Agenda

2. Questions & topics you wish to be addressed today
3. Grouper v2.0 time frame & highlights (Shilen & Chris)
   - Point-in-time audit demo
   - Member sort & search
   - Attribute UI
   - Upgrading to v2.0
   - Invite external users
   - syncing groups between Groupers
   - Atlassian connector
4. A discussion about LDAP provisioning kicked off by Lynn Garrison
5. Questions & topics
4. evolution of ldappcng
What’s new with Grouper

Internet2 Spring Member Meeting
Chris Hyzer
Agenda

• Attribute framework UI
• Upgrade from 1.6
• Penn’s Secure Space – implementation of Grouper external users / rules
• Group sync to another Grouper
• Atlassian – Grouper connector
Attribute framework UI

• Attribute framework UI is an ajax UI (similar to lite membership screen)
• Creates, edits, assigns attributes
• For Grouper 2.0
• Currently in SVN, you can create attributes, names, hierarchies, privileges, roles, role hierarchies, actions, action hierarchies etc
Attribute framework UI (continued)

• Attributes and actions
• Attribute privileges
• Attribute names (including hierarchy)
• Groups and roles (including hierarchy and privileges)
• Attribute assignments (to do)
• Permission assignments (to do)
Upgrade from 1.6

- March 2011 Penn upgraded from 1.6 to 1.7
- 1.7 is an internal Grouper release with point-in-time, rules, and external subjects
- Upgrade took 5 hours (including testing)
- Performed on a Friday night at 5pm
- No significant downtime required for readonly services
- Link to wiki (TODO)
Upgrade from 1.6 (continued)

- Disable nagios monitoring on WS
- Select counts of tables for post upgrade sanity
- Set UI / WS to readonly mode
- Turn off daemons, ldap sync, etc
- Backup membership lite view to a table (not necessarily needed for this upgrade)
Upgrade from 1.6 (continued)

• Backup DB schema (DBA)
• Increase tablespace for schema
• Backup old webapp dirs on UI / WS / daemons
• Clean out old entries from the change log
• Analyze tables
Upgrade from 1.6 (continued)

- Generate Grouper DDL upgrade script from GSH
- Move the drop views part toward the end (works for oracle)
- Disable indexes to make the upgrade script go faster
- Run script
- Enable indexes
Upgrade from 1.6 (continued)

• Add EPPN to Penn person source table and sources.xml
• Copy new build to WS/UI (note Penn has build script posted on wiki to manage envs)
• Check SQL counts
• Enable nagios, read/write mode, ldap sync
• Test
• Publish new version of client, send notifications
Penn’s Secure Space

- Penn launched Secure Space in Fall 2010
- Initially it was for PennKey holders only
- Momentarily we will release a version which supports external users (via Grouper)
  - Next week?
Penn’s Secure Space (continued)

• Secure Space is built on Grouper with three groups per space: admins, users, readonly

• When logging in, the grouper client / WS is used to cache the list of groups for user

• On create/delete space, GC/WS is used to create/delete groups

• Group memberships are managed via the membership lite UI screen
Penn’s Secure Space (continued)

• Penn’s Grouper has rules to only allow external users in certain SS folders
• Penn’s Grouper external users must be invited to be able to register
• SS uses InCommon
• EPPN is required for external users
• External users self-register their name, email, institution
Penn’s Secure Space (continued)

• Penn installed Shibboleth Discovery Service (DS/WAYF), customized:
  – Pennify
  – Support channel
  – Make it easy for Penn users
  – Recommend ProtectNetwork for users who don’t have an InCommon account which releases EPPN
Penn’s Secure Space (continued)

• Grouper shows external users with different icon, and description:
  • [unverifiedInfo] First Last - