Grouper BaseCAMP session
August 15, 2019
Milwaukee, Wisconsin
Agenda

Introduction to Grouper
Features and Roadmap
Use cases from Duke
Use cases from Penn

Chris Hyzer: University of Pennsylvania
Shilen Patel: Duke
What is Grouper
Control access policy centrally

Leverage “system of record” groups
To assign access
To deprovision assignments
Add or subtract exceptions
Manage ad hoc groups
Share policies among several applications
See what resources someone has access to

View access from a person or service principal point of view
Easily onboard someone to be “like” an existing or past employee
Deprovision access when affiliations change
Depends on how many applications Grouper is integrated with
Delegation

Assign folder privileges
Allow departments and groups to manage their resources
Privileges available on folders, groups, and attributes
Privileges can inherit from ancestor folders
Auditing

Keep track of changes, who made them and when
Point-in-time gives you a view in the past
Certain point in time
Time range
Who was in a group at a certain point in time
Who was in the group over the last year
What access someone had 2 years ago
Rules

When an action happens
If a condition is true
Make something else happen

E.g. remove access if user changes affiliation
E.g. email access administrator if user changes jobs
E.g. veto if not eligible
E.g. automatically assign expire date
Attributes

Grouper attribute framework
Assign attributes to groups, folders, entities, attribute assignments, etc
Attribute assignments can have values
Can be multi-assign
Can be multi-valued
Permissions

Implement RBAC permissions

Roles

Role inheritance

Resources that a role or user has access to

Resource hierarchies

Actions that the user or role can perform on the resource

Action hierarchies
Subjects / entities

Entities (aka Subjects) are things that can be used in Grouper

- Member of group
- Assignee of privilege
- Has permission
- Assigned attributes

Grouper is connected to one or many subject sources (SQL or LDAP)

It’s nice if you have an IdM to merge your entities into one identifier namespace
Folders

Folders hold Grouper objects:

- Groups
- Folders
- Attributes

Folders are a namespace

Privileges, attestation, other features can be assigned at the folder level and inherit to sub-objects
Privileges

Configure who has access to various objects and features in Grouper

Inherit privileges from folders

Delegate folders to various organizational levels

For example group privileges control:

- Who can view the group exists
- Who can read the memberships
- Who can admin the group
- Who can change memberships
- Etc
Composites

Composite groups help create policies

A composite owner has two factors

‘Intersections’ require members are in both factor groups
- For example: require members are active employees

‘Complements’ require members in first factor but not second factor
- For example: subtract members in the red button group

‘Union’ doesn’t exist, just add a group as a member of another group
- For example: members can be faculty or staff
Types

Grouper Deployment Guide defines certain types of groups and folders

Grouper manages attributes to identify objects as being a certain type

- basis: Basis groups represent arcane codes or attributes from external systems are used generally in reference groups and not directly in access policy.
- ref: Reference groups are institutionally meaningful cohorts used in access policy
- policy: Access policy groups are used by downstream systems to allow or deny users access to services or resources.
- security: Security groups are collections of entities who have from access privilege on a group/folder/attribute, e.g. studentSystemAdmins.
- others: readonly, org, test, app
Grouper loader

- The Grouper loader loads groups on cron and real-time from external sources
- Two types
  - SQL
    - Load a single group from SQL
    - Load a list of groups from SQL
  - LDAP
    - Load a single group from an LDAP filter
    - Load a list of groups from LDAP filter returning groups
    - Load a list of groups from an LDAP filter returning people with attributes
Grouper reports

- Composite, see members (e.g. users who aren’t employees)
- Folder reports (memberships in folder who do not have training)
- SQL report (most anything is possible)
- Your own report engine with the Grouper database

Set report security by a group
Schedule reports with email notifications
View past reports to identify trends
Deprovisioning

Centrally view memberships, privileges, permissions

Unassign someone’s access in one screen

Manage metadata settings about deprovisioning so the correct entitlements get adjusted when someone’s affiliation changes

Buffer changes with grace periods and corrections for delays in source systems
Attestation

Periodically review groups
Configure the schedule
Email reminders
Configure at a folder or group level
Folder level will inherit to group descendant
Soon reports will be able to be attested
Visualization

See how groups are connected
View policies visually
See an entities access visually
See where groups are provisioned
See member counts at a glance
Workflow / approvals / electronic forms

Will be released hopefully by 8/21/2019 (in the next week)
Configure a workflow on a group with custom form and form elements
Various people or groups approve the workflow at various states (nodes)
Requestor is automatically added to group(s) at end of workflow
Email notifications for approvers
UI screens to see forms from various views (requestor, approver, admin)
Auditing of who did what when
Snapshots of forms stored at each step in workflow
Roadmap

