Grouper at the University of Minnesota

Christopher A. Bongaarts
Grouper Virtual Working Group
May 20, 2013

UNIVERSITY OF MINNESOTA

Driven to Discover℠

In the beginning…

- Grouper 1.2.1 in production August 2008
- Driver: BPEL access management for Enterprise Financial System project
  - Using LDAP groups to represent roles
  - Wanted UI with delegated administration
- Similar desires for helpdesk access to user management interface

Timeline, continued

- Upgraded to 1.5.2 in March 2010
- Switched to UW LDAP source adaptor April 2010
- Upgrade to 2.1.3 planned for summer 2013

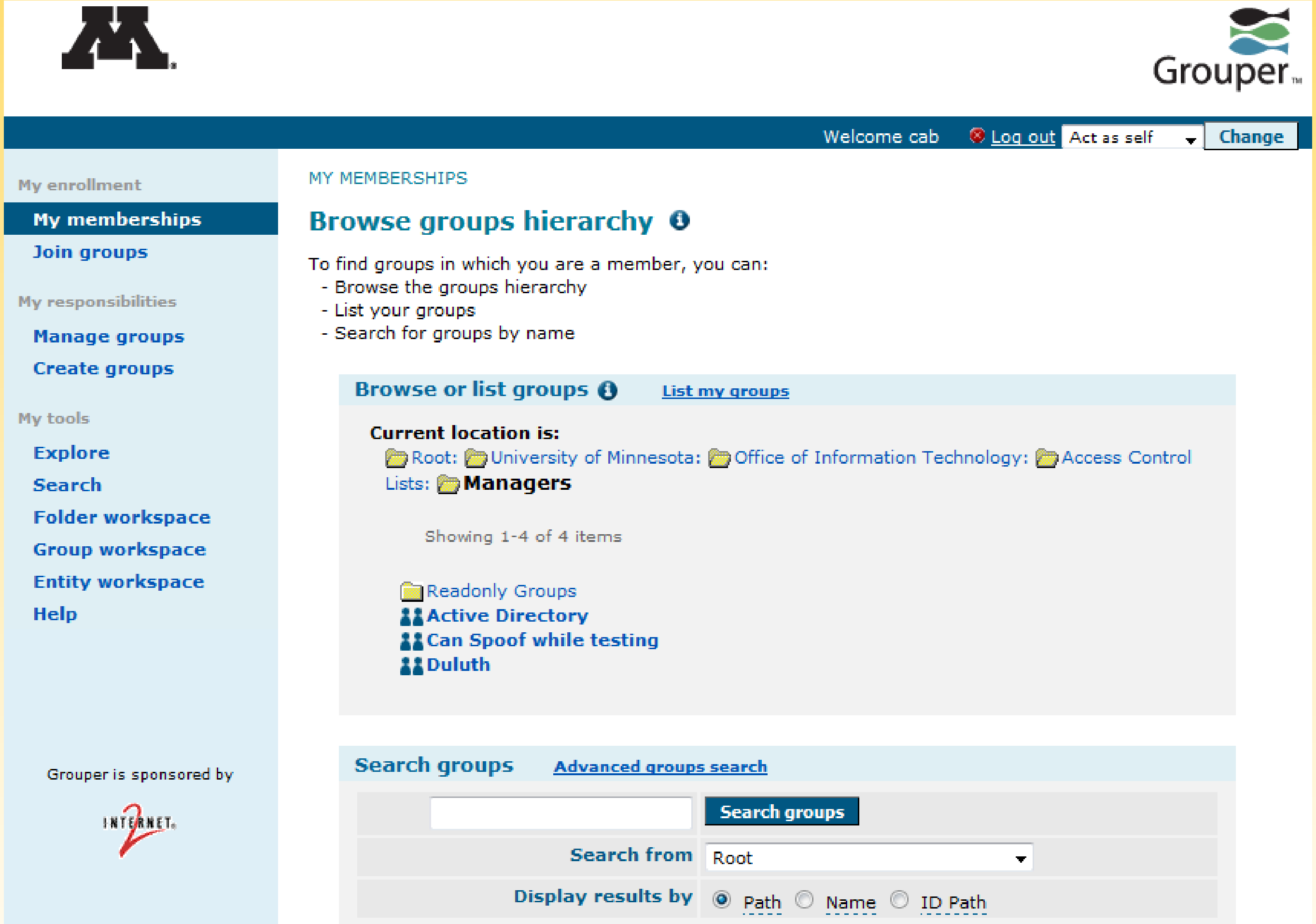
Applications using Grouper for access management

