Open Apereo 2016
100% Open for Education

Grouper in Action
Access Management Strategies for Higher Education and Research

Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College
Jeff Pasch, New York University
Julio Mascavelca, New York University
Madan Dorairaj, New York University
1. **Introduction to Grouper**
   a. Grouper Overview
   b. Features and capabilities
   c. What’s new
2. **Grouper in Action**
   a. Access Policy and Reference Groups - Lafayette
   b. Grouper, Sakai, and Google - NYU
   c. Organizational Hierarchy and O365 - Penn
   d. Fine grained database permissions - Penn
3. **Hands on Grouper**
   a. Folder and grouper management
   b. Searching and adding subjects
   c. Direct vs indirect membership
   d. Grouper loader jobs
   e. Composite group
4. **Open Q&A**
Access management strategy

- Tools & processes to translate IAM concepts into typical campus environment
  - Which people?
  - What systems & business processes?
  - What policies?
  - What purposes?
  - Whose authority?
Why have an access management strategy?

• Lower cost and time to deliver a new service
• Simplify access management by using the same group in many places
• Empower the right people to manage access
• Answer who can access what
Access management stages:

Access management stages

2. Maintain access groups determined from systems of record
   - Courses, departments,…
   - Define service-specific access policies in the centralized access management system
Access management stages

3. Distributed management
   - Departmental applications
   - Ad-hoc teams
   - Exceptions
Access management stages

4. Increase integration
   • Direct integration with applications
   • Roles & privileges to support applications more deeply

For Math Department, while John works there
Grouper is...  

Grouper is an enterprise access management system designed for the highly distributed management environment and heterogeneous information technology environment common to Universities.

- Coordinated Collaboration
- Single Point of Control
- Distributed Management
The Grouper Story

• Mature, community driven project (2005 initial release)
• Internet2
• National Science Foundation (NSF) Grant No. OCI-0330626, OCI-0721896, and OCI-1032468
• Joint Information Systems Committee (JISC) (UK)
• University of Chicago, University of Pennsylvania, Duke University, University of Washington, University of Memphis, University of Bristol (UK)
The Grouper Story

• Key aims
  • Delegation and distributed management
  • Integration with most any existing Identity Management infrastructure
The Grouper Story

• Grouper v2.X expanded beyond groups
  • Roles & permissions

• Rules

- If removed from group A
- then remove from group B
"We view TIER as a coordinated approach to enable trust and identity in education and research at scale for thousands of institutions and service providers while also satisfying diverse local use cases."

—Ron Kraemer, Vice President and CIDO, University of Notre Dame

“It’s not just about federation, it’s about enabling high-value collaboration across thousands of disciplines and millions of people. Hence agreement on attribute and authorization management, application integration, administration procedures,…”

— RL ‘Bob’ Morgan
Grouper™

- Delegation
- Rules
- Subjects
- Change Log
- Policy
- Audit

- Provisioning Service Provider
- Subject API
- LDAP/AD
- Person Registry
- Systems of Record
- Grouper Loader
- Web UI
- Grouper Shell

- Groups, Roles and Permissions
- Grouper Admin

* PSP connectors may be needed
Grouper Concepts

- Folders in hierarchies
- Group
- Direct members
- Subgroup
- Indirect members
- Composite groups
Security and Delegation

- Create groups
- Create subfolders
- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out
Access management lifecycle support

- Membership start & end times (optional)
- Move or copy folders, groups, etc
- User audit
- Point in time audit
- Rules
Auditing

• “User audit” will audit who does what
• Point-In-Time auditing will keep track of the history of the repository
  • Who was in this group at a point in time (or time range) in the past
  • Who are all the people who have been in this group
  • What groups was this person in at a point in the past (or time range)
Grouper loader

- Daemon that periodically syncs external sources with Grouper
- Can work for groups or permissions (e.g. org chart)
- SQL or LDAP sources
- Grouper admins can configure jobs based on attributes
Beyond groups...

- Attributes
- Roles
- Permissions

- Attribute definition
- Permission definition

Role inheritance
Delegation model extends that for Groups
Ad-hoc Collaboration Communities
Creates various groups in Grouper

Create/View tool sets

For course use

For non-course use

Name: Test Community

Example WordPress url:
https://sites.duke.edu/adhoc_test_community

Example Duke Mailing list address:
adhoc-test-community@duke.edu

Create
## Tool Set for Test Community

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat Room</td>
<td>A private Jabber chat room</td>
</tr>
<tr>
<td>Email Messaging</td>
<td>Email list using Sympa</td>
</tr>
<tr>
<td>Other</td>
<td>Placeholder to allow non-Toolkit resources to share activities</td>
</tr>
<tr>
<td>Quad</td>
<td>Quad is currently a Pilot project</td>
</tr>
<tr>
<td>Sakai</td>
<td>A learning management system</td>
</tr>
<tr>
<td>Virtual Computer Lab Access</td>
<td>VCL makes it possible to run lab software without visiting the lab in person</td>
</tr>
</tbody>
</table>
Groups and Roles for: Test Community

Use the links on this page to add or remove anyone with a Duke NetID from your course tool set. You can also add and remove guests with a Yahoo, Gmail or AOL email address. Once you add members to a group in Toolkits and set their roles, those members and their permissions are duplicated across all applications you open up to the community. Note that officially registered students, TAs, and instructors are automatically included in the appropriate groups and do not need to be added by hand.

