IAM Online

Get Schooled on Grouper 2.0
Wednesday, September 14, 2011 – 3 p.m. ET

Tom Barton, University of Chicago
Chris Hyzer, University of Pennsylvania

Please note: you will not hear any audio until the session begins

IAM Online is brought to you by InCommon, in cooperation with Internet2 and the EDUCAUSE Identity and Access Management Working Group
Outline

• Grouper and the access management story
• Brief tour of Grouper’s access management capabilities
• An access management problem and its solution using Grouper v2.0
• Grouper Survey results
Grouper Story

• Open source, community-driven project of the Internet2 Middleware Initiative
  • Initial release v0.5 in December 2004
• Grouper originally focused on robust management of groups, emphasizing:
  • Delegation and distributed management
  • Integration with most any existing IdM infrastructure. See case studies and campus contributions at: https://spaces.internet2.edu/display/Grouper/Community+Contributions
• Grouper v2.0 provides broader set of access management capabilities, including roles & permissions
  • Released 6 September 2011
Access management is a process: making authZ more than authN

- Start out using a single user attribute, affiliation, in LDAP or AD to let applications implement access policies
- Enrich centralized access management using groups determined from systems of record
  - Courses, financial accounts, departments
  - Define service specific access in central IAM system
- Get central IT out of the loop
  - Distributed management
  - Exceptions
  - Departmental apps
- Increase integration of access management
  - Direct application integration with web services
  - ESB/SOA, REST/SOAP
  - Roles & privileges to support applications more deeply
Grouper: core concepts

Folders in hierarchies

Group

Direct members

Subgroup

Indirect members

\[ \text{Composite groups} \]

\[ \bigcap \]

\[ \text{Group} \]

\[ \text{Direct members} \]

\[ \text{Subgroup} \]

\[ \text{Indirect members} \]

\[ \text{Composite groups} \]
Security & delegation in Grouper

- Create groups
- Create subfolders
- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation
Beyond groups

Attributes
Roles
Permissions

Attribute definition
Permission definition

Role inheritance

Delegation model extends that for Groups
Access management lifecycle support

- Membership start & end times (optional)
- Move or copy folders, groups, etc
- User audit
- Point in time audit
- Rules
## New and Improved in Grouper v2.0

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rules</strong></td>
<td>Execute built-in actions and expression language to add business logic to Grouper actions</td>
</tr>
<tr>
<td><strong>Attribute and Permissions UIs</strong></td>
<td>Ajax-y UIs to define, view, and assign attributes and permissions</td>
</tr>
<tr>
<td><strong>Permission Disallow</strong></td>
<td>To manage inheritance of permissions via Role, Resource, or Action hierarchies</td>
</tr>
<tr>
<td><strong>Permission Limits</strong></td>
<td>Built-in Policy Decision Point that combines run-time context with permissions to produce Allow/Deny</td>
</tr>
<tr>
<td><strong>Point in Time Audit</strong></td>
<td>Query Grouper’s state at a previous time</td>
</tr>
<tr>
<td><strong>External Subjects</strong></td>
<td>Invitation processes leverage federation to let external Subjects be given group memberships and permissions</td>
</tr>
<tr>
<td><strong>Syncing Groupers</strong></td>
<td>Federate groups between two Groupers</td>
</tr>
<tr>
<td><strong>Member Search &amp; Sort</strong></td>
<td>Selective Subject attribute caching for improved sorting and searching capability and speed</td>
</tr>
<tr>
<td><strong>LdappcNG enhancement</strong></td>
<td>Improved performance through caching</td>
</tr>
</tbody>
</table>
Upcoming in Grouper v2.1 & v2.2

• LdappcNG real-time and incremental provisioning
  • v2.1
  • Q4 2011

• New Ajax-y UI
  • v2.2
  • Q2 2012
IAM Online Grouper Permissions

- Use case description
- Architecture
- Permissions setup
- Oracle Fine Grained Access Control
- Demo
- Real-time provisioning
- Workflow
- Note: all code in slide notes and SVN (viewVC)
- Note: youtube demo (part 1) (part 2)
- Note: presentation and notes here (google “grouper documents”, though not OLD one)
Use case description

