

[Link to 2024 ACAMP Wiki](#)

Advance CAMP Thu. Dec 12, 2024

Room - III

Session Title: Train or Build frontend for Grouper

CONVENER: Graham

MAIN SCRIBE(S): Liz Groff

ADDITIONAL CONTRIBUTORS:

of ATTENDEES: 24

DISCUSSION:

Graham: Had 30 year old maillist and never rolled it out for technical staff and has to be on a particular compact

Graham: Started out as a distribution system. Groups can be consumed in multiple ways and has APIs but no visibility. It's simple to use, easy to edit membership, send email, but has a lot of limitation. Has no namespace everything is flat. People invented name spaces and has a simple permissions model one owner, zero to many managers and can be a hassle to reassign ownership. Designed for mail lists, groups got used for other purposes.

Graham: Few years ago we put it into production and tying it into core IT system and introducing it as a service to the community. We have a centralized IT structure but faculty has their own little IT staff. Their faculty dept groups do their own editing.

Graham: Third phase is to retire the service and migrate active lists.

We had to make a decision to train non-technical staff and faculty. Grouper has a lot of features but a lot of complexity. We had to expose them to what they needed to see and how easy to we want the change to be for them. It was more of a organizational change than a technical one.

Graham: Making people realize this is a good thing. We had to decide to build an interface or train staff. We picked build.

Graham: We didn't want to have to handle faculty members shooting themselves in the foot by having root access.

Martin: How many people would login to grouper?

Graham: A faculty member can come in and get a group for their class, research dept, etc. Anyone can request a group.

Graham: We purposely made this a simple scope. They keep asking us for certain features but using it bare minimum so it doesn't balloon out and focus on what we have. You can add/remove members and tweak attributes, view the groups you are in and request exchange distribution groups. You cannot request a reference group; groups in each unit's grouper space is managed by unit IT. Distribution groups are more ad-hoc and comfortable letting anyone request those groups.

Graham: NodeJS back with Express and GraphQL end very simple to help querying all the data and built entirely on top of grouper web services. Web services API call you can use for custom workflows. Uses GSH templates

Demo:

Graham: You can filter with distribution groups and security groups separately. We had attestation turned on and approval to share the web code to release.

Graham: If I pick one of these groups, lots of test groups. Nobody is in it I can add a reference group. You have to know the path to the group you want. Can use reference or other groups logged in user can see. We are working on an autocomplete like the Grouper UI.

If you have a file of members you can just dump them in there if you wanted to. This group I tried to add doesn't have permissions to view that group so it errored out.

Graham: We are connecting to the API to a service account to make changes but it mocks a specific user's access.

Graham: We are not letting people rename groups. If you expose it outside of Grouper it can cause issues.

Graham: Group status we show enabled dates. That's it for security groups.

Graham: Managing exchange groups. (Different options than for security groups.) The way we implemented distribution groups. There are 5 grouper groups under the covers.

Graham: Distribution groups have group settings that can be set as attributes specific to Exchange. If they want to hide from directory, etc

Liz: Can anyone change their group attributes if they wanted?

Graham: Yes. Only showing the attributes if you have the privileges.

Erica: Is that automated through powershell?

Graham: Yes. All groups are exposed next to each other so you wouldn't need to go to a different grouper folder to make changes as needed.

Graham: We do show all the groups you are a member of. It's not very useful but it is there. We have been requested a view of the groups you can see. Ones you can view/read. There is no way for them to see that. We are trying to find the right way to do that.

Graham: Grouper shell template with a UI would be a fairly long form. It would be hard to do it in one form or three different places. We have 3 different exchange group types -

Standard Groups - group with any person in it

Course Groups - class distribution groups

Graham: Academic Plan Group

- every student in an academic plan

Graham: Restricted sender groups:

Exchange makes it a bit more complicated for restricted sender groups with exchange protocols. It doesn't trust the exchange protocols . (wizard for requesting group)

Graham: Group managers - manage the group

Graham: Group readers - what groups you can see

Graham: It kicks off a workflow when you submit it. It has a pretty long GSH template that creates the accounts with attributes and members. It gets put into a pending grouper folder. Admins can approve or reject the groups.

Graham: Course and plan groups have the same workflow. Which department you want and course number - follow the wizard and pick what you want.

Erica: Do you have your class rosters in Grouper?

Graham: Yes we have a folder for every term. Each semester has a folder for each department

Erica: Are you using an API from Banner?

Graham: We are PS shop and we have loader jobs from them and it dumps it into groups that we build it.

Gail: What builds that feed?

Graham: Magic? We don't really know as some have retired and it's an older system and we have lost some people. We are working on addressing that issues. We are trying to get more real time updates from them as we can. We are working on an ERP replacement.

Bruce: Did you say you build the list on the course you are pulling from the student data?