Add Person with a Duke NetID  Add a Guest  Batch add users

All (1)  Admin (1)

What do these roles mean?

<table>
<thead>
<tr>
<th>Name</th>
<th>NetID</th>
<th>Role</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shilen Patel</td>
<td>shilen</td>
<td>Admin</td>
<td>Edit</td>
</tr>
<tr>
<td>Group</td>
<td>Chat Room</td>
<td>Wiki</td>
<td>WebFiles Space</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>-----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Instructor</td>
<td>Owner</td>
<td>View, Modify, Comment, Admin</td>
<td>owner</td>
</tr>
<tr>
<td>Manager/TA</td>
<td>Admin</td>
<td>View, Modify, Comment, Admin</td>
<td>Read/Write /Delete</td>
</tr>
<tr>
<td>Developer</td>
<td>Participant</td>
<td>View, Modify, Comment</td>
<td>Read/Write /Delete</td>
</tr>
<tr>
<td>Mentor</td>
<td>Participant</td>
<td>View, Modify, Comment</td>
<td>Read/Write</td>
</tr>
<tr>
<td>Student</td>
<td>Participant</td>
<td>View, Modify, Comment</td>
<td>Read/Write</td>
</tr>
<tr>
<td>Visitor/Auditor</td>
<td>Participant</td>
<td>View</td>
<td>Read</td>
</tr>
</tbody>
</table>
Open Apereo 2016
100% Open for Education

Grouper - What’s new?
Release 2.3.0 new features

- Grouper Loader improvements including scheduling configuration to facilitate high-availability changes and handling unresolvable subjects
- New Web Service operations for attribute definitions, actions, and messaging
Release 2.3.0 new features (continued)

- Grouper messaging system with integration to the change log and ESB
- UI screens for attribute definitions and inherited privileges
- Export to GSH - allows export of Grouper objects to a Grouper Shell (GSH) script
- Folder privileges have been changed to be "admin" and "create" instead of "stem" and "create"
- TIER API "hasMember" operation implemented in the Grouper web services module to support integration and interoperability. Well, this is already out of date
Release 2.3.0 - provisioning

• Provisioning Service Provider Next Generation (PSPNG)
  • Simplify configuration
  • Increase performance

• 2.3.0 Provisioning targets
  • LDAP groups
  • Active Directory groups
  • LDAP attributes (entitlements)

• Other features:
  • Incremental and full refresh
  • Group selection: by folder or group, or both
  • Higher-level and higher-performance programming API
Grouper roadmap

- TIER packaging (continued)
- Revise building and package management (continued)
- UI
  - incorporate more rules
  - wizards for configuration
  - support attributes / permissions / etc
- PSPNG refinements
- Upgrade vt-ldap to ldaptive
- Improve GSH
- TIER SCIM API
- Grouper instrumentation
Provisioning opportunities (post 2.3.0)

- Grouper messaging
- Automated integration tests
- Deprovisioning safety nets
- More targets: suggestions?
Grouper roadmap schedule

• Grouper 2.4 in Q1 2017
• This release is time based, not feature based, so not exactly sure what will be in it, will know more at TechEx
• We will be spending time supporting 2.3 in the near term and then focusing on 2.4
• We would like to do yearly major releases in the spring
• Minor releases we are not sure
  • If they don’t take a lot of time maybe quarterly
  • Maybe snapshot releases that include patches?
• Patches as needed
Upcoming event

IAM online

• IAM Webinar Wed. July 13 2016 at 2pm ET (Grouper stories)
Grouper - Access Policy and Reference Groups @ Lafayette College
Open Apereo 2016
100% Open for Education

Grouper - Grouper, Sakai, and Google @ NYU
Grouper - Organizational hierarchy in Grouper at Penn
Grouper @ Penn

- Used Grouper centrally at Penn
- 120k groups
- 2.7 million immediate memberships
- 10k permission assignments
- Heavily delegated
Organizational hierarchy at Penn

- Penn uses a loader job to sync organizational chart
- SQL warehouse has:
  - Orgs with people
  - Org rollups
- Loader job to load the orgs with people
- Loader job to load the rollups
- Includes / excludes
- Wiki document
Example org

EXPLORE

Browse groups hierarchy

You can look for groups throughout the hierarchy. (You might not be able to see some groups if you lack appropriate privileges.)