- BPEL workflows
- Helpdesk account management
- WorkFlowGen
- VPN groups
- Oracle Business Intelligence (OBIEE)
- Various departmental sites

Other uses

- Google Apps provisioning
  - Overrides for health care component
- Netfiles (Xythos WFS) central groups
- Identifying test directory users

Example group



Welcome cab Log out Act as self Change

My enrollment
- My memberships
- Join groups

My responsibilities
- Manage groups
- Create groups

My tools
- Explore
- Search
- Folder workspace
- Group workspace
- Entity workspace
- Help

Grouper is sponsored by

MY MEMBERSHIPS

Browse groups hierarchy

To find groups in which you are a member, you can:
- Browse the groups hierarchy
- List your groups
- Search for groups by name

Browse or list groups

List my groups

Current location is:
Root: University of Minnesota: Office of Information Technology: Access Control Lists: **Managers**

Showing 1-4 of 4 items

Readonly Groups
Active Directory
Can Spoof while testing
Duluth

Search groups

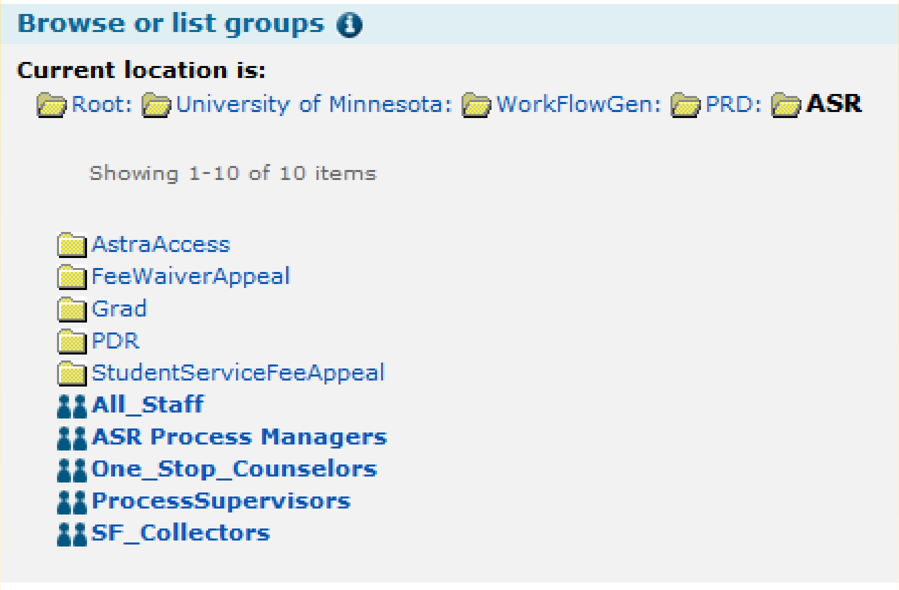
Advanced groups search

Search groups

Search from: Root

