Agenda

Intro to Grouper
Project status & recent news
  • v2.1
  • v2.2
  • demo of new UI
Brief campus case studies: what we're doing with Grouper and why
  • Michael Hodges, University of Hawaii
  • Chris Bongaarts, University of Minnesota
Longer term roadmap
Wrap-up, opportunities to follow up
Introduction to Grouper

Tom Barton
University of Chicago and Internet2
Manager – Grouper Project
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
Additional benefits of access management

• Delegation to empower the right people to manage access. Take central IT out of the loop.

• Operational transparency. 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

\[\text{Math Faculty Group} \rightarrow \text{Math Faculty Resources} \text{ can access}\]
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. Deeper 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

HR-Admin

• Rules

- If removed from group A
- then remove from group B
Grouper: core concepts

- Folders in hierarchies
- Group
  - Direct members
  - Subgroup
    - Indirect members
  - Composite groups

\[ \text{Group} = \bigcap \text{Direct members} \]
Security & delegation

- Create groups
- Create subfolders
- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out
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
• Move or copy folders, groups, etc
• Rules
• User audit
• Point in time audit
Access management for UChicago VPN

Different groups, different authorities
VPN only uses “vpn:authorized”
V2.1, V2.2, New UI

Chris Hyzer
University of Pennsylvania
Internet2
2.1.4

• Will be released momentarily (if not already)
• 4 months since 2.1.3
• 19 Jiras
2.1.4 (Important Jiras)

- Deleting attribute def with group which has privs, deletes members of group
- Rule to adjust privs based on group
- “Support” for Java 7
- Subject API search by status
- Lifelong group membership rule
- LDAP authentication for WS
- Various bugs and tweaks
2.2 Progress

- Config file overlays
- Grouper privileges are group lists
- Services in Grouper
- Unix GID management
2.2 Plan

• PSP improvements
• Conversion of legacy group types/attributes to new attribute framework
• Grouper user data
• SCIM interface
• UI
New Grouper UI

• Focus on most used parts of the UI
• Extensive user experience study and design
• Dojo for accessibility and improved usability and device support
• Make it easier for people to find things and perform tasks
• Responsive web design for mobile support
• See design: http://grouper-ui.uchicago.edu/hifi
New Grouper UI – main screen

Grouper
Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the support documentation.

Recent Activity

Added John Smith as a member of the Editors group. 2/1/2013 8:03 AM
Revoked Bob Weston's membership in the Editors group. 1/21/2013 9:00 AM
Assigned the ADMIN privilege to Jane Clivemore in the Senior Editors group. 12/20/2012 9:00 AM

My Favorites
- Admins
  - Root: Applications: Wiki
- Editors
  - Root: Applications: Wiki
- Senior Editors
  - Root: Applications: Wiki

Groups I Manage
- Admins
  - Root: Applications: Directories
- Managers
  - Root: Applications: Directories
- Approvers
  - Root: Applications: Wiki

My Services
- Virtual Private Network
- Wiki
- Blogs
- View all services
New Grouper UI – main screen

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the support documentation.

Recent Activity

- Added John Smith as a member of the Editors group.
- Revoked Bob Weston's membership in the Editors group.
- Assigned the ADMIN privilege to Jane Clivemore in the Senior Editors group.
New Grouper UI – main screen

Grouper
Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the support documentation.

Recent Activity

- Added John Smith as a member of the Editors group. 2/1/2013 8:03 AM
- Revoked Bob Weston's membership in the Editors group. 1/21/2013 9:00 AM
- Assigned the ADMIN privilege to Jane Clivemore in the Senior Editors group. 12/20/2012 9:00 AM

My Favorites
- Admins
  - Root : Applications : Wiki
- Editors
  - Root : Applications : Wiki
- Senior Editors
  - Root : Applications : Wiki

Groups I Manage
- Admins
  - Root : Applications : Directories
- Managers
  - Root : Applications : Directories
- Approvers
  - Root : Applications : Wiki
- Editors
  - Root : Applications : Wiki

My Services
- Virtual Private Network
- Wiki
- Blogs
- View all services
New Grouper UI – main screen

Grouper
Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the support documentation.

Recent Activity

- Added John Smith as a member of the Editors group. 2/1/2013 8:03 AM
- Revoked Bob Weston’s membership in the Editors group. 1/21/2013 9:00 AM
- Assigned the ADMIN privilege to Jane Clive in the Senior Editors group. 12/20/2012 9:00 AM
New Grouper UI – main screen

Grouper
Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the support documentation.

Recent Activity

Added John Smith as a member of the Editors group. 2/1/2013 8:03 AM
Revoked Bob Weston’s membership in the Editors group. 1/21/2013 9:00 AM

Assigned the ADMIN privilege to Jane Clivemore in the Senior Editors group. 12/20/2012 9:00 AM

My Favorites
- Admins
  - Root: Applications: Wiki
- Editors
  - Root: Applications: Wiki
- Senior Editors
  - Root: Applications: Wiki

Groups I Manage
- Admins
  - Root: Applications: Directories
- Managers
  - Root: Applications: Directories
- Approvers
  - Root: Applications: Wiki

My Services
- Virtual Private Network
- Wiki
- Blogs
- View all services
New Grouper UI – group screen

Editors

The members of this group have basic editor permissions in the Wiki. Editors have permissions to create and edit content but require approval in order to publish.

