Grouper conceptual entities in SAML assertions and in repositories

David Langenberg, U Chicago:

One of our offices, the College Programming Office (CPO), has a fairly complex set of web apps and content sites which are managed by a small set of admin users who then need to delegate lower levels of access out to other users on a site-by-site basis.

The levels of access that are involved include, but are not limited to:

1. Global admins - those who have full admin on all sites and can add users
2. Global users - those who can access all sites, but can not add other admins
3. Site admins - have full access to one specific site
4. Content editors - have some limited privileges to modify existing content on a site
5. Site-specific users - may have access to some small section of one site

Currently all of these sites use LDAP logins for access, but the administrative privileges have to be managed on a site-by-site basis. With an office that includes many FTE's and also a staff of 6-8 student employees who are changing on a yearly (or more frequent) basis, the management of these user tables can present a significant challenge.

If we were able to map out a specific set of privileges and specify them in one central location, adding, removing, and modifying users as they change, it could definitely save significant staff hours.