- From Penn State, also needed at University of PA
- 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
- This service is called SecureUserDate (SUD)
Use case description (continued)

- PSU and UP 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**
IAM Online - Grouper Permissions

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
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
Grouper demo server

- Publicly accessible server that runs various versions of Grouper for demo purposes
- Grouper demo server: [https://grouperdemo.internet2.edu/](https://grouperdemo.internet2.edu/)
- [Grouper demo wiki](https://spaces.internet2.edu/x/OoEaAQ)
- You can [register an InCommon login ID](https://grouperdemo.internet2.edu/)

9/14/11
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>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folder</strong></td>
<td>fagc: apps: secureUserData: permissions:</td>
</tr>
<tr>
<td><strong>UUID</strong></td>
<td>963bd02023bc492a99993c0c81ca219</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>rowOrColumnPermissionDef</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Permission</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>row or column permission for the Secure User Data application</td>
</tr>
<tr>
<td><strong>Multi-assignable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Value type</strong></td>
<td>No value</td>
</tr>
<tr>
<td><strong>Multi-valued</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Assign to</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attribute definition</td>
</tr>
<tr>
<td></td>
<td>Folder</td>
</tr>
<tr>
<td></td>
<td>Group</td>
</tr>
<tr>
<td></td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Membership</td>
</tr>
<tr>
<td></td>
<td>Membership - immediate only</td>
</tr>
<tr>
<td><strong>Assign privileges to everyone</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>
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
IAM Online - Grouper Permissions

Setup permission name for each set of columns

Find an attribute definition name

<table>
<thead>
<tr>
<th>Attribute definition</th>
<th>Enter search text to find an attribute definition to filter by</th>
</tr>
</thead>
</table>

Attribute name

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Enter search text to find an attribute name to edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>:permissions:columns</td>
<td></td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:columns:columns_all</td>
<td></td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:columns:columns_contact</td>
<td></td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:columns:columns_ids</td>
<td></td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:columns:columns_name</td>
<td></td>
</tr>
</tbody>
</table>

Attribute name

| Attribute definition | fgac:apps:secureUserData:permissions:rowOrColumnPermissionDef | |
| Folder | fgac: | apps: | secureUserData: | permissions: | columns: | |
| UUID | 58e3436a7dbe47ae8d0ec114ce5a6138 | |
| ID | columns_contact | |
| ID Path | fgac:apps:secureUserData:permissions:columns:columns_contact | |
| Name | columns_contact | |
| Description | Contact information for the user (email, phone, etc) | |
Setup column permission name inheritance
Setup permission name for each group of rows

<table>
<thead>
<tr>
<th>Attribute definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rows:rows</td>
<td>represents the rows of student data</td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:rows:rows_all</td>
<td></td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:rows:rows_fgacFacultyAndStaff</td>
<td></td>
</tr>
<tr>
<td>fgac:apps:secureUserData:permissions:rows:rows_fgacStudents</td>
<td></td>
</tr>
<tr>
<td>9ca4e93a33b441cbb3392cf6798a3ed</td>
<td></td>
</tr>
<tr>
<td>rows_fgacStudents</td>
<td></td>
</tr>
<tr>
<td>ID Path</td>
<td></td>
</tr>
<tr>
<td>Name ** rows_fgacStudents</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

**Attribute definition**
- rows:rows
- fgac:apps:secureUserData:permissions:rowOrColumnPermissionDef
- fgac:apps:secureUserData:permissions:rows:rows_fgacFacultyAndStaff
- fgac:apps:secureUserData:permissions:rows:rows_fgacStudents
- 9ca4e93a33b441cbb3392cf6798a3ed
- rows_fgacStudents

**Folder**
- fgac: apps: secureUserData: permissions: rows:

**UUID**
- 1ca4e93a33b441cbb3392cf6798a3ed

**ID**
- rows_fgacStudents

**ID Path**
- fgac: apps: secureUserData: permissions: rows: rows_fgacStudents

**Name**
- rows_fgacStudents
Setup row permission name inheritance

Attribute name graph

| Attribute name | fgac:apps:secureUserData:permissions:rows:rows_all |

rows_all

rows_fgacFacultyAndStaff

rows_fgacStudents
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>Role:</td>
</tr>
<tr>
<td></td>
<td>Entity:</td>
</tr>
<tr>
<td></td>
<td>Action:</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:secureUser: fastestdev2</td>
<td>columns_ids</td>
<td>all read write</td>
</tr>
<tr>
<td>fgac:apps:secureUser: fastestdev2</td>
<td>columns_name</td>
<td>all read write</td>
</tr>
<tr>
<td>fgac:apps:secureUser: fastestdev2</td>
<td>rows_fgacStudents</td>
<td>all read write</td>
</tr>
<tr>
<td>fgac:apps:secureUser: fastestdev3</td>
<td>columns_contact</td>
<td>all read write</td>
</tr>
<tr>
<td>fgac:apps:secureUser: fastestdev3</td>
<td>columns_ids</td>
<td>all read write</td>
</tr>
<tr>
<td>fgac:apps:secureUser: fastestdev3</td>
<td>columns_name</td>
<td>all read write</td>
</tr>
<tr>
<td>fgac:apps:secureUser: fastestdev3</td>
<td>rows_fgacFacultyAndStaff</td>
<td>all read write</td>
</tr>
</tbody>
</table>

9/14/11
## 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>
IAM Online - Grouper Permissions

Setup: enable client subject for WS

Current location is: Grouper Administration: webServiceClientUsers

Name: webServiceClientUsers
Path: Grouper Administration: webServiceClientUsers
Description: users allowed to log in to the UI

Advanced features

Add member
Enter search text to find a member to add

Add member

Membership list

Showing group members: 1-4 of 4  page size: 50

Sort by: Name

- jdbc - remoteUser - remoteUser
- GrouperSysAdmin
- secureUserData_client
- test1 ws client

9/14/11
IAM Online - Grouper Permissions

Setup: privileges for grouperClientSubject (e.g.)

Attribute definition privileges

Add search text to find an entity to add to the list

Add entity to list

Indirect privileges

Show indirect privileges due to group memberships

Showing privilege entities: 1-2 of 2

<table>
<thead>
<tr>
<th>Admin</th>
<th>Read</th>
<th>Update</th>
<th>Optin</th>
<th>Optout</th>
<th>View</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>[unverifiedInfo] Chris Hyzer - Protect Network [externalUserID] mchy</td>
</tr>
<tr>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>secureUserData_client</td>
</tr>
</tbody>
</table>

Cancel  Save

9/14/11  30
Setup: groups without members represent schemas

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
Full sync Grouper to Oracle security tables

1. SUD sync logic
   - WS select

2. SQL select

3. SQL insert/delete

Grouper ➔ SUD sync logic ➔ Oracle
Run the full sync Java program

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

```
C:\mchyzer\grouper\trunk\poc_secureUserData>java -cp conf;lib\grouperClient.jar;lib\log4j.jar;lib\ojjdbc14.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 permiss schema: FASTDEV2, action: read, group: fgacAlumni
- Del 1 row permiss schema: FASTDEV4, action: write, group: fgacStudents
- Del 1 col permiss schema: FASTDEV4, action: read, cols: name
- Del 1 col permiss schema: FASTDEV2, action: read, cols: ssn
- Add row permiss schema: FASTDEV2, action: write, group: fgacStudents
- Add row permiss schema: FASTDEV2, action: read, group: fgacStudents
- Add col permiss schema: FASTDEV3, action: read, cols: name
- Add col permiss schema: FASTDEV2, action: read, cols: ids
- Add col permiss schema: FASTDEV3, action: read, cols: contact
```
IAM Online - Grouper Permissions

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>Q2S10S23</td>
<td>56709</td>
<td>fgacFacultyAndStaff</td>
</tr>
<tr>
<td>Q2S18046</td>
<td>54321</td>
<td>fgacFacultyAndStaff</td>
</tr>
<tr>
<td>Q2S1GO22</td>
<td>98765</td>
<td>fgacStudents</td>
</tr>
<tr>
<td>Q2S1GO21</td>
<td>12345</td>
<td>fgacStudents</td>
</tr>
<tr>
<td>Q2S13U8P</td>
<td>98765</td>
<td>fgacFacultyAndStaff</td>
</tr>
</tbody>
</table>

- **SECUREUSERDATA_ROW_PERMISS**

<table>
<thead>
<tr>
<th>ID</th>
<th>GROUP_EXTENSION</th>
<th>SCHEMA_NAME</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2S1005A</td>
<td>fgacFacultyAndStaff</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
<tr>
<td>Q2S18049</td>
<td>fgacFacultyAndStaff</td>
<td>FASTDEV3</td>
<td>write</td>
</tr>
<tr>
<td>Q2S1GO24</td>
<td>fgacStudents</td>
<td>FASTDEV2</td>
<td>read</td>
</tr>
<tr>
<td>Q2S1GO23</td>
<td>fgacStudents</td>
<td>FASTDEV2</td>
<td>write</td>
</tr>
</tbody>
</table>

- **SECUREUSERDATA_COL_PERMISS**

<table>
<thead>
<tr>
<th>ID</th>
<th>COLSET</th>
<th>SCHEMA_NAME</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2S1BO5C</td>
<td>name</td>
<td>FASTDEV2</td>
<td>read</td>
</tr>
<tr>
<td>Q2S1GO27</td>
<td>contact</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
<tr>
<td>Q2S168B1</td>
<td>name</td>
<td>FASTDEV2</td>
<td>write</td>
</tr>
<tr>
<td>Q2S168B2</td>
<td>contact</td>
<td>FASTDEV3</td>
<td>write</td>
</tr>
<tr>
<td>Q2S1GO25</td>
<td>name</td>
<td>FASTDEV3</td>
<td>read</td>
</tr>
<tr>
<td>Q2S1GO26</td>
<td>ids</td>
<td>FASTDEV2</td>
<td>read</td>
</tr>
<tr>
<td>Q2R69V3A</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
Application schemas accessing FGAC’ed data

SchemaX accesses data

1. Query on FGAC’ed table/view

Filtered results

2. 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

3. Oracle

SchemaY

FGAC
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 (continued)

- Designate an Oracle package to hold the FGAC code
  - Full code in slide notes

```sql
-- expire context every X minutes to get up to date security information
c_seconds_contextExpires constant number := 60*1;

PROCEDURE show_context;

PROCEDURE set_context_if_needed;

PROCEDURE set_context_backdoor(as_schema varchar2);

FUNCTION userdata_select_rows_predicate (schema_in VARCHAR2,
name_in VARCHAR2) RETURN VARCHAR2;

FUNCTION user_schema RETURN VARCHAR2;

FUNCTION userdata_update_rows_predicate (schema_in VARCHAR2,
name_in VARCHAR2) RETURN VARCHAR2;

FUNCTION userdata_select_cols_ids (schema_in VARCHAR2,
name_in VARCHAR2) RETURN VARCHAR2;
```
Oracle FGAC row predicate

- Two functions are where clause predicates relating to the query: one for select, one for update

```sql
return ' personid in (select sm.personid ' || ' from fastdev1.secureuserdata_memberships sm, ' || ' fastdev1.secureuserdata_row_permss srp ' || ' where sm.group_extension = srp.group_extension ' || ' and srp.action = ' 'read' ' || ' and srp.schema_name = fastdev1.secureuserdata_fgac_pkg.user_schema() ) ';
end;
```

- Six functions are “where clause” predicates relating to the

```sql
allowed := SYS_CONTEXT (c_context,c_col_prefix || 'read_ids');
if (allowed = 'T') then
    return '1=1';
end if;
return '1=0';
end;
```
Oracle FGAC (continued)

- Assign the policies to table
- Here is an example of 1 of the 8 policies (full code in slide notes)

```sql
BEGIN
  dbms_rls.add_policy (object_schema => 'FASTDEV1',
                      object_name => 'secureuserdata_user',
                      policy_name => 'sud_fgac_update_rows',
                      function_schema => 'FASTDEV1',
                      policy_function => 'secureuserdata_fgac_pkg.userdata_update_rows_predicate',
                      statement_types => 'UPDATE',
                      update_check => TRUE,
                      policy_type => dbms_rls.DYNAMIC
  );
END;
/
```
Oracle FGAC queries from owner schema: all data