Display results by: ● Path ○ Name ○ ID Path

Another example group



Browse or list groups

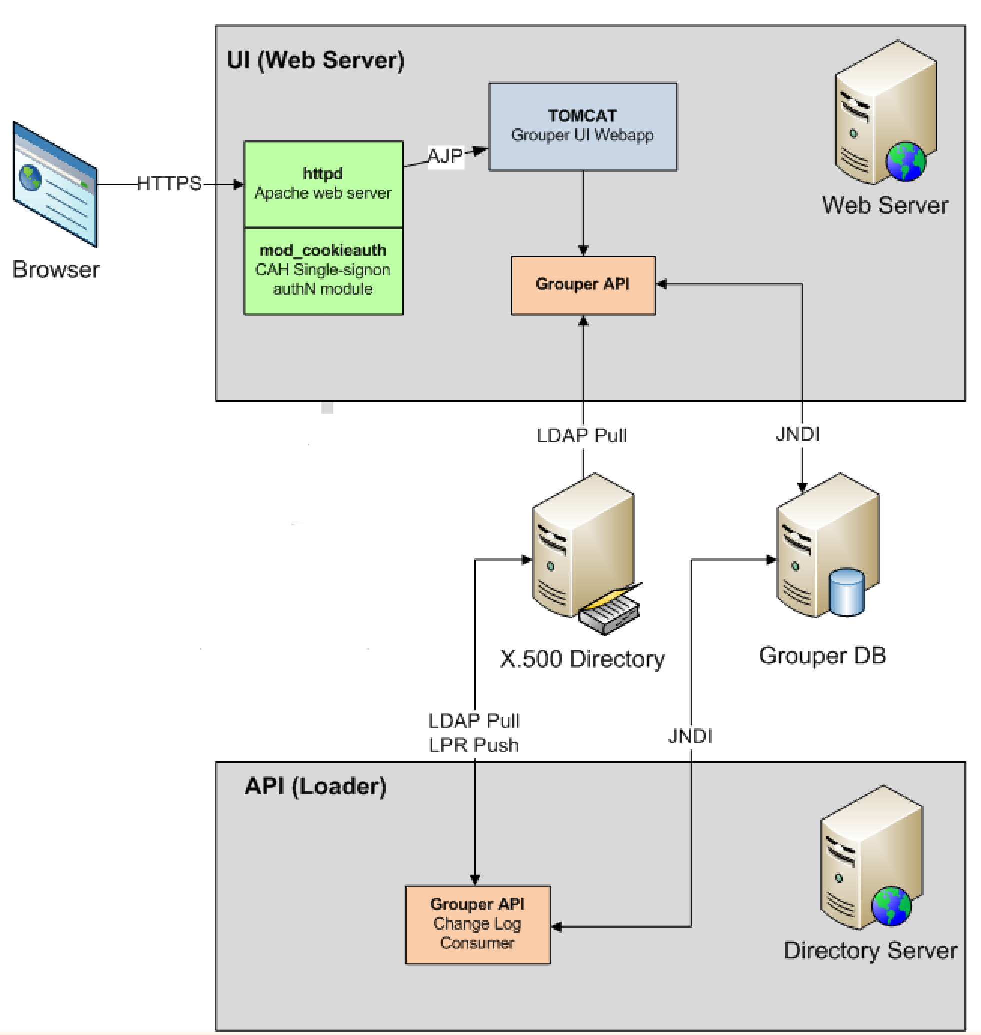
Current location is:

Root: University of Minnesota: WorkFlowGen: PRD: **ASR**

Showing 1-10 of 10 items

AstraAccess
FeeWaiverAppeal
Grad
PDR
StudentServiceFeeAppeal
All_Staff
ASR Process Managers
One_Stop_Counselors
ProcessSupervisors
SF_Collectors

Deployment Architecture



Access methods

- Group management via web UI only
  - Requires two-factor authN (OTP fob)
- Client access
  - LDAP (expressed as group objects, isMemberOf)
  - Shibboleth (SAML isMemberOf attribute)
    - Gets data from LDAP
    - Attribute filters with stem regexes work slick

Directory provisioning

- Using Grouper Loader changelog API
- Locally written Java class sends updates to person registry database
- Person registry pushes updated group data to LDAP directory

Future directions

- Investigate using the PSP for LDAP provisioning
- Create local documentation
- Encourage more applications to use Grouper for access control

Contact

Chris Bongaarts
Identity Management
University of Minnesota
cab@umn.edu