Browse or list groups

Current location is:


- 5600 - Law

Search groups

Advanced groups search

Search groups
# Org loader configuration

<table>
<thead>
<tr>
<th>Types</th>
<th>Description and Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>grouperLoader</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderAndGroups</td>
<td>grouper</td>
</tr>
<tr>
<td>grouperLoaderDbName</td>
<td>select olpmv.GROUP_NAME as group_name, olpmv.GROUP_DISPLAY_NAME as group_display_name, olpmv.READERS, olpmv.VIEWERS, olpmv.ORG_ID from ORG_LOADER_PERSON_META_V olpmv</td>
</tr>
<tr>
<td>grouperLoaderGroupQuery</td>
<td>penncommunity:employee:org:%_personorg</td>
</tr>
<tr>
<td>grouperLoaderGroupTypes</td>
<td>0 46 6 * * ?</td>
</tr>
<tr>
<td>grouperLoaderGroupsLike</td>
<td>crontab</td>
</tr>
<tr>
<td>grouperLoaderIntervalSeconds</td>
<td>SQL_GROUP_LIST</td>
</tr>
<tr>
<td>grouperLoaderPriority</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderQuartzCron</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderQuery</td>
<td>select group_name, subject_id from org_loader_person_v</td>
</tr>
<tr>
<td>grouperLoaderScheduleType</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderType</td>
<td></td>
</tr>
</tbody>
</table>

---

*Note: The image contains a table with various configuration settings for an org loader.*
Old org structure in org name


When we had a re-org and apps broke we changed this
Orgs as groups
Org rollup structure

The following table lists all entities which are members of this group.

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>🤷‍♂️ 5600 - Law</td>
<td>Direct</td>
</tr>
<tr>
<td>🤷‍♂️ 5601 - Law School Deans Office</td>
<td>Direct</td>
</tr>
<tr>
<td>🤷‍♂️ 5602 - Biddle Law Library</td>
<td>Direct</td>
</tr>
<tr>
<td>🤷‍♂️ 5603 - Information Technology Services</td>
<td>Direct</td>
</tr>
</tbody>
</table>
Using organizational hierarchy in apps

• Create an app group
• Add the organizational group(s) to app group
• App group could be include/exclude or all other additions
O365 needs the organization for billing

- O365 needs the sponsoring organization / division
- Person could be in more than one organization
- Use the primary org code
- Allow an org override
- Do not allow multiple overrides
- Admins have access to read/write various orgs or rollups
O365 overrides original solution

- Admins would use Grouper UI to manage override group
- Create if not exist
- Have READ/UPDATE privileges on org override groups or by group to rollup
- Problems
  - Users might not have correct access
  - Steps to use the Grouper UI to inspect/assign orgs
  - Don’t know if there is another org assigned
  - Daily process to pick up changes
O365 overrides final solution

- Application using the Grouper WS to manage better
- Shows the overrides in a table for orgs/divs
- Tells the user there are multiple overrides for a user without showing data they are not allowed to see
- Kicks off process to provision user to FIM
- Allows assignments to org rollups for easier management
- Leverages Grouper groups/privileges
O365 overrides final solution

- Application using the Grouper WS to manage better
- Shows the overrides in a table for orgs/divs
- Tells the user there are multiple overrides for a user without showing data they are not allowed to see
- Kicks off process to provision user to FIM
- Allows assignments to org rollups for easier management
- Leverages Grouper groups/privileges
O365 privileges on org in Grouper (test env)

The following table lists all entities with privileges in this group.

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Admin</th>
<th>Read</th>
<th>Update</th>
<th>OptIn</th>
<th>OptOut</th>
<th>Attribute read</th>
<th>Attribute update</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bryan W Hopkins</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lisa Joann Campeau</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Colleen Cawley</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Charles Gervase Harvey</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Chris Hyzer</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Manage org overrides screen

Employee organization and student division overrides

Readable employee organizations: 2793  Show organizations
Readable student divisions: 48  Show divisions
Writable employee organizations: 2793  Show organizations
Writable student divisions: 48  Show divisions

O365 FAQ

Override a student division or employee organization

<table>
<thead>
<tr>
<th>Person</th>
<th>Charles Gervase Harvey (harveycg, 10754302) (active) Staff - Isc-applications &amp; Informa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee organization or student division</td>
<td>Employee organization  Student division</td>
</tr>
<tr>
<td>Employee organization</td>
<td>School of Arts and Sciences - 0234 - Fels Administration</td>
</tr>
</tbody>
</table>

Submit

<table>
<thead>
<tr>
<th>Action</th>
<th>Pennid</th>
<th>Pennkey</th>
<th>Name</th>
<th>Type</th>
<th>Org or div</th>
<th>Center or school</th>
<th>Org or div description</th>
<th>Center or school description</th>
<th>Errors and v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>10021368</td>
<td>mchyer</td>
<td>Chris Hyzer</td>
<td>Org</td>
<td>1912</td>
<td>19</td>
<td>Annenberg Center Rental Sales</td>
<td>Annenberg Center For Performing Arts</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2016, University of Pennsylvania. All rights reserved.
Privacy information
Manage org overrides screen logic

- Global context cache of objects (few minutes)
- When user logs in, look in membership cache to get memberships and privileges
- Expand privileges to be indirect by org
- Of the memberships in overrides, filter the ones the user can READ
- In drop down for orgs/divs, only show results that the user can UPDATE
- Make sure everything ok and give error message to right of result
Open Apereo 2016
100% Open for Education