2.5 to be released in the next few months

2.4 will be feature frozen and only bug fixes and security issues will be made

- Configuration in the database
- E-forms (workflow and approvals)
- Configuration wizards
- Delete dates on groups
- Rules in UI
- Grouper Deployment Guide V2
Training

- Attend a two day Grouper training
- Given twice per year
- For new users or not so new users
- Learn how to use Grouper and how to authorize services the right way
- Read the Grouper Deployment Guide
- See self service training videos (a little dated, will be updated in next year hopefully)
Demo server

Sign up for demo server: https://grouperdemo.internet2.edu
See Grouper is various versions
You can see the UI and WS
Use Cases from Duke
Grouper Use Case: WearDuke

- Initiative to use wearable devices to track student activity and sleep patterns.

- Students would enroll and take surveys using the WearDuke application.

- Eligible students are first year undergraduates who live in Gilbert-Addoms (GA).

- Students have to sign a consent and re-consent after they turn 18.
Grouper Use Case: WearDuke

Traditional approach
- A lot of sensitive data moving around
- A lot of applications like WearDuke – this approach doesn't scale well
- SoRs have custom integrations with many applications
Grouper Use Case: WearDuke

Grouper approach

- SoRs send data to Grouper instead

- Reference groups are created in Grouper
Student System
Reference group of first year students and reference group of students under 18

Housing System
Reference group of students living in GA

Grouper
Group memberships

Shibboleth
Releases whether the authenticated user is a member of the WearDuke eligible group and WearDuke participates group

WearDuke Application
Grouper Use Case: VPN

This system requires Multi Factor Authentication. Please enter your username, password and security key.

Security key options:
- Touch the key icon in your Duo app to retrieve key.
- Touch YubiKey button while inserted into a USB port.
- Type ‘Push’ to receive a prompt on your Duo app.
- Type ‘Phone’ to receive a confirmation phone call.
- Type ‘sms’ to receive a text message with a new key.

Group: -Default-
- Fuqua School of Business
- INTL-DUKE
- Library Resources Only
- Nicholas Internal
- Protected_Data
- Public Safety
- SSRL_Secure

Fuqua
Fuqua excludes
Fuqua includes
Fuqua system of record
Grouper Use Case: VPN

- Systems of record provide most of the data
- Include/exclude groups delegated out to departments to manage
- All manual changes are audited
- Provisioning to AD is a built-in feature
**Grouper Use Case: UNIX login and file permissions**

- UNIX systems use LDAP for user and group data
- Grouper provisions groups to LDAP as well
- Provisioning includes gidNumbers
Grouper Use Case: AWS

- Grouper groups are used to manage “roles” in Amazon
- Amazon’s SAML integration allows us to easily pass group memberships

- Many other Shibboleth integrations
Using Grouper audit data to pull membership history (e.g. multi-factor enrollment)
Use Cases from Penn
Use case 1 from Penn: coarse grained authz

- System was compromised

Hacker hacks a URL not protected by shib

App server shib
Use case 1 from Penn: coarse grained authz - temporary fix

- Add VPN
- Users hate VPN
- Tedious on mobile devices
- Users allowed on VPN need to be added, removed, superset of app users

App server

VPN with MFA
Use case 1 from Penn: coarse grained authz - permanent fix

- **Browser**
- **Apache Shib**
  - 100% Reverse proxy
  - Restrict users to group of app users who are active employees and in MFA
- **Grouper group intersection of app users and active employees in two step**
- **Grouper group loaded of app users**
- **App server Shib**
  - On private network
Use case 2 from Penn: banner team collaboration

- Attested ad hoc group of team members
- LMS loaded groups
- Trained team members
- HR loaded groups
- Trained active team members
- MFA loaded group
- Trained active MFA team members
- Note: there are exemptions
- Team email list
- Banner non prod env
- Wiki / Jira
- Box group with access to box folder
- Clarizen cloud PM entitlement
- Team email list
Use case 3 from Penn: banner production

- Trained people
- LMS loaded groups
- HR loaded groups
- MFA loaded group
- Note: there are exemptions
- Trained active faculty and staff
- Loaded active schemas, reports, groups
- Loaded active accounts
- Banner prod env assertion
  - Coarse grained authz
- Prod users email list
- - Report of users to deprovision
  - - Attestation
  - - Notification when user changes orgs
  - - Notification when user changes orgs