Internet2 Techex 2017

Grouper in Action

Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College
Carl Waldbieser, Lafayette College
Bert Bee-Lindgren, Georgia Tech
Agenda

1. **Introduction to Grouper**
   a. Grouper Overview
   b. Features and capabilities
   c. What’s new

2. **Hands on Grouper**
   a. Folder and group management
   b. Searching and adding subjects
   c. Direct vs indirect membership
   d. Grouper loader jobs
   e. Composite group

3. **TIER deployment guide**

4. **Grouper @ LaFayette**

5. **Grouper @ GaTech**

6. **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

Physics 101 Course Group

Email Group
Wiki Access
Lab Reservations
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

Math Faculty Group + Math Support Group can access Math Faculty Resources
Access management stages

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

For Math Department, while John works there

HR Admin Role
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

  HR-Admin

• 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 is a solution for managing groups, roles, and permissions. It integrates with various systems, including LDAP/AD, Person Registry, and Systems of Record. It supports web services and provides a web UI and Grouper Shell for administration. Grouper loaders and provisioning service providers are used to manage subjects. Delegation and rules are managed within Grouper. Notifications can be sent via XMPP/HTTP. ESB is used for integration. For PSP management, additional connectors may be needed.
Grouper Concepts

Folders in hierarchies

Group

Direct members

Subgroup

Indirect members

Composite groups

= $\bigcap$
Security and Delegation

- Admin folders
- Create sub-groups/folders/etc
- 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
Internet2 Techex 2017

Grouper - What’s new?

Grouper in Action
Release 2.3.0.patch new features

See release notes for full list

https://spaces.internet2.edu/display/Grouper/v2.3+Release+Notes

(google “grouper release notes”)

- Grouper loader improvements for real time updates
- External subject web services
- Find bad memberships daemon
- TIER instrumentation (with UI)
- Migrate XML config to properties overlays
Release 2.3.0.patch new features (continued)

- Subject API diagnostics
- Grouper loader in UI
- Attestation
- New GSH command line utility
- Messaging implementation, WS, and service bridge
- Many UI usability improvements
- Provisioning fixes and improvements
- Lots of other improvements
Grouper roadmap

- Migrate to New UI
- Deprovisioning in UI
- Provisioning in UI
- Other UI features:
  - Membership reports
  - Migrate entitlements from one user to another
- Configuration stored in database
Create new folder

- Go to grouper demo (google “grouper demo”)
- [https://grouperdemo.internet2.edu](https://grouperdemo.internet2.edu)
- Click on UI 2.3
- Go to the folder: training:techEx2017
- Create a folder based on your netID (e.g. mchyzer).
  - Don't use special chars except maybe underscore.
- Click into that folder
Create 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
## Filter for:

Folder, group, or attribute name

- **affiliations**
- **courses**
- **etc**
- **loader**
- **psp**
- **test**
Create an “apps” folder in your folder

- In “apps”, make a “wiki” folder
- In “wiki”, make an “etc” folder
  - Sometimes the extension of the folder shows in the UI, so make it unique-ish e.g. “wikiEtc”
- In “etc”, make an admins group
  - Sometimes the extension of the group shows in the UI, so make it unique-ish e.g. “wikiAdmins”
- Talk to your neighbors, get their name, add them to the wiki admins group
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
A test group

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>

| Remove selected members |

<table>
<thead>
<tr>
<th>Entity name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show: 50</td>
<td></td>
</tr>
</tbody>
</table>
**test_group**

Member name or ID: 

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

More

---

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>

---

| Remove selected members |

---

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

---

Show: 50

---

Showing 1-1 of 1 · First | Prev | Next | Last
### test_group

**Member name or ID:**

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

More 

### Members

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

<table>
<thead>
<tr>
<th>Filter for:</th>
<th>Has direct membership</th>
<th>Member name</th>
<th>Apply filter</th>
<th>Reset</th>
</tr>
</thead>
</table>