- Note: there is a short circuit, if owner schema, allow access
Oracle FGAC queries from student billing application: sees students and no contact info

```
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

```
update FASTDEV1.SECUREUSERDATA_USER set personid = 'abc' where id = 'A3'
```

0 rows updated

```
update FASTDEV1.SECUREUSERDATA_USER set first_name = 'James' where id = 'A3'
```

1 row updated
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>
Oracle FGAC queries from faculty/staff file sharing application: can update contact info, not name

update FASTDEV1.SECUREUSERDATA_USER set email = 'sarad@a.edu' where id = 'B4';

1 row updated

update FASTDEV1.SECUREUSERDATA_USER set first_name = 'Susan' where id = 'B4';

0 rows updated
Add a requirement: read-only access of file sharing application to student rows. Assign in Grouper

- Kick off the sync’ ing app, or wait for cron
Add a requirement (continued). See rows in Oracle

```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><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>

```sql
update FASTDEV1.SECUREUSERDATA_USER set email = 'john@a.edu' where id = 'A3'
```

Commit is OFF

Execute/compile statement at caret

9/14/11
Real-time row membership notification

1. Student or staff group membership changes

Grouper

2. XMPP XML message with group and subjectId

SUD real-time logic

3. Check Grouper and Oracle for membership

Oracle

4. Insert or delete membership in cached table (if needed)
Real-time row membership notification demo

- Add Ryan Jones as a student
- Note: in reality the student system and loader will do this

### Current location is:
- Agac:
- Community:
- Students

<table>
<thead>
<tr>
<th>Name</th>
<th>students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>fgac:community:students</td>
</tr>
<tr>
<td>Description</td>
<td>students in the fgac use case</td>
</tr>
</tbody>
</table>

### Add member
Enter search text to find a member to add

- Ryan Jones

### Membership list

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Smith</td>
<td></td>
</tr>
<tr>
<td>Ryan Jones</td>
<td></td>
</tr>
<tr>
<td>Sara Davis</td>
<td></td>
</tr>
</tbody>
</table>

Showing group members: 1-3 of 3  page 1

9/14/11
Real-time row membership notification demo

- Start the real time XMPP listener:

```
C:\mchyzer\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

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

- See the listener process the message

```
C:\mchyzer\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)
Real-time permission notification

1. Relevant permission or role assignment

2. XMPP XML message to refresh all permissions

3. Check Grouper and Oracle for permissions

4. Insert or delete permission diffs in cached table

Grouper → WS → SUD real-time logic → SQL → Oracle
Real-time permission notification demo

- Allow file sharing app to read student data

### Assign new permission

<table>
<thead>
<tr>
<th>Permission definition:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission resource:</td>
<td>✓ fgac.apps:secureUserData:permissions:rows:rows_fgacStudents</td>
</tr>
<tr>
<td>Role:</td>
<td>✓ fgac.apps:secureUserData.roles:user</td>
</tr>
<tr>
<td>Entity:</td>
<td>✓ fgac.apps:secureUserData:schemas:FASTDEV3</td>
</tr>
<tr>
<td>Action:</td>
<td>✓ read</td>
</tr>
<tr>
<td>Allowed:</td>
<td>✓ Allow</td>
</tr>
</tbody>
</table>

### Permissions Table

<table>
<thead>
<tr>
<th>role</th>
<th>Entity</th>
<th>Resource</th>
<th>all</th>
<th>read</th>
<th>write</th>
</tr>
</thead>
<tbody>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV2</td>
<td>columns_ids</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV2</td>
<td>columns_name</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV2</td>
<td>rows_fgacStudents</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV3</td>
<td>columns_contact</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV3</td>
<td>columns_ids</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV3</td>
<td>columns_name</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV3</td>
<td>rows_fgacFacultyAndStaff</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>fgac: apps:secureUserData: schemas:FASTDEV3</td>
<td>rows_fgacStudents</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

9/14/11
Real-time permission notification demo

- The listener was already started

- 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

See the listener process the message
Access request workflow

- Penn will use its Kuali Rice eDocLite with a template like this
- Can auto-provision, though needs some work for allow/disallow and schema entity creation
Access request workflow mockup (continued)

Column permissions

![Assignment](New assignment) ![Action](All) ![Columns](All) ![Allowed](T)

Assignment: Remove assignment ![Action](Read) ![Columns](ID's) ![Allowed](F)

More column permissions

Individuals requesting access to the University's administrative data must indicate their acceptance of the following statement:

As an individual whose position requires interaction with any or all of the University's administrative information systems, I may be provided with direct access to confidential and valuable data and/or use of data systems. In the interest of maintaining the integrity of these systems and of ensuring the security and privacy of University resources, I will maintain the confidentiality of my password for all systems to which I have access. I will maintain in strictest confidence the data to which I have access. Any confidential information will not be shared in any manner with others who are unauthorized to view such data. I will use my access to the systems for the sole purpose of conducting official business of the University. I understand that the use of these systems and their data for personal purposes is prohibited. I understand that any abuse of access to the University's systems and their data, any illegal use of copying of software, any misuse of the University equipment may result in disciplinary action, loss of access to the University's systems, and possible sanctions consistent with the University Policy on Adherence to University Policy.

I will abide by this policy

Supervisor Action:

For Supervisor use only. Please select the appropriate School/Center Access Administrator from the list.

School/Center Access Administrator

Form Routing:

To add a comment to your request or approval action, enter it in the Note field provided and click the Save button. Click the appropriate button (submit, approve, disapprove, etc.) to submit the form for continued processing in the workflow.
Access request workflow

1. Requestor: Fills out eForm
2. Supervisor: Approves
3. Senior BA: Approves
4. Central IT: Approves, creates schema
5. EDocLite: Grants/revokes permissions
6. WS
7. XMPP
8. SQL

Oracle

SUD real-time logic

Grouper

FGAC
Questions?
Grouper Survey

- Late June – early July 2011

<table>
<thead>
<tr>
<th>Stage</th>
<th>Respondents (121)</th>
<th>Identified Respondents (69)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>37</td>
<td>24</td>
</tr>
<tr>
<td>Deploying</td>
<td>20</td>
<td>13</td>
</tr>
<tr>
<td>Evaluating</td>
<td>40</td>
<td>21</td>
</tr>
</tbody>
</table>

- International adoption: 4 continents
- Healthy pipeline of new adopters
### Some takeaways

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong community</td>
<td>Integration architecture works: more than 30 applications</td>
</tr>
<tr>
<td></td>
<td>mentioned by respondents</td>
</tr>
<tr>
<td></td>
<td>Comprehensive, multi-featured</td>
</tr>
<tr>
<td>Weaknesses</td>
<td>Admin UI isn’t suited to non-technical users</td>
</tr>
<tr>
<td></td>
<td>Documentation wiki needs improvement</td>
</tr>
<tr>
<td>Adoption Obstacles</td>
<td>LDAP provisioning connector lacks real-time incremental</td>
</tr>
<tr>
<td></td>
<td>capability</td>
</tr>
</tbody>
</table>

- v2.0: wiki improvements begun
- v2.1: real time & incremental LDAP provisioning
- v2.2: new Ajax-y UI
Participate in the Community

- MACE-Paccman access management use case library
  https://spaces.internet2.edu/display/macepaccman/Use+Cases

- Join the Grouper-Users list --- let us know about your requirements and experiences
  http://www.internet2.edu/grouper/lists.html

- Share your Grouper deployment and integration experiences with the community:
  https://spaces.internet2.edu/display/Grouper/Community+Contributions
Evaluation
Please complete the evaluation of today’s IAM Online. You can also use this as a place to suggest future Grouper webinar topics.
www.surveymonkey.com/s/IAMOnline_Sept2011

Upcoming Events

Internet2 Fall Member Meeting
October 3-6, 2011 - Raleigh North Carolina
http://events.internet2.edu/2011/fall-mm/

Shibboleth Workshop Series: Installation of IdP and SP
November 7-8, 2011 – California State University Chancellor’s Office, Long Beach, Calif. (open to anyone)
www.incommon.org/educate/shibboleth
Next IAM Online
Wednesday, October 12, 2011 – 3 p.m. EDT

Governance of Identity and Access Management at Institutions of Higher Education

Brendan Bellina, University of Southern California
Matthew Dalton, Ohio University

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.