Internet2 Techex 2018

Grouper in Action - 101

Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College
Carl Waldbieser, Lafayette College
James Babb, Internet2
Agenda

- Introduction to Grouper
- 101.1: Subjects
- 101.2:
  a. Folders
  b. Groups
  c. Attributes
- 101.3: Finding Grouper objects
- 101.4: Managing memberships
- 101.5: Composite groups
Internet2 Techex 2018

Introduction to Grouper

Grouper in Action - 101
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
**Subjects**

- **Definition** - A subject is a thing that can be assigned a Group membership, privilege, or permission.
- Each institution defines their subjects, generally these are **people**, and **service principals** that authenticate system communication.
- Grouper has built in subjects for “sys admin user”, “every entity”, and all groups.
Subjects in UI

• Note: in the Grouper UI, subjects are referred to as “entities”
Subject attributes

- **ID**: Should be an opaque unchanging unique label.
- **Identifier**: An attribute that uniquely looks up a subject, this can change over time and doesn’t need to be opaque.
- **Name**: String name for subject (generally “First Last”).
Subject attributes (continued)

• Description: Long form text about subject. Should help a UI user differentiate between two subjects with same name

• Member ID: UUID for the subject, grouper assigned

• Source ID: Identifies which “source” a subject originates from
Subject attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique ID</td>
<td>10021368</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:mchyzer@upenn.edu">mchyzer@upenn.edu</a></td>
</tr>
<tr>
<td>Name</td>
<td>Chris Hyzer</td>
</tr>
<tr>
<td>Description</td>
<td>Chris Hyzer (mchyzer, 10021368) (active) Staff - ISC-applications &amp; Information Services - Application Architect (also: Alumni)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name_last_public</td>
<td>Hyzer</td>
</tr>
<tr>
<td>preferred_first_name</td>
<td>Chris</td>
</tr>
<tr>
<td>first_name</td>
<td>Michael</td>
</tr>
<tr>
<td>name_first_public</td>
<td>Chris</td>
</tr>
<tr>
<td>name_public</td>
<td>Chris Hyzer</td>
</tr>
<tr>
<td>email_public</td>
<td><a href="mailto:mchyzer@upenn.edu">mchyzer@upenn.edu</a></td>
</tr>
<tr>
<td>pennname</td>
<td>mchyzer</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:mchyzer@upenn.edu">mchyzer@upenn.edu</a></td>
</tr>
<tr>
<td>description_lower</td>
<td>chris hyzer (mchyzer, 10021368) (active) staff - isc-applications &amp; information services - application architect (also: alumni),christopher,<a href="mailto:mchyzer@isc.upenn.edu">mchyzer@isc.upenn.edu</a>,<a href="mailto:mchyzer@upenn.edu">mchyzer@upenn.edu</a>,michael</td>
</tr>
<tr>
<td>last_name</td>
<td>Hyzer</td>
</tr>
<tr>
<td>eppn</td>
<td><a href="mailto:mchyzer@upenn.edu">mchyzer@upenn.edu</a></td>
</tr>
<tr>
<td>Member ID</td>
<td>c5c8ef55-76be-4b0d-9910-9efbf465cff3</td>
</tr>
<tr>
<td>Source ID</td>
<td>pennperson</td>
</tr>
<tr>
<td>Source name</td>
<td>Penn person</td>
</tr>
</tbody>
</table>
Subject source types

- Built-in
- SQL
  - Generally you identify a table or view with subjects as each row, columns are attrs
- LDAP
  - Filters find subjects and contain attributes
Subject identifiers

- **ID**: Look up a subject by its unchanging (generally opaque) ID. e.g. institutionID
  - Across all sources, the primary key for a subject can be its Grouper UUID, or the tuple (sourceId, subjectID)
  - Subjects have one and only one

- **Identifier**
  - Subjects can have multiple identifiers that uniquely identify the subject in the source
  - E.g. netId, eppn, (email address?)
Subject lookup, search