Remove selected members

<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>

Show: 50

Showing 1-3 of 3 · First | Prev | Next | Last
Assign hierarchical privs to wiki folder

- Go to wiki folder
- On the “More” tab
- Click “privileges inherited to objects in folder”
- Add
- Find your wiki admins group
- Assign to all types: ADMIN
- Create a wikiUsers group
- Have your neighbor verify that they can add/remove members to that group
Turn the group into include/exclude

- Click on Admin UI
- Find the group
- Edit
- “Add include/exclude”
- Save
- Go back to New UI
### Edit group

Current location is:
- Root: 🗂️
- test: 👤 all_the_anns

<table>
<thead>
<tr>
<th>Name</th>
<th>all_the_anns</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>all_the_anns</td>
</tr>
<tr>
<td>Alternate ID Path</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Assign privileges to everyone</td>
<td>Read</td>
</tr>
<tr>
<td>Select group types</td>
<td>add</td>
</tr>
</tbody>
</table>

Save

Back to group summary
Go back to New UI, analyze membership

• Go to overall group
• See a membership
  • If none there, then add one to the system of record
• Actions -> trace membership
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

Back to group
### test_group

**Member name or ID:** Ann Brown  
[Enter an entity name or ID, or search for an entity.](#)  

**Assign these privileges:**  
- MEMBER  
- ADMIN  
- UPDATE  
- 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:** Entity name  
[Apply filter](#)  
[Reset](#)  
[Advanced](#)

**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  
[Actions](#)

Showing 1-1 of 1  
First | Prev | Next | Last
The following table lists all entities with privileges in this group.

Filter for: Entity name

Update: Assign the ADMIN privilege

<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>
<th>Actions</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>
<td></td>
</tr>
<tr>
<td>Bob Anderson</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Show: 50
Go to system of record, make loader

- Go to system of record group
- More tab - > Loader
- Edit
- Copy settings from

https://spaces.internet2.edu/display/Grouper/Grouper+loader+SQL+simple+example

- Can google “grouper loader SQL simple loader”
- SELECT 'jdbc' AS subject_source_id, subjectId AS subject_id FROM subject WHERE subjectId IN ('test.subject.0', 'test.subject.1', 'test.subject.2')
## Loader settings

This group has loader configuration

<table>
<thead>
<tr>
<th>Source type</th>
<th>SQL pull the members from a SQL database. Can be SQL or LDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loader type</td>
<td>SQL_SIMPLE the SQL query loads the members of this group. Can be SQL_SIMPLE or SQL_GROUP_LIST</td>
</tr>
<tr>
<td>Database name</td>
<td>grouper jdbc:mysql://localhost:3306/grouper_v2_3?CharSet=utf8&amp;useUnicode=true&amp;characterEncoding=utf8 server ID that is configured in the grouper-loader.properties that identifies the connection information to the database server. Note: “grouper&quot; means use the Grouper registry database connection.</td>
</tr>
<tr>
<td>SQL query</td>
<td>SELECT <code>jdbc</code> AS subject_source_id, subjectId AS subject_id FROM subject WHERE subjectId IN ('test.subject.0', 'test.subject.1', 'test.subject.2') query for memberships. Since this is SQL_SIMPLE, the SUBJECT_ID or SUBJECT_IDENTIFIER or SUBJECT_ID_OR_IDENTIFIER column is required, and the SUBJECT_SOURCE_ID column is optional (but recommended for better performance). SUBJECT_ID has the best performance, and SUBJECT_IDENTIFIER and SUBJECT_ID_OR_IDENTIFIER are slower since they require subject API lookups. If the data has group names as members, it must be in a SUBJECT_IDENTIFIER column.</td>
</tr>
<tr>
<td>Schedule type</td>
<td>CRON Cron setting runs on a certain schedule. Can be CRON (recommended) or START_TO_START_INTERVAL</td>
</tr>
<tr>
<td>Schedule</td>
<td>0 0 6 * * ? At 6:00 AM</td>
</tr>
<tr>
<td>Priority</td>
<td>this job has the default and middle priority of 5 (higher numbers have a higher priority)</td>
</tr>
<tr>
<td>Require members in other group(s)</td>
<td></td>
</tr>
<tr>
<td>Job name</td>
<td>SQL_SIMPLE_training:techEx2017:mchyzer:apps:mchyzerWiki:wikiUsers_systemOfRecord_7a6ca27c8def4085a59a5b2eddef453b used in the database in the grouper_loader_log table to identify records for this job</td>
</tr>
</tbody>
</table>
Run loader features