Grouper - Fine grained database permissions
Use case description

- Personal user data stored in SQL DB
- Applications across the University need to access the data
- Principle of least privilege at a row and column level
- User information (test data set):
  - PersonID
  - NetID
  - First and last name
  - Email address
  - Phone numbers
- SQL access will take place with different schemas per application
Use case description (continued)

- Only need read-only access managed, but for this example, let’s manage READ/WRITE

- Student billing web app
  - Schema: FASTDEV2
  - IDs (read-only)
  - Name (read/write)
  - Student rows

- Fac/staff file sharing app
  - Schema: FASTDEV3
  - IDs (read-only)
  - Name (read-only)
  - Contact info (read/write)
  - Faculty/staff rows

- Oracle
## Sample data

<table>
<thead>
<tr>
<th>ID</th>
<th>PersonID</th>
<th>NetID</th>
<th>First</th>
<th>Last</th>
<th>Email</th>
<th>Work#</th>
<th>Home#</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>12345</td>
<td>js</td>
<td>John</td>
<td>Smith</td>
<td><a href="mailto:js@a.edu">js@a.edu</a></td>
<td>3-1234</td>
<td>123-4567</td>
</tr>
<tr>
<td>B4</td>
<td>98765</td>
<td>sd</td>
<td>Sara</td>
<td>Davis</td>
<td><a href="mailto:sd@a.edu">sd@a.edu</a></td>
<td>5-2345</td>
<td>234-5678</td>
</tr>
<tr>
<td>C5</td>
<td>54321</td>
<td>rj</td>
<td>Ryan</td>
<td>Jones</td>
<td><a href="mailto:rj@a.edu">rj@a.edu</a></td>
<td>7-4567</td>
<td>345-6789</td>
</tr>
<tr>
<td>T7</td>
<td>56789</td>
<td>jc</td>
<td>Julia</td>
<td>Clark</td>
<td><a href="mailto:jc@a.edu">jc@a.edu</a></td>
<td>9-6789</td>
<td>456-7890</td>
</tr>
</tbody>
</table>

* Students

* Faculty
<table>
<thead>
<tr>
<th>ID</th>
<th>PersonID</th>
<th>NetID</th>
<th>First</th>
<th>Last</th>
<th>Email</th>
<th>Work#</th>
<th>Home#</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>12345</td>
<td>js</td>
<td>John</td>
<td>Smith</td>
<td><a href="mailto:js@a.edu">js@a.edu</a></td>
<td>3-1234</td>
<td>123-4567</td>
</tr>
<tr>
<td>B4</td>
<td>98765</td>
<td>sd</td>
<td>Sara</td>
<td>Davis</td>
<td><a href="mailto:sd@a.edu">sd@a.edu</a></td>
<td>5-2345</td>
<td>234-5678</td>
</tr>
<tr>
<td>C5</td>
<td>54321</td>
<td>rj</td>
<td>Ryan</td>
<td>Jones</td>
<td><a href="mailto:rj@a.edu">rj@a.edu</a></td>
<td>7-4567</td>
<td>345-6789</td>
</tr>
<tr>
<td>T7</td>
<td>56789</td>
<td>jc</td>
<td>Julia</td>
<td>Clark</td>
<td><a href="mailto:jc@a.edu">jc@a.edu</a></td>
<td>9-6789</td>
<td>456-7890</td>
</tr>
</tbody>
</table>

**Students**

**Faculty**
Browse groups hierarchy

You can look for groups throughout the hierarchy. (You might not be able to see some groups if you lack appropriate privileges.)

Browse or list groups

Current location is:

Root: fgac: apps: secureUserData: schemas

Showing 1-2 of 2 items

FASTDEV2
FASTDEV3
Architecture

- One table in Oracle with personal user information
- Secure the table with Oracle FGAC (Fine grained access control) / VPD (Virtual private database)
- Security data needs to be replicated from Grouper to Oracle for performance reasons
- Store memberships for rows and permissions for schemas in Grouper
- Access request workflow with Kuali Rice edoclite / Grouper
- Note: a schema in Oracle is the connecting DB user
Setup on Grouper demo server: affiliations

- Normally these would be available in Grouper as loader jobs
- They are not on the Grouper demo server, so add
Setup: row level groups

- Create the application folder, and organize subfolders
- Add the community groups as members
Setup: row/column level permission definition

- Permission definition has configuration and security

<table>
<thead>
<tr>
<th>Attribute definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folder</strong></td>
</tr>
<tr>
<td><strong>UUID</strong></td>
</tr>
<tr>
<td><strong>ID</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Multi-assignable</strong></td>
</tr>
<tr>
<td><strong>Value type</strong></td>
</tr>
<tr>
<td><strong>Multi-valued</strong></td>
</tr>
</tbody>
</table>

**Assign to**

- Attribute definition
- Folder
- Group
- Member
- Membership
- Membership - immediate only

**Assign privileges to everyone**

- admin
- update
- read
- view
- optin
- optout
Setup read/write action for this permission def

- Include an “all” which implies read and write
- Note: this is specific to this one permission definition, and does not affect other permissions in Grouper
Setup permission name for each set of columns
Setup column permission name inheritance