- Lookup returns 0 or 1 subjects
- Search returns 0 or many subjects
- You can lookup a subject by sourceID and subjectID
- Lookup by sourceID and subjectIdentifier
- Search by ID or identifier across all sources
- Search by free-form text
Subject storage in Grouper

• Grouper stores some subject information in a table
• Primary key is UUID
• Unique key is sourceld and subjectld
• Stores an identifier, name, description, search fields, sort fields
Unresolvable subjects

- A subject that was assigned things in Grouper, and no longer can be found
- Someone left the institution
- Or their subjectId changed (shouldn't happen :) )
- USDU - Unresolvable Subject Deletion Utility - find unresolvable subjects and removes them from Grouper
Subject API

- Configure a new source by implementing a Java interface (few or no people do this)
- Interface with subjects via Grouper WS
- Lookup or search for subjects
Hands on: Subjects in UI

- Search for “Bob Ander” in upper right
Hands on: Look at LDAP Subject

- Click on the result: Bob Anderson
- Click: More
- Note the source ID and unique ID
Hands on: Subject diagnostics

- Click Misc -> Subject API diagnostics
- Select EDU Ldap source
- For subject ID enter: banderson
- For search string: o
Hands on: Subject diagnostics

Subject API diagnostics

Source ID: EDU Ldap (person)
The Source ID is configured in the subject.properties file. Some sources are internal for Grouper and one or more are custom for your institution. The fewer the better.

Subject ID: banderson
Enter a Subject ID to search for. This should be an unchanging opaque identifier. This defaults to the subject.properties source param 'subjectIdToFindOnCheckConfig' or to a hardcoded default value if not configured, which is used in the status servlet.

Subject Identifier: someSubjectIdentifier
Enter a Subject Identifier to search for. This is any identifier that uniquely identifies this subject in this source. e.g. netId, eppn, etc. It is nice if identifiers are unique across sources, which defaults to the subject.properties source param 'subjectIdentifierToFindOnCheckConfig' or to a hardcoded default value if not configured. This is used in the status servlet.

Search String: o
Enter a Search String to search for. This usually searches based on name, id, identifier, description, etc. This defaults to the subject.properties source param 'stringToFindOnCheckConfig' or to a hardcoded default value if not configured, which is used in the status servlet.
Internet2 Techex 2018

Folders

Grouper in Action - 101
Folder

- Definition: Folder (aka stem) is a namespace which contains groups, folders, and attributes
- Each child object is in one hierarchical parent folder
- Folders themselves can be assigned custom attributes
- Folder extensions are separated by commas
Folder fields

- **UUID**: All Grouper objects have a UUID
- **Extension**: “ID” on UI, label that is the name
  - Shouldn’t change
  - Referred to by applications on lookups
- **Display extension**: “name” on UI, label is the name seen in UI
  - Can change
- **Description**: Free form documentation
Folder fields (continued)

- **Name**: (ID Path in UI): extension of all parent folders and this folder separated by colons
  - E.g. app:banner:etc

- **Display name**: (Path in UI): display extension of all parent folder and this folder separated by colons
  - E.g. app:Banner:Administrative folder
Hands on: Creating a folder

- Navigate to the “test” folder
- Click “Create new folder”
Hands on: Creating a folder (continued)

- Fill in details, and save
Hands on: Editing a folder

- In the folder you created, edit it
Hands on: Editing a folder (continued)

- Change some fields, Save
Hands on: Moving a folder

- Click More actions -> Move folder
Hands on: Moving a folder (continued)

• Move to “app”, click Move
Hands on: Copying a folder

- Click More actions -> Copy folder
Hands on: Copying a folder (continued)

- Move to test, click Copy
Internet2 Techex 2018

Groups

Grouper in Action - 101
Group

- Definition: Group is an object which contains members
- A group is located in a folder
- Groups can have attributes assigned to them
Group fields

- UUID: All Grouper objects have a UUID
- Extension: “ID” on UI, label that is the name
  - Shouldn’t change
  - Referred to by applications on lookups
- Display extension: “name” on UI, label is the name seen in UI
  - Can change
- Description: Free form documentation
Group fields (continued)

- Name: (ID Path in UI): extension of all parent folders and this group separated by colons
  - E.g. app:banner:etc:banner_admin

