

Georgia Tech Tackles Membership Intersections in Grouper

As background, Georgia Tech's Information Technology Group (ITG) has been working on a project to integrate Grouper with their Door Control system. They have utilized Georgia Tech's Identity and Access Management (IAM) department's internal ESB, BuzzAPI, as a proxy to Grouper's Web Services. Through BuzzAPI, ITG can maintain special Door Control Grouper groups that leverage reference groups sourced from GT's LDAP (GTED). ITG's Door Control groups are then provisioned back to GTED as entitlements. ITG's Door Control software can then read ldap entitlements to determine a person's access to a door. ITG has also built UI's for viewing a person's Grouper memberships as well as for allowing admins to create memberships through their custom UI.

A problem has surfaced recently in ITG's UI when creating memberships. They would like to be able to add multiple people to groups at once and at the same time add a group as a requirement, or condition, of membership. To make the selection of the conditional group easier, they are using Grouper Web Services (proxied through BuzzAPI) to find all the groups that the selected population have in common. The goal is to then present the intersection of groups as a selection set for the admin user to choose as the conditional group(s).

There have been a couple hurdles to this process that will require some thought. Firstly, ITG is using Grouper Lite Web Services which can only be called for one person at a time in order to retrieve their memberships. When you have many people's memberships that you are trying to retrieve, store, and compare, the resulting response time isn't desirable. Secondly, the memberships that would be used as conditions, like affiliation with a given department, are sourced from LDAP. An idea was floated to first query these affiliations from LDAP for efficiency's sake and then translate the LDAP affiliations to Grouper group names. The problem therein lies with the fact that our LDAP affiliation names do not intuitively match their corresponding Grouper group name which makes it difficult to build a successful Web Services call to create the conditional membership.

To get around these problems, there are multiple solutions that we are looking into. The most attractive option may be to use Grouper's Batch Web Services that allow for multiple subjects to be queried at once. This may create efficiencies when trying to retrieve all the common memberships in Grouper for a given selection of people. The other option would be to store the exact LDAP affiliation name in Grouper alongside the resulting Grouper affiliation group. This is already being done in the Grouper group description for these affiliation groups, but we might be able to make it more visible by storing it in a custom attribute or somewhere where it could be queried more easily.

The GT IAM and ITG teams will continue to look into good solutions to this problem of finding membership intersections for large groups of people. There may be a much easier way to do this that we haven't discovered. Please feel free to leave a comment if you have encountered similar issues and ended up solving them. We'd love to hear from you.