Attribute name graph

Attribute name: fgac:apps:secureUserData:permissions:columns:columns_all

Diagram showing the relationships between different attribute names:
- columns_all
- columns_name
- columns_contact
- columns_ids
Setup permission name for each group of rows

<table>
<thead>
<tr>
<th>Attribute definition</th>
<th>fgac:apps:secureUserData:permissions:rowOrColumnPermissionDef</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>fgac: apps: secureUserData: permissions: rows:</td>
</tr>
<tr>
<td>UUID</td>
<td>1ca4e93a33b441cbbb3392cf6798a3ed</td>
</tr>
<tr>
<td>ID</td>
<td>rows_fgacStudents</td>
</tr>
<tr>
<td>ID Path</td>
<td>fgac:apps:secureUserData:permissions:rows:rows_fgacStudents</td>
</tr>
<tr>
<td>Name</td>
<td>rows_fgacStudents</td>
</tr>
<tr>
<td>Description</td>
<td>represents the rows of student data</td>
</tr>
</tbody>
</table>
Setup row permission name inheritance
Assign the permissions

<table>
<thead>
<tr>
<th>Permission type:</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission definition:</td>
<td>fgac:apps:secureUserData:permissions:rowOrColumnPermissionDef</td>
</tr>
<tr>
<td>Permission resource:</td>
<td></td>
</tr>
<tr>
<td>Role:</td>
<td></td>
</tr>
<tr>
<td>Entity:</td>
<td></td>
</tr>
<tr>
<td>Action:</td>
<td></td>
</tr>
<tr>
<td>Enabled / disabled:</td>
<td>Enabled only</td>
</tr>
</tbody>
</table>

Assignments

<table>
<thead>
<tr>
<th>Entity</th>
<th>Resource</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV2</td>
<td>columns_ids</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV2</td>
<td>columns_name</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV2</td>
<td>rows_fgacStudents</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV3</td>
<td>columns_contact</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV3</td>
<td>columns_ids</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV3</td>
<td>columns_name</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:schemas:FASTDEV3</td>
<td>rows_fgacFacultyAndStaff</td>
<td>all: ☐, read: ✔, write: ✔</td>
</tr>
</tbody>
</table>
Setup: insert sample data
Table: SECUREUSERDATA_USER

<table>
<thead>
<tr>
<th>ID</th>
<th>PERSONID</th>
<th>NETID</th>
<th>FIRST_NAME</th>
<th>LAST_NAME</th>
<th>EMAIL</th>
<th>WORK_PHONE</th>
<th>HOME_PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>12345</td>
<td>js</td>
<td>John</td>
<td>Smith</td>
<td><a href="mailto:js@a.edu">js@a.edu</a></td>
<td>3-1234</td>
<td>123-4567</td>
</tr>
<tr>
<td>B4</td>
<td>98765</td>
<td>sd</td>
<td>Sara</td>
<td>Davis</td>
<td><a href="mailto:sd@a.edu">sd@a.edu</a></td>
<td>5-2345</td>
<td>234-5678</td>
</tr>
<tr>
<td>C5</td>
<td>54321</td>
<td>rj</td>
<td>Ryan</td>
<td>Jones</td>
<td><a href="mailto:rj@a.edu">rj@a.edu</a></td>
<td>7-4567</td>
<td>345-6789</td>
</tr>
<tr>
<td>T7</td>
<td>56789</td>
<td>jc</td>
<td>Julia</td>
<td>Clark</td>
<td><a href="mailto:jc@a.edu">jc@a.edu</a></td>
<td>9-6789</td>
<td>456-7890</td>
</tr>
</tbody>
</table>
Setup: groups without members represent schemas
Full sync Grouper to Oracle security tables

1. WS select

2. SQL select

3. SQL insert/delete
Run the full sync Java program

- Code in SVN:
  
  http://anonsvn.internet2.edusvn/i2mi/trunk/grouper-misc/poc_secureUserData/

```
C:\mchyzer\grouper\trunk\poc_secureUserData>java -cp conf;lib\grouperClient.jar; 
lib\log4j.jar;lib\ojdbc14.jar;dist\secureUserData.jar edu.internet2.middleware.poc_secureUserData.SudFullSync
  - Del 1 mships of group: fgacAlumni
  - Del 1 mships of group: fgacStudents, personid: 98766
  - Add mship for group: fgacStudents, personid: 12345
  - Add mship for group: fgacStudents, personid: 98765
  - Del 1 row perm miss schema: FASTDEV2, action: read, group: fgacAlumni
  - Del 1 row perm miss schema: FASTDEV4, action: write, group: fgacStudents
  - Del 1 col perm miss schema: FASTDEV4, action: read, cols: name
  - Del 1 col perm miss schema: FASTDEV2, action: read, cols: ssn
  - Add row perm miss schema: FASTDEV2, action: write, group: fgacStudents
  - Add row perm miss schema: FASTDEV2, action: read, group: fgacStudents
  - Add col perm miss schema: FASTDEV3, action: read, cols: name
  - Add col perm miss schema: FASTDEV2, action: read, cols: ids
  - Add col perm miss schema: FASTDEV2, action: read, cols: contact
```