- Display name: (Path in UI): display extension of all parent folder and this folder separated by colons
  - E.g. app:Banner:Administrative folder:Banner Administrators
Hands on: Creating a group

- Navigate to the “test” folder
- Click “Create new group”
Hands on: Creating a group (continued)

- Fill in details, and save
Hands on: Editing a group

- In the group you created, edit it
Hands on: Editing a group (continued)

- Change some fields, Save
Hands on: Moving a group

Click More actions -> Move group
Hands on: Moving a group (continued)

- Move to “app”, click Move
Hands on: Copying a group

- Click More actions -> Copy group
Hands on: Copying a group (continued)

- Move to test, click Copy
Attributes

Grouper in Action - 101
Attribute

• Definition: Attribute is metadata attached to another Grouper object
• An attribute consists of a definition, and a name
• An attribute definition object and name object are located in a folder
• Attributes can have values
• The definition has all the configuration
• The name is a name and is what is assigned
Attribute diagram

Privileges
Where can it be assigned?
Data type (number or string etc?)
Etc

AttributeDef

Attribute names have one and only one corresponding definition

AttributeName
AttributeName
AttributeName

Group2
Group1

Those attributes can be assigned to objects
Attribute definition fields

• UUID: All Grouper objects have a UUID
• Extension: “ID” on UI, label that is the name
  • Shouldn’t change
  • Referred to by applications on lookups
• Description: Free form documentation
• Name: (ID Path in UI): extension of all parent folders and this attribute definition separated by colons
• E.g. app:banner:attr:banner_expire_date
Attribute definition fields (continued)

• Type: e.g. attribute or permission
• Assign to:
  • Group
  • Folder
  • Member
  • Membership
  • Immediate membership
  • Attribute definition
  • An assignment of one of the above (one-level deep)
Attribute definition fields (continued)

- Multi-assignable: can this attribute be assigned to the same owner more than once
- Value type: (generally none or String)
  - No value
  - String
  - Integer
  - Decimal
  - Timestamp
  - Member UUID
Attribute definition fields (continued)

• Multi-valued: can this attribute assignment have multiple values
Attribute name fields

- **UUID**: All Grouper objects have a UUID
- **Extension**: “ID” on UI, label that is the name
  - Shouldn’t change
  - Referred to by applications on lookups
- **Display extension**: “name” on UI, label is the name seen in UI
  - Can change
- **Description**: Free form documentation
Attribute name fields (continued)

• Name: (ID Path in UI): extension of all parent folders and this group separated by colons
  • E.g. app:banner:etc:banner_admin

• Display name: (Path in UI): display extension of all parent folder and this folder separated by colons
  • E.g. app:Banner:Administrative folder:Banner Administrators

• Corresponding attribute definition
Hands on: Creating an attribute

- Navigate to the “test” folder
- Click “Create new attribute definition”
**Hands on: Creating an attribute** (continued)

<table>
<thead>
<tr>
<th>Create in this folder:</th>
<th>test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a folder name or search for a folder where you are allowed to create new attribute definitions.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute definition ID:</th>
<th>myAttrDef</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID is the unique identifier for this attribute definition. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description:</th>
<th>my attribute definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description contains notes about the attribute definition, which could include: what the attribute definition represents, why it was created, etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type:</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute definition type describes the attribute definition. Generally it will be attribute or permission. Type is used for templates, limit describes a permission, and service identifies which application the object refers to.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assign to:</th>
<th>Attribute definition attribute assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Folder attribute assignment</td>
</tr>
<tr>
<td>Group / Role / Local entity</td>
<td>Group / Role / Local entity attribute assignment</td>
</tr>
<tr>
<td>Member</td>
<td>Member attribute assignment</td>
</tr>
<tr>
<td>Membership</td>
<td>Membership attribute assignment</td>
</tr>
<tr>
<td>Membership - immediate only</td>
<td>Membership - immediate only - attribute assignment</td>
</tr>
</tbody>
</table>

Designate which types of objects that this definition can be assigned to. There are six base object types, or you can assign attributes to the assignment of attributes to those base object types. Membership can be assigned to an immediate or an effective membership, and will still exist as an orphan if the membership is unassigned until the membership is reassigned. Immediate membership attribute assignments are only assignable to immediate memberships and are automatically deleted once the membership is unassigned.

