Using Grouper to manage AD permissions

A Duke Use Case
AD Distributed Control Use Case

- Campus-wide AD forest into which departmental admins wish to migrate departmental forest assets & ZenWorks assets and manage Unix/OSX resources
- IDM-maintained user identities with “mix ins” by departments; departmentally-maintained resources and ad hoc affiliates
- Need to manage high privilege for departmental resources and constrained privs for users; interfaces for non-Windows users
Central = Blue
Departmental = Green
Note overlap
Groups and Roles

- Globally
  - Managers (duke:employees:managers:all)
  - IT Admins and Managers (duke:employees:it_managers_and_admins)
  - IT Admins (duke:employees:it_admins)
  - IT Managers (duke:employees:it_managers)
Groups and Roles

- Departmentally (ex. within the folder duke:orgs:TrinityCollege:A&S:Chem)
  - Members
  - IT Admins system of record
  - IT Managers system of record
  - Include and exclude groups
  - IT Admins
  - IT Managers
Permissions and Resources

- Resources to map AD OUs
- Permissions grouped into permissionSets by default
- Actions qualifier used. For instance “full” or “updateHomeDirectoryAttribute”.
- IT managers can modify permissions on their OUs
  - (IT Admins(chem), full, dept(chem))
  - (IT Admins(chem), updateHomeDirectoryAttribute, people(chem))
Oracle Identity Manager

Updates to employee attributes

Updates to "dynamic" groups based on employee attributes using Grouper Web Services

Grouper UI
Managers update list of admins

Manager UI
Managers update permissions

Perms View
GROUPER
Change Log

Update Access on OUs in ou=Dept
Update AD Groups

Active Directory

Admin UI
Admins update attributes in ou=people
Actors and a short demo...

- **Actors**
  - Rob (nobody)
  - Shilen (Chem IT Mgr)
  - Hiro (Tech Svcs IT Admin)
  - Bill Day (a Chem user)
  - Dr. Prissant (another victim)

- Shilen uses OIM to make Rob a Chem user w/o privs
- Shilen adds Rob to IT Admins includes granting him control over some Chem resources automatically
- Hiro can access AD, but has no rights in Chemistry
- Shilen grants Tech Services control rights in Chemistry (via Grpr Perms)
- Hiro can now control Chemistry resources in AD (and users in UI)
Actors and a short demo...

- **Actors**
  - Rob (nobody)
  - Shilen (Chem IT Mgr)
  - Hiro (Tech Svcs IT Admin)
  - User X (a Chem user)
  - User Y (another victim)

- Shilen uses OIM to make Rob a Chem user w/o privs
- Shilen adds Rob to IT Admins includes granting him control over some Chem resources automatically
- Hiro can access AD, but has no rights in Chemistry
- Shilen grants Tech Services control rights in Chemistry (via Grpr Perms)
- Hiro can now control Chemistry resources in AD (and users in UI)