*
Local cache of security tables and memberships

- **SECUREUSERDATA_MEMBERSHIPS**
  
<table>
<thead>
<tr>
<th>ID</th>
<th>PERSONID</th>
<th>GROUP_EXTENSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2SI0523</td>
<td>56789</td>
<td>fgacFacultyAndStaff</td>
</tr>
<tr>
<td>Q2SI8046</td>
<td>54321</td>
<td>fgacFacultyAndStaff</td>
</tr>
<tr>
<td>Q2SJGOZ2</td>
<td>98765</td>
<td>fgacStudents</td>
</tr>
<tr>
<td>Q2SJGOZ1</td>
<td>12345</td>
<td>fgacStudents</td>
</tr>
<tr>
<td>Q2SI3U8P</td>
<td>98765</td>
<td>fgacFacultyAndStaff</td>
</tr>
</tbody>
</table>

- **SECUREUSERDATA_ROW_PERMİSS**
  
<table>
<thead>
<tr>
<th>ID</th>
<th>GROUP_EXTENSION</th>
<th>SCHEMA_NAME</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2SI805A</td>
<td>fgacFacultyAndStaff</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
<tr>
<td>Q2SI8049</td>
<td>fgacFacultyAndStaff</td>
<td>FASTDEV3</td>
<td>write</td>
</tr>
<tr>
<td>Q2SJGOZ4</td>
<td>fgacStudents</td>
<td>FASTDEV2</td>
<td>read</td>
</tr>
<tr>
<td>Q2SJGOZ3</td>
<td>fgacStudents</td>
<td>FASTDEV2</td>
<td>write</td>
</tr>
</tbody>
</table>

- **SECUREUSERDATA_COL_PERMİSS**
  
<table>
<thead>
<tr>
<th>ID</th>
<th>COLSET</th>
<th>SCHEMA_NAME</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2SI805C</td>
<td>name</td>
<td>FASTDEV2</td>
<td>read</td>
</tr>
<tr>
<td>Q2SJGOZ7</td>
<td>contact</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
<tr>
<td>Q2SJ6B1</td>
<td>name</td>
<td>FASTDEV2</td>
<td>write</td>
</tr>
<tr>
<td>Q2SJ6B2</td>
<td>contact</td>
<td>FASTDEV3</td>
<td>write</td>
</tr>
<tr>
<td>Q2SJGOZ5</td>
<td>name</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
<tr>
<td>Q2SJGOZ6</td>
<td>ids</td>
<td>FASTDEV2</td>
<td>read</td>
</tr>
<tr>
<td>Q2R69VNA</td>
<td>ids</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
</tbody>
</table>
Oracle FGAC/VPD/RLS

- Oracle Fine Grained Access Control (FGAC) aka: Virtual Private Database (VPD)
  - A way to apply a virtual (hidden to the user) “where clause” to limit rows (Row Level Security (RLS))
  - A way to null-out columns in a way that is hidden to the user
  - Based on schema, or if trusted schema, data in the context

- Note: this part does not have to be FGAC, you could use a view with functions, or something else…
  - With Oracle, FGAC is supposed to perform better than a view with functions
Run a PL/SQL function that appends a predicate to the query based on the schema or data in context. Can restrict insert/update/deletes. Predicate joins to SUD security tables from Grouper.
Oracle FGAC (continued)

- For performance, cache security in the connection context (similar to ThreadLocal)
  - Only cache for a certain amount of time (5 minutes?)
  - Can cache on connect trigger, or on demand
    - “on demand” might be better if users connect to the DB for things unrelated to the FGAC
  - Cache who the user is, when cache was created, if can read/write all rows, which column sets can read/write
Oracle FGAC queries from owner schema: all data

- Note: there is a short circuit, if owner schema, allow access

```sql
select * from FASTDEV1.SECUREUSERDATA_USER
```
Oracle FGAC queries from student billing application: sees students and no contact info

```sql
select * from FASTDEV1.SECUREUSERDATA_USER
```

<table>
<thead>
<tr>
<th>ID</th>
<th>PERSONID</th>
<th>NETID</th>
<th>FIRST_NAME</th>
<th>LAST_NAME</th>
<th>EMAIL</th>
<th>WORK_PHONE</th>
<th>HOME_PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>12345</td>
<td>js</td>
<td>John</td>
<td>Smith</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B4</td>
<td>98765</td>
<td>sd</td>
<td>Sara</td>
<td>Davis</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Oracle FGAC queries from student billing application: can update name, not ids.
Oracle FGAC queries from faculty/staff file sharing application: sees fac/staff and all columns

```sql
select * from FASTDEV1.SECUREUSERDATA_USER
```