<table>
<thead>
<tr>
<th>Multi-assignable:</th>
<th>If this attribute can be assigned to the same owner object more than once. For instance, a Group can have more than one Rule attached to it, so the Rule attribute is multi-assignable</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Value type:</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this attribute assignment holds one or more values, this is the type. If there are no allowed values, select No value.</td>
<td></td>
</tr>
</tbody>
</table>
Hands on: Creating an attribute name

- Go to the “myAttrDef” attribute def
- Click “Create new attribute name”

The following table lists all attribute names associated with this attribute definition.
Hands on: Creating an attr name (continued)

### New attribute name

<table>
<thead>
<tr>
<th>Attribute definition:</th>
<th>test:myAttrDef</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The attribute definition holds the settings and security for attribute. Each attribute definition can have multiple attribute names. Every attribute name is associated with one and only one attribute definition.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Folder:</th>
<th>test</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enter a folder name or search for a folder where you are allowed to create new attribute def names.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of attribute name:</th>
<th>myAttrName *</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name is the label that identifies this attribute name, and might change.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID of attribute name:</th>
<th>My Attr Name</th>
<th>Edit the ID *</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ID is the unique identifier you set for this attribute name. The ID must be unique within this folder, and should rarely change. It can be used by other systems to refer to this attribute name. The ID field cannot contain spaces or special characters.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description:</th>
<th>this is my attribute name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description contains notes about the attribute name, which could include: what the attribute name represents, why it was created, etc.</strong></td>
<td></td>
</tr>
</tbody>
</table>
Hands on: Assigning an attribute

- Go to the “test” folder
- Click on More actions -> Attribute assignments
Hands on: Assign attribute (continued)

- Click Assign attribute
Hands on: Assign attribute (continued)

- Find myAttrName, click Save
Hands on: Assign value

- Find myAttrName assignment
- Click Actions -> Add value
Hands on: Assign value (continued)

- Use “Some value”
Hands on: Assign value (continued)

• See “Some value”
Hands on: Subjects in UI

• Search for “Bob Ander” in upper right
Hands on: Look at LDAP Subject

• Click on the result: Bob Anderson
• Click: More
• Note the source ID and unique ID
Hands on: Find a group

• Search for “banner_user” in upper right
Hands on: Find a group (continued)

- Click on “banner_user”
Hands on: Make a favorite

- Find a group, folder, and subject
- Click: More actions -> Add to my favs
Hands on: See favorites

- Click on “home”
- See favorites
Left menu

- Shows folders, groups, attribute definitions, attribute names
- Shows the first X (few dozen), then stops
- Does not auto refresh when objects are created or deleted
- You can manually refresh
Hands on: Browse left menu

• Expand and contract and click on left menu
• Click the reload button
Main menu

• Shows folders, groups, attribute definitions, attribute names
• Shows the entire list paged
• Each click will show a fresh accurate list
• You can manually reload the browser
Hands on: Browse main menu

• Click on a folder
• Click on other folders in the main menu
Groups I manage

• This widget shows groups that the current user can change memberships or admin
Hands on: Groups I manage

- Click on “home”, see “Groups I manage”
My services

• Shows services
• Folders must be marked as a service
• The current user is a member of a group (and can READ memberships in that group) in the service
Hands on: My services

• Click on “home”, see “My services”
Hands on: My services

- Click on “home”, see “My services”
My folders

- Shows folders that the current user can create objects in or admin
Hands on: My folders

- Click on “home”, click “gear”, click “My folders”
My memberships

- Shows memberships of the current user (that they can READ)
Hands on: My memberships

• Click on “home”, click “gear”, click “My memberships”
Recently used

• Click on “home”, click “gear”, click “Recently used”
Hands on: My memberships

- Click on “home”, click “gear”, click “My memberships”