper UI
  – Integration of the new attribute framework in the UI
  – Learning curve
Future development

• In development
  – Mail-enabling groups with Exchange

• Coming soon
  – Provisioning in multiple directories
  – Integration with OIM
Manifest – the Service Application

Manifest is our new service, with Grouper as its logic engine, to manage populations which are known to us and those which will be new to us. Manifest will enable administrators to provide service entitlements to groups.
Why Grouper?
Grouper: selection criteria

Number of requirements 129

Keith 92/71%
Unicon 100/78%

Most of the contrary responses have to do with workflow requirements and reporting requirements.

Grouper does not provide workflow.

Grouper provides access to its data logs for an external reporting agent.
Grouper: problem addressed

- Grouper will house the business rules, replacing views and code
- Exposing that logic in a simpler manner will help Middleware manage the complexity
- Campus consumers will get a better idea of what they are getting and how their data might be better tuned
- Campus consumers will become more engaged in the data that they receive
- The same goes for providing campus services to groups formed within Grouper
Manifest roadmap
Release 1.0
(Announced December 2012)

• Create a group
• Manage a group
• Add members to a group who have NetID, by email invitation or by directly entering their NetID into the application
• Add a SAML2 Entity ID to a group, enabling the group to control access to web applications using the NetID Login Service
Release 1.1
(Announced March 2013)

Ability for authorized groups to invite someone to join the group and make them eligible for a NetID if they don't already have one.
Release 2.0

(Expected Release late Spring 2013)

• Ability to place start and end dates on group memberships
• Enables shared enterprise services to register their service in Manifest
• Enables administrators to browse a menu of registered services/groups
• Provides a process for requesting a group’s access to a service
• Workflow has been uploaded to the wiki here
  https://spaces.internet2.edu/display/Grouper/University
  +of+Wisconsin+--+Madison+Grouper+Project+Page
Future 1/2

• A user interface that allows the management of service entitlements

• Ability to use federated or social identity in lieu of NetID while being a member of a group

• Composite groups, involving group math that uses Data Driven Groups (e.g., the entire student population or all classified staff) that have been loaded into Manifest from the campus Person Hub (a database that houses information about people, populated from various source systems on campus)

• Reports and audits
Future 2/2

- Attestation (auditing of account data to remove inactive or invalid users)
- Ability to use Manifest group data to provision campus applications
- Direct connection to departmental databases that contain person data
- Use Manifest to determine whether an authenticated user should have access to non-web applications/systems
- Self-service account linking (linking non-NetID accounts to a user’s NetID)
- For application developers: supplemental attribute delivery for display, application authorization, just in time provisioning, etc.
The Infrastructure
package MsnIAM

«component» SpecPop

Invitation APIs (JDBC)

Person APIs (JDBC)

«component» GroupSvcApp

Group WS methods

Privilege WS methods

Membership WS methods

Attribute WS methods (SOAP)

«component» Grouper 2.x

Resolve Subjects

Grouper Loader

Subject API (?)

Data-driven Groups

«component» PersonHub

Populate group info into Person Hub

PHExport (JDBC)

«component» Shib 2 IdP

Attribute Resolver

Person APIs (JDBC)

PersonHub APIs (JDBC)

Attribute Resolver

Data-driven Groups
Hosts

2 instances of Grouper, load balanced

Virtualized Oracle database
Name space

Visit

https://spaces.internet2.edu/display/Grouper/uw-madison+stem+and+group+naming+standards
Usage (March 8)

Grouper daily report

OVERALL:

- memberships: 2,622
- groups: 219
- members: 620
- folders: 60
- unresolvable subjects: 0
- bad memberships: 0

WITHIN LAST DAY:

- new memberships: 20
- new groups: 3
- updated groups: 0
- new folders: 0
Challenges

• Onboarding campus services so that they receive eligibility information from one place

• Loading Data Driven Groups into Grouper and maintaining that data

• Design and development of a User Interface that satisfies workflow requirements and invitations
Best practices

• Enroll in email lists  
  http://internet2.edu/grouper/lists.html

• Participate in wiki  
  https://spaces.internet2.edu/display/grouper/community+Contributions

• Engage governance bodies (WARG / IVG)

• For project health use tools like Jira and Wiki, with PM practices
Evaluation
Please complete the evaluation of today’s IAM Online:
http://www.surveymonkey.com/s/IAMOnline_March_2013

Next IAM Online – April 10, 2013 (3 pm ET)
Aligning Identity and Access Management with Your Information Security Program

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline
Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by Internet2’s InCommon, in cooperation with the EDUCAUSE Identity and Access Management Working Group