Graham: We won't see a course until there is at least one student in it. We are trying to get more data into Grouper as we can see these groups before one student is in the course. Our data is the employee side is not fine grained. Is someone on paid leave still active? We are trying to have those conversations to articulate what we want and what we need. The departments are building out the reference groups to help us catch these issues. I got a person over here and another over here and i build a composite of those groups it will not show it appropriately. We want people to use data driven decisions instead of manually doing these.

Graham: I'm curious is anyone else is doing this as well? Are you letting everyone into grouper?

Chris B. (Minnesota): we have a loader job; that adds all users who have update or admin on any group to a Grouper Access group that protects Grouper itself (Shib attribute for UI, LDAP attribute for WS (mod_ldap)).

Gail: we are currently using a homegrown for maillisting type group. It's thrown into where it needs to be and trying to figure out how to it may fit into grouper for access control and happy hour mailing list. I'm interested in your UI

Graham: We use to have them in a list and our marketing wanted specific lists. The major email provider made changes where we use to do forwarding to external emails but they told use we couldn't do it anymore. We turned off that ability and turned to Simple List. It's separate from grouper and a manual update.

Graham: We are a microsoft Shop and didnt want to put Google on there. There is a mail list folder and get their lists from that folder.

Chris H: so you simplified it so it only has one name

Graham: They all have one name and distribution groups you only need to know the email address.

Chris H: So only certain people can make course groups?

Graham: Yeah so only instructors can only request course groups?

Chris H: The staff is okay with that?

Graham: In grouper we don't expose the course groups/folders. You have to ask for access. They can go in and create a group called geography 101 that's not a course group and that would be exposed.

Gail: Still goes through the approval process?

Graham: Yes, staff or faculty requests a course group it gets automatically done.

Kevin (RIT): I like requesting the course group because we just make them all for the previous 2 terms, current, and future 2 terms. It has current past and future and we have almost 200k groups a semester. Nobody really uses them

Graham: We make them but they do have to ask for access if they want it. Most courses will have more than one and a staff will create a new one and we are forcing one distribution group per course to try and clean that up.

Kevin: What we do from our internal system is prefixes Library - WSL - every group you create has to start with that prefix.

Graham: The actual group name has the prefix?

Kevin: Yeah has to be in the name

Chris B.: We give them access to the security groups that control access to the manually maintained groups they have to control and they don't get to touch the reference groups and we set the attributes for the provisioning policy groups.

Graham: We create a bunch of folder structure and turn over control. The reference groups get automatically connected. They can do whatever they want inside. It has been good and bad. People are falling back on what they know with maillists and we are trying to retire that and get them to follow the grouper guides.

Graham: We throw back requests telling them they are doing it wrong and it is up to you. We give them the tools and they need to learn how to use them.

Chris H: Your UI is very focused on your use case...GSH templates that have more wizardry type things (referencing things they may want to change/update their UI)

Graham: The way we built the request process is very similar to the one we have now. We have one screen and send the request and it's very simple and we try to maintain that.

Martin: We use UIs for accessibilities for ADA is this something that is a driver?

Graham: We haven't put it through ADA yet but that is on the list. We wanted the path of what would be the least confusing to users.

Chris H: Chasing wack a mole with special requests on the UI features

Graham: We are trying to keep a handle on the requests and looking what people are asking for and are very critical. Is it needed for business processes? It's a balancing act.

Chris H: Are they exchange groups provisionable?

Graham: Not yet, they all live in a specific part of resource app exchange groups. We are looking to provisionable.

Graham: Trying to let them manage these groups without a UI would cause problems as they would have to go to different areas to change access to certain things.

Graham: We do checks for requested groups to make sure it doesn't collide with any other naming schema within the university. We have had this happen with students and they will try to create a mail list for themselves to use their gmail.

Chris H: Do you want groups in the folder with an extra tab with features?

Chris B: Drop down on the choose actions?

Graham: We make pretty heavy use of GSH templates. All that info from the form gets pushed into a GSH template and creates the group

Chris H: We had course bloat as well. Very small percentage was used and switched our ERPS and didn't realize they weren't being populated anymore and only 3 people have complained. I'm hoping with ABAC you can build a policy with the attribute assignments and term = current term and things like that. I can understand you only want admins or updaters to access this UI. You are cutting off a feature set. Not that they need to get to everything

Graham: We have done that for a couple departments but we are looking at that as people get more comfortable with it.

Chris: Main challenge with student searches show other students and it's not supposed to do that. I can see a separate instance for them to show other things.

Chris H: You cant have the right descriptive value to show you the right John SMith

Chris: We can show the netID which is unique and the user has to figure that out.

Chris H: staff you can see the dept/title, if you're a student worker is gets more complicated.

Graham: Security by obscurity. It's querying our LDAP for users and reads the privacies fields. I can query by name, primary email. My query as a user you wont show entities that are private.