Groups session

Grouper, Google Groups, federated groups

Chris Hyzer: 3 topics: What's new with Grouper and how to use it. Google Groups. Federated groups, roles, and calendaring.

Scott: On Grouper: Particularly how to use attributes. UNC Chapel looking at that.

Chris: Release notes from Grouper roadmap reviewed. 1.5 in winter. Added: Light one-screen UI for easier administration links from other applications. (1.6 added skinning and replaceable text.) Auditing. Move and copy (along with underlying permissions, etc.). Notification. (1.6 optional notification of flattened group.) New attribute framework, with attributes supported on virtually any entity (including attribute assignments). Roles and permissions built on attribute system: role a group associated with permissions. Not just RBAC, though: permissions can also be assigned to individuals. Permission triple: subject + qualifier + resource. Shibboleth integration: attribute resolver. Performance improvements, membership dates.
1.6 on its way out now. Subject support. Context-based groups. ESB built from notification engine: send XMPP message or contact this web service address on specified events; listen for events from external system.
On the Roadmap, maybe by next winter: Permissions and attribute UI. Integration with uPortal, and possibly dependency of uPortal on Grouper. Improved auditing and reporting. Penn will try to deploy always-available Grouper web services. Rule-based actions: for example, negotiated merges like "if member explicitly removed, don't automatically re-add member."

Richie: Permission managment = privilege management over resources?

Chris: Yes. Already a concept of "privileges" for Grouper-internal actions, so a different word for external applications' use. Goal is high efficiency for resolving all hierarchies. E.g., a role can inherit permissions from another role; resource structure hierarchies (if you can read all documents in English Dept., can read document in English 101); hierarchy of permissions themselves.

Steve: Integrating Grouper with Google Apps Ed?

Chris: Later. How to use attributes?

Scott: Trying to map to Grouper attributes. But where is best to apply them?

Chris: Type and attribute definitons used to be effectively global. Can now define attribute permissions within folder tree without polluting other spaces. Attributes on folders sounds good. Might be able to re-use for rules. Possible issue of overloaded attributes being dealt with by UI.

??: Tagging attributes to cut across hierarchy?

Chris: One of the goals for the feature. "These are for this application; these are for students..." "Domain" attribute type in there for that sort of tagging. // Hope to see use cases and potential solutions discussed on the wiki, maybe with sample Grouper shell code.

Steve: We're upgrading to 1.6 this summer.

Chris: Not tracking who's using what version right now. Would be good to do that.

Ray: I'll trawl on the Grouper user list.

Liz: How can a group be "a loan officer"?

Chris: "Loan officer" would be a role, which is a type of group with permissions. Periodically you might export permission info into your app DB, or you might ask web service at runtime for permissions. Supports "act as": can prompt users to decide what role they're playing.

??: Using Grouper shell to test 1.5. Will there be a UI for attributes?

Chris: Not in 1.6, but hopefully in next release. That's the delay on removing old attributes. // Now for Google Groups.

Steve: Growing number of campuses signing for GAE. Sites and Docs. In last 12 months, the services have evolved rapidly. How can campus IT make it easier to use course-related and other complex group-role data in GAE? Some schools just bringing over their course enrollments. U. Washington doing something like this in Fall.

Rob: GAE draws people with Google identity as opposed to site identity.

Steve: Not always. NISL working group has everything in Google Docs, and Steve's the only one from Brown.

Rob: Is part of this federated ID? Which would be Grouper's involvement?

Steve: Can thank the COmanage team for trail-blazing on federated management. Federated groups part of the Brown roadmap. How to bring SAML-enabled InCommon members into Google even if they don't have contracts with Google?

Rob: Any possibility of Google joining InCommon?

Randy: If every Google Apps user needs a Google domain account, how would it be done?

Val: If your domain is integrated with Google Apps, you get prompted to log in at your institution.

Randy: We use SAML to get into Google, but either need to stay within that domain or use Google domain?

Val: If there's another school that uses SAML for integration, you do seem to get IDed by your original institution when crossing domains.

Dave Hicks: We're integrating our groups into Google: filter our info, put it into Google to create groups. If multiple domains (students vs. staff), need shared sites. Still pretty flakey on group management when crossing domains. Every night reconciles based on course enrollment. In production for a couple of months. Instructor able to email class, for example. Couple of bugs, but GAE just today announced better cross-domain support. SQL data is source. Besides students, uploading "natural groups": departments, ad hoc groups, query-based groups. Transaction-based updates to provisioning. No guarantee on fast response at Google, though. No API to find a single shared contact, have to loop through list.

Steve: Any issues with policy controls?

Dave: Haven't seen that yet. Some differences on nested groups, though. A group that contains another group: you have to be an owner of the subgroup to mail to its members. Can protect membership list from other members.

Ray: NYU is trying to federated with Grouper and then feed into Sakai and Xythos authz.

Randy: Calendaring is another story, though. All users in calendar event are visible by default, and you'd have to override by individual. Until just recently couldn't hide people from Directory, either.
Federated groups, roles, and calendaring.

Chris: Are there features that need to be added to Grouper to make this easier?

Steve: Currently what's needed is to replicate COmanage model. Someone who comes in from another campus gets noted, and then a group administrator finds them and adds them.

Ken: Two concepts: two groups from same source share a resource. Lygo, a physics group in the USA has an offshoot in Italy; something similar for COIN. Want to replicate group in different contexts.

Steve: Might want membership of one group copied into another Grouper instance.

Rob: If there's a composite on the target side?

Chris: How to handle it would be up to the replicater. First step is usually to support external users in internally managed groups?

Steve: Registration, invite, bulk load all make sense.

Chris: Only needs to know subject to add to group or add permission. Can use your IdM or the internal Grouper as source of subject. Does anyone but COmanage have external users in Grouper?

??: *Yes, but didn't catch details.*

Steve: How many people having to deal with federated membership? Get many requests from researchers and faculty to open up access to wikis or course management system. Answer so far has been to issue guests a Brown ID.

Just a few. For library resources, for example.

??: Aren't there some Dutch developers federating with Grouper?

Jim Green: We have GAE integration via SAML.

Steve: Heard complaints about how Google API is throttled down.

??: The throttling is one reason we were interested in just-in-time provisioning, as a workaround for not being able to provision all classes.

Randy: After four or five threads, performance declined rapidly.

Will: In some other APIs, performance guidelines are published. Worth checking into.

Dave: If you enable Google Groups for your domain, people can remove themselves; their nightly reconciliation undoes that.

There was a successful post-session experiment with cross-SAML sharing in GAE.