Introduction to Grouper

Tom Barton
University of Chicago and Internet2
Outline

• Access management: WUWT?
• Grouper story
• Grouper basics
• An example
• New & improved in latest & upcoming releases
Identity & Access Management (IAM)

- Identity
  - You
- Authentication
  - Log in
- Authorization
  - What you can do
- Access management
  - Map policy & authority to authorization
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 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
Access management stages: authorization > authentication

1. Start out using a single user attribute, affiliation, in LDAP or Active Directory. This lets services implement simple access policies.
Access management stages: authorization > authentication

2. 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

3. Get central IT out of the loop
   - Distributed management
   - Exceptions
   - Departmental applications

Math Faculty Group + Math Support Group → can access Math Faculty Resources
Access management stages: authorization > authentication

4. Increase integration of access management
   - Direct integration with applications using web services
     - SOAP/REST/ESB
   - Roles & privileges to support applications more deeply

For Math Department, while John works there
The Grouper Story

• Open source, community-driven project of the Internet2 Middleware Initiative
  • Initial release v0.5 in December 2004
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
Contributing organizations, so far

- Brown University
- California Polytech
- Cardiff University
- Campus Crusade for Christ International
- Cornell University
- Duke University
- Freie Universität Berlin
- GIP RECIA
- LIGO
- Newcastle University

- Northern Arizona University
- Ohio State University
- SURFnet
- University of Bristol
- University of Chicago
- University of Kansas
- University of Memphis
- University of Pennsylvania
- University of Washington
- University of West Bohemia

April 2012
Latest addition to the community

• Unicon offers IT Services for Education, Specializing in Open Source
  • Cooperative Support Program for Grouper, Shibboleth, CAS, uPortal, uMobile, Sakai
  • Annual subscription, 4 levels, provides access to and funds dedicated support team who work directly with the open source projects
Grouper: core concepts

Folders in hierarchies
- Group
  - Direct members
  - Subgroup
    - Indirect members
  - = \{ \text{Direct members} \cap \text{Subgroup members} \}

Composite groups
Security & delegation

- 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
Tom Barton’s UChicago group memberships

My memberships

To find groups in which you are a member, you can:
- Browse the groups hierarchy
- List your groups
- Search for groups by name

Showing 1-50 of 145 items

1. Grouper Administration:Wheel Group
2. The University of Chicago:Applications:aams:Create ChicagoID
3. The University of Chicago:Applications:aams:roles:trusted
4. The University of Chicago:Applications:Bulkmail:Recipients:All Recipient Groups
5. The University of Chicago:Applications:Bulkmail:Recipients:Students:All Students
6. The University of Chicago:Applications:Bulkmail:Recipients:Students:Graduate Students
7. The University of Chicago:Applications:Bulkmail:Recipients:Students:Undergraduate Students
8. The University of Chicago:Applications:Bulkmail:users
10. The University of Chicago:Applications:Bulkmail:Users:4
11. The University of Chicago:Applications:Bulkmail:Users:Bulkmail Users
12. The University of Chicago:Applications:Business Objects Enterprise:rf:users
13. The University of Chicago:Applications:Chalk:Authorized
14. The University of Chicago:Applications:Chalk:Eligible Factor
15. The University of Chicago:Applications:CityRyde:authorized
16. The University of Chicago:Applications:CityRyde:Eligible Factor
17. The University of Chicago:Applications:Cmail:users:authorized
18. The University of Chicago:Applications:Cmail:users:eligible_factor
Memberships become LDAP attributes

dn: uid=tbarton,ou=people,dc=uchicago,dc=edu
ucismemberof: uc:org:nsit:integration:techag
ucismemberof: uc:org:nsit:srdirs
ucismemberof: uc:applications:confluence:NSIT:esx
ucismemberof: uc:applications:confluence:NSIT:Directors
ucismemberof: uc:org:nsit:staff
ucismemberof: uc:applications:bulkmail:users
ucismemberof: uc:org:library:gnet:admins
ucismemberof: uc:applications:gnetid:admins
ucismemberof: uc:applications:wireless:authorized
ucismemberof: uc:applications:cmail:users:authorized
ucismemberof: uc:reference:affiliations:effective:staff
UChicago VPN simple delegation example

Different groups, different authorities
VPN only uses “vpn:authorized”
### UChicago applications managed by Grouper, so far