<table>
<thead>
<tr>
<th>ID</th>
<th>PERSONID</th>
<th>NETID</th>
<th>FIRST_NAME</th>
<th>LAST_NAME</th>
<th>EMAIL</th>
<th>WORK_PHONE</th>
<th>HOME_PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4</td>
<td>98765</td>
<td>sd</td>
<td>Sara</td>
<td>Davis</td>
<td><a href="mailto:sd@a.edu">sd@a.edu</a></td>
<td>5-2345</td>
<td>234-5678</td>
</tr>
<tr>
<td>C5</td>
<td>54321</td>
<td>rj</td>
<td>Ryan</td>
<td>Jones</td>
<td><a href="mailto:rj@a.edu">rj@a.edu</a></td>
<td>7-4567</td>
<td>345-6789</td>
</tr>
<tr>
<td>T7</td>
<td>56789</td>
<td>jc</td>
<td>Julia</td>
<td>Clark</td>
<td><a href="mailto:jc@a.edu">jc@a.edu</a></td>
<td>9-6789</td>
<td>456-7890</td>
</tr>
</tbody>
</table>
Real-time row membership notification demo

- Start the real time XMPP listener:

```
C:\mchyer\grouper\trunk\poc_secureUserData\java -cp conf;lib\*;dist\secureUserData.jar edu.internet2.middleware.poc_secureUserData.SudRealTime
```

- Less than 1 minute after Grouper change, XMPP message goes from Grouper to SUD real time logic
- Note, it is configured to only send/receive relevant messages

```
(1:01:00 AM) PennGroups: <sudChangeLogMessage><changeType>rowGroupChange</changeType><rowGroupExtension>fgacStudents</rowGroupExtension><rowSubjectId>54321</rowSubjectId></sudChangeLogMessage>
```

- See the listener process the message

```
C:\mchyer\grouper\trunk\poc_secureUserData\java -cp conf;lib\*;dist\secureUserData.jar edu.internet2.middleware.poc_secureUserData.SudRealTime
- Add mship for group: fgacStudents, personid: 54321
```
Real-time row membership notification demo

- See that Ryan is now a student, select users from fastdev2 (student application)
Open Apereo 2016
100% Open for Education

Grouper - Hands on exercises
Create new folder

New folder

Create in this folder: Root
Enter a folder name or search for a folder where you are allowed to create new folders.
Enter 'Root' for the top level folder

Folder name: test
Name is the label that identifies this folder, and might change.

Folder ID: test
ID is the unique identifier for this folder. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description:
Description contains notes about the folder, which could include: what the folder represents, why it was created, etc.

Save  Cancel
New group

Create in this folder: test
Enter a folder name or search for a folder where you are allowed to create new groups.

Group name: test_group
Name is the label that identifies this group, and might change.

Group ID: test_group
ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description: A test group
Description contains notes about the group, which could include: what the group represents, why it was created, etc.

Show advanced properties

Save  Cancel
The following table lists all entities which are members of this group.

<table>
<thead>
<tr>
<th>Filter for</th>
<th>All members</th>
<th>Member name</th>
<th>Apply filter</th>
<th>Reset</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Show: 50
**Member name or ID:** affiliations:student

Enter an entity name or ID, or search for an entity.

**Assign these privileges:**
- Default privileges
- Custom privileges

Add or import a list of members.

A test group

The following table lists all entities which are members of this group.

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob Anderson</td>
<td>Direct</td>
</tr>
</tbody>
</table>

Filter for: All members  
Member name

Remove selected members

Showing 1-1 of 1 - First | Prev | Next | Last
A test group

The following table lists all entities which are members of this group.

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann Gasper</td>
<td>Direct, Indirect</td>
</tr>
<tr>
<td>Bob Anderson</td>
<td>Direct</td>
</tr>
<tr>
<td>student</td>
<td>Direct</td>
</tr>
</tbody>
</table>

Filter for: Has direct membership

Remove selected members

Show: 50

Showing 1-3 of 3 · First | Prev | Next | Last
Ann Gasper is a member of the test_group group by the following paths:

Ann Gasper is a direct member of

- test:test_group

Ann Gasper is a direct member of

- affiliations:student system of record
  - which is a direct member of
    - affiliations:student system of record and includes
      - which is a composite factor minus student excludes of
        - affiliations:student
          - which is a direct member of
            - test:test_group
**test_group**

**Member name or ID:** Ann Brown
Enter an entity name or ID, or search for an entity.

**Assign these privileges:**
- [ ] MEMBER
- [x] ADMIN
- [ ] UPDATE
- [x] READ
- [ ] VIEW
- [ ] OPTIN
- [ ] OPTOUT
- [ ] ATTRIBUTE READ
- [ ] ATTRIBUTE UPDATE

[Add] or import a list of members.

---

**A test group**

**More**

[Members] [Privileges] [More]

---

The following table lists all entities with privileges in this group.

**Filter for:**

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Apply filter</th>
<th>Reset</th>
<th>Advanced</th>
</tr>
</thead>
</table>

**Update:**

Assign the ADMIN privilege [Update selected]

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Admin</th>
<th>Read</th>
<th>Update</th>
<th>Optin</th>
<th>OptOut</th>
<th>Attribute read</th>
<th>Attribute update</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob Anderson</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

[Show: 50] (Showing 1-1 of 1)  [First]  [Prev]  [Next]  [Last]
The following table lists all entities with privileges in this group.