More

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

Filter for:  All members

<table>
<thead>
<tr>
<th>Entity Name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Administrators</td>
<td>Direct</td>
</tr>
<tr>
<td>Staff</td>
<td>Direct</td>
</tr>
<tr>
<td>Abbott Jane</td>
<td>Direct</td>
</tr>
</tbody>
</table>
New Grouper UI – privileges screen

Editors

The members of this group have basic editor permissions in the Wiki. Editors have permissions to create and edit content but require approval in order to publish.

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>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Senior Administrators</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Staff</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Carolin, Hank</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Real World Cases Studies

• Brief campus case studies
  • Michael Hodges, University of Hawaii
  • Chris Bongaarts, University of Minnesota
Grouper beginnings at the University of Hawaii

- Michael Hodges, Manager, Enterprise Middleware, Identity and Access Management
• Designing the Stem, we kept it very simple:
  – auto (automatically generated institutional groups)
    • everyone
    • everyone@honolulu
    • faculty
    • students@manoa
  – custom (applications and individuals manage these)
    • uhsystem
      – banner
      – ohr
  – test (applications and individuals test here)
    • mhodges (developer’s UH Username)
• First Pilot Project, make an auditor happy
  – Utilize Grouper groups to enhance our daily termination reports.
  – Reports are sent daily to each of the ERP account administrators (and others).
  – **Problem**: They each try and sift through the haystack for Usernames, and sometimes miss.
  – **Solution**: each account admin maintains a Grouper group. The termination reports include only those of interest. Everyone is happier.
  – The pilot is a success.
Getting Started with Grouper

• Second Pilot Project, augment LISTSERV lists
  – Automate membership of the UH Hilo Fac/Staff campus-wide discussion LISTSERV list.
  – **Problem**: Some people consider the list to be ham, others spam.
  – **Solution**: Allow the campus list administrator to augment an “auto” list using Grouper “inclusion” and “exclusion” groups.
  – We (IAM) populate the “auto” group for the campus and perform the Grouper math (auto + inclusion – exclusion) to rebuild the list, nightly.
Going Places with Grouper

• Expand the Augmented LISTSERV lists pilot
  – Provide Group Administration tools
    • Friendly interface for managing inclusion/exclusion group membership.
    • Support group functionality for enabling/disabling:
      – Reflection to LISTSERV lists (in the near future)
      – Reflection to Sakai groups, Google groups, etc.
      – End-user options (none vs. opt-in/out)
  – Provide End-User tools
    • Provide users with a personal list of auto groups/reflections so that they can opt in/out of each.
Going Places with Grouper

- Support more institutional groups
  - Expand the “auto” groups to include additional institutional groups: students by major, program; departments for each campus; etc.

- Evangelize *(middleware rocks!!!)*
  - Leverage our UH Applications Developers forum to share, educate, and inspire others in IT to leverage this and other tools being developed to support authentication, authorization, and utilization of middleware in general.
Grouper at the University of Minnesota

Christopher A. Bongaarts
Grouper Virtual Working Group
May 20, 2013
In the beginning...

• Grouper 1.2.1 in production August 2008
• Driver: BPEL access management for Enterprise Financial System project
  – Using LDAP groups to represent roles
  – Wanted UI with delegated administration
• Similar desires for helpdesk access to user management interface
Timeline, continued

- Upgraded to 1.5.2 in March 2010
- Switched to UW LDAP source adaptor April 2010
- Upgrade to 2.1.3 planned for summer 2013
Applications using Grouper for access management

- BPEL workflows
- Helpdesk account management
- WorkFlowGen
- VPN groups
- Oracle Business Intelligence (OBIEE)
- Various departmental sites
Other uses

• Google Apps provisioning
  – Overrides for health care component
• Netfiles (Xythos WFS) central groups
• Identifying test directory users
Example group
Another example group
Deployment Architecture
Access methods

• **Group management via web UI only**
  – Requires two-factor authN (OTP fob)

• **Client access**
  – LDAP (expressed as group objects, isMemberOf)
  – Shibboleth (SAML isMemberOf attribute)
    • Gets data from LDAP
    • Attribute filters with stem regexes work slick
Directory provisioning

- Using Grouper Loader changelog API
- Locally written Java class sends updates to person registry database
- Person registry pushes updated group data to LDAP directory
Future directions

- Investigate using the PSP for LDAP provisioning
- Create local documentation
- Encourage more applications to use Grouper for access control
Contact

Chris Bongaarts
Identity Management
University of Minnesota

cab@umn.edu
## Grouper Roadmap

<table>
<thead>
<tr>
<th>V 2.2</th>
<th>Not Yet Assigned</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>New UI</td>
<td>Security plugins</td>
<td>Grouper Core enhancement</td>
</tr>
<tr>
<td>Services</td>
<td>Access Management Standard WS API</td>
<td>Community contributions</td>
</tr>
<tr>
<td>Improved configuration</td>
<td>Further KIM-Grouper integration</td>
<td></td>
</tr>
<tr>
<td>SCIM interface</td>
<td>More WS operations</td>
<td></td>
</tr>
<tr>
<td>Treat privileges as Group lists</td>
<td>Register for notifications</td>
<td></td>
</tr>
<tr>
<td>Unix GID management</td>
<td>More provisioning connectors</td>
<td></td>
</tr>
<tr>
<td>Legacy attribute migration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COmanage integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Getting Started and Learning More

- Grouper Training Videos
  - 51 videos, with an average 120 views
- Tracks for:
  - Managers
  - System. Admins
  - Developers/Architects
  - End Users
Contributing to the Community

- Share information about your deployment with the community

- Participate on the Grouper-Users list
Thanks!

Further information:

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

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