<table>
<thead>
<tr>
<th>aams</th>
<th>im</th>
<th>Service Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Astra</td>
<td>isx</td>
<td>sharepoint</td>
</tr>
<tr>
<td>Bulkmail</td>
<td>IT Ecosystem</td>
<td>shibboleth</td>
</tr>
<tr>
<td>Business Objects Enterprise</td>
<td>LDAP</td>
<td>statements</td>
</tr>
<tr>
<td>Chalk</td>
<td>lists</td>
<td>portlet</td>
</tr>
<tr>
<td>CityRyde</td>
<td>Mail Forwarding</td>
<td>SVN</td>
</tr>
<tr>
<td>Cmail</td>
<td>Mail Quarantine</td>
<td>tank</td>
</tr>
<tr>
<td>cnet</td>
<td>Microsoft Exchange</td>
<td>unifiedcomm</td>
</tr>
<tr>
<td>Confluence</td>
<td>modem pool</td>
<td>versions</td>
</tr>
<tr>
<td>Directory Administration</td>
<td>monitoring</td>
<td>virtualization</td>
</tr>
<tr>
<td>dmca</td>
<td>myUChicago</td>
<td>voip</td>
</tr>
<tr>
<td>Facilities SIMS</td>
<td>Non-po</td>
<td>vpn</td>
</tr>
<tr>
<td>gnetid</td>
<td>Onecard</td>
<td>web hosting</td>
</tr>
<tr>
<td>grouper</td>
<td>online directory</td>
<td>webproxy</td>
</tr>
<tr>
<td></td>
<td>password expiration</td>
<td>webshare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>webspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wireless</td>
</tr>
</tbody>
</table>
## New & improved in Grouper v2.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real-time provisioning</strong></td>
<td>Changes to user access can now happen in real time based on Grouper's changelog. This is accomplished with the new <strong>Provisioning Service Provider (PSP)</strong>, which replaces LDAPPCNG.</td>
</tr>
<tr>
<td><strong>Provision from LDAP/AD</strong></td>
<td>Update Grouper from LDAP or AD via PSP or Grouper Loader.</td>
</tr>
<tr>
<td><strong>More Web Services</strong></td>
<td>Improved support for applications that outsource their internal access management to Grouper.</td>
</tr>
<tr>
<td><strong>Local Entities</strong></td>
<td>Manage access by service principals to info stored in Grouper.</td>
</tr>
<tr>
<td><strong>Grouper Installer</strong></td>
<td>It's quick and easy to get started using Grouper with the new installer. Really!</td>
</tr>
<tr>
<td><strong>Subject Filter and Attribute Decorator</strong></td>
<td>Manage who can see which subject attributes and how they are displayed.</td>
</tr>
<tr>
<td><strong>Grouper Failover Client</strong></td>
<td>Higher availability of web services using a new failover client library and discovery service library.</td>
</tr>
</tbody>
</table>
## Roadmap – v2.2 (2012Q4 – 2013Q1)

<table>
<thead>
<tr>
<th>Release</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2</td>
<td>New Grouper UI</td>
<td>Provide new UI capabilities that better meet community needs.</td>
</tr>
<tr>
<td>2.2</td>
<td>Services in Grouper</td>
<td>Tag objects in Grouper so that folders, groups, permissions can be associated with a &quot;service&quot; to make it easier for users to perform tasks in Grouper.</td>
</tr>
<tr>
<td>2.2</td>
<td>Improved Grouper configuration</td>
<td>Make Grouper more easily deployable and upgradeable across environments with cascaded config files and expression language in config file entries.</td>
</tr>
<tr>
<td>On-going</td>
<td>Grouper Core</td>
<td>Continue adding capabilities to meet requirements from the field.</td>
</tr>
<tr>
<td>On-going</td>
<td>Community contributions</td>
<td>Solicit and publicize community contributions of extensions and complements to Grouper.</td>
</tr>
</tbody>
</table>
## Roadmap – not yet assigned to a release

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy attribute migration</td>
<td>Migrate legacy attributes into the new attribute framework.</td>
</tr>
<tr>
<td>Further KIM-Grouper integration</td>
<td>Work cooperatively within the OSIdM4HE activity (real name TBA) to refine the Kuali Identity Management services interfaces and extend existing integration beyond group-level into roles &amp; permissions.</td>
</tr>
<tr>
<td>Register for notifications</td>
<td>Add ability for users to register to be notified of changes to specified objects.</td>
</tr>
<tr>
<td>Unix GID management</td>
<td>Built-in support for managing unix GIDs.</td>
</tr>
<tr>
<td>COmanage integration</td>
<td>Work cooperatively with the COmanage project to integrate Grouper within COmanage.</td>
</tr>
<tr>
<td>Further uPortal-Grouper integration</td>
<td>Complete Phase II deliverables in collaboration with the uPortal team.</td>
</tr>
</tbody>
</table>
Thanks!

Further information:

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

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