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Admin</th>
<th>Read</th>
<th>Update</th>
<th>OptIn</th>
<th>OptOut</th>
<th>Attribute read</th>
<th>Attribute update</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann Brown</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bob Anderson</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Show: 50
## Edit group

**Current location is:**  
Root: test: all_the_anms

<table>
<thead>
<tr>
<th>Name</th>
<th>all_the_anms</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>all_the_anms</td>
</tr>
<tr>
<td>Alternate ID Path</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

**Assign privileges to everyone**  
- [ ] Read  
- [ ] View  
- [ ] Optin  
- [ ] Optout  
- [ ] Attribute read

**Select group types**  
- [ ] addIncludeExclude  
- [x] grouperLoader  
- [ ] requireInGroups

[Save]  
[Back to group summary]
select SIS_COURSES.uid as subject_id from SIS_COURSES
where givenName = "Ann"
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>all_the_anns</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Path</strong></td>
<td>test:all_the_anns</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>all_the_anns</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>all_the_anns</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>test:all_the_anns</td>
</tr>
<tr>
<td><strong>Alternate ID Path</strong></td>
<td></td>
</tr>
<tr>
<td><strong>UUID</strong></td>
<td>d8d464b45a8e4526a054ac2608312837</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Types</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>grouperLoader</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderAndGroups</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderDbName</td>
<td>grouper</td>
</tr>
<tr>
<td>grouperLoaderGroupQuery</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderGroupTypes</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderGroupsLike</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderIntervalSeconds</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderPriority</td>
<td></td>
</tr>
<tr>
<td>grouperLoaderQuartzCron</td>
<td>0 0 * * * ?</td>
</tr>
<tr>
<td>grouperLoaderQuery</td>
<td>select SIS_COURSES.uid as subject_id from SIS_COURSES where givenName = &quot;Ann&quot;</td>
</tr>
<tr>
<td>grouperLoaderScheduleType</td>
<td>CRON</td>
</tr>
<tr>
<td>grouperLoaderType</td>
<td>SQL_SIMPLE</td>
</tr>
</tbody>
</table>
The following table lists all entities which are members of this group.

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann Anderson</td>
<td>Direct</td>
</tr>
<tr>
<td>Ann Anderson</td>
<td>Direct</td>
</tr>
<tr>
<td>Ann Brown</td>
<td>Direct</td>
</tr>
<tr>
<td>Ann Brown</td>
<td>Direct</td>
</tr>
<tr>
<td>Ann Clark</td>
<td>Direct</td>
</tr>
<tr>
<td>Ann Doe</td>
<td>Direct</td>
</tr>
</tbody>
</table>

Options:
- Add to my favorites
- Join group
- Copy group
- Delete group
- Edit group
- Edit composite
- Move group
- Export members
- Import members
- Remove all members
- View audit log
- Run loader process to sync group
- Schedule loader process
- Admin UI
New group

Create in this folder: test
Enter a folder name or **search for a folder where you are allowed to create new groups.**

Group name: employee_Anns
Name is the label that identifies this group, and might change.

Group ID: employee_Anns
ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description:
Description contains notes about the group, which could include: what the group represents, why it was created, etc.

Show advanced properties ▼

Save  Cancel
employee_Anns

The following table lists all entities which are members of this group.

Filter for: All members  Member name

Remove selected members

Entity name  Membership

Show: 50

More actions:
- Add to my favorites
- Join group
- Copy group
- Delete group
- Edit group
- Edit composite
- Move group
- Export members
- Import members
- Remove all members
- View audit log
- Admin UI
**employee_Anns**

*Edit group composite*

**Composite:**
- No
- Yes

**First factor group:**
- affiliations:staff

Enter a group name or ID, or search for the first factor.

**Operation:**
- and (intersection)

There are three composite operations: intersection, complement, and union.

- **Intersection** means members of the overall group must be in both factor groups. **Intersection** is used for example when requiring members to be active employees.

- **Complement** means members are in the first group but not in the second group. **Complement** is used for exclude lists.

- **Union** is not needed, you can just add the groups as members of the overall group.

**Second factor group:**
- test:all_the_anms

Enter a group name or ID, or search for the second factor.

[Save] [Cancel]
The following table lists all entities which are members of this group.

Note: this group is a composite owner: 👤 employee_Anns is a composite intersection of 👤 staff and 👤 all_the_anns

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann Langenberg</td>
<td>Indirect</td>
</tr>
<tr>
<td>Ann Smith</td>
<td>Indirect</td>
</tr>
</tbody>
</table>
Apereo 2016 Grouper Sessions

Exploring Internet2 Grouper & NIST RBAC/ABAC
Time: May 25, 2016, 10:45 AM - 11:30 AM
Location: KC 907
Misagh Moayyed - Software Engineer, Unicon
Bill Thompson - Lafayette College

Scriptable Grouper - Lafayette College's Big Fish Story
Title: Scriptable Grouper - Lafayette College's Big Fish Story
Time: May 24, 2016, 3:00 PM - 3:45 PM
Location: KC 907
Carl Waldbieser - Lafayette College
Thanks!

Further information:

Infosheets, mail lists, wiki, downloads, etc: 
www.internet2.edu/grouper

Grouper demo server:
https://grouperdemo.internet2.edu/