- Schedule the job
- Run the job
- Run diagnostics
- See members
- See overall members
- Add one of them to the excludes group
- See the overall 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 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>

### Action Menu
- 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
See composite

- Go to some of the groups
- More actions, edit composite
- Don’t make changes, but see which groups are composites
- Draw out how the groups are related
- Which takes precedence, includes or excludes
  - I.e. if someone were in both, would they be in the overall?
The following table lists all entities which are members of this group.
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_anns
Enter a group name or ID, or search for the second factor.

[Save]  [Cancel]
Make the excludes group attestable

- Go to the excludes group
- More actions -> attestation
- Edit attestation
- Yes, has attestation
- Don't set as attested (or clear it afterwards if you set it)
- Save
- Should say needs attestation
- I can run daemon as admin
- Maybe we will get emails?
  - If subject source and record setup correctly
See more attestation screens

- Global attestation
- Global settings
- Folder attestation
- Folder settings
- Group audit history
- Set an attestation
- See the history again
- Go to Lite UI and see attributes
### Attribute assignments

<table>
<thead>
<tr>
<th>Owner group</th>
<th>Attribute name</th>
<th>Enabled?</th>
<th>Assignment values</th>
<th>Attribute definition</th>
<th>Assignment UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>testB</td>
<td>attestation</td>
<td>enabled</td>
<td></td>
<td>attestationDef</td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InheritAttestGroup</td>
<td>attestation</td>
<td>enabled</td>
<td>2017/10/15</td>
<td>attestationValueDef</td>
<td>95145...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationCalculatedDaysLeft</td>
<td>enabled</td>
<td>0</td>
<td>attestationValueDef</td>
<td>24ed6...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationDirectAssignment</td>
<td>enabled</td>
<td>false</td>
<td>attestationValueDef</td>
<td>c45d4...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>testAttest</td>
<td>attestation</td>
<td>enabled</td>
<td>2017/10/15</td>
<td>attestationDef</td>
<td>22f74...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationEmailAddresses</td>
<td>enabled</td>
<td></td>
<td>attestationValueDef</td>
<td>0b5e7...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationDateCertified</td>
<td>enabled</td>
<td>2017/10/15</td>
<td>attestationValueDef</td>
<td>428be...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationCalculations</td>
<td>enabled</td>
<td></td>
<td>attestationValueDef</td>
<td>4aa59...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationDaysBeforeToRemind</td>
<td>enabled</td>
<td>180</td>
<td>attestationValueDef</td>
<td>8e361...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationDirectAssignment</td>
<td>enabled</td>
<td>true</td>
<td>attestationValueDef</td>
<td>98e05...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationDaysUntilRecertify</td>
<td>enabled</td>
<td>true</td>
<td>attestationValueDef</td>
<td>c83f6...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>overallgroup</td>
<td>attestation</td>
<td>enabled</td>
<td></td>
<td>attestationDef</td>
<td>65381...</td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata on assignment</td>
<td>attestationLastEmailedDate</td>
<td>enabled</td>
<td>2017/10/15</td>
<td>attestationValueDef</td>
<td>a888e...</td>
</tr>
</tbody>
</table>
Thanks!

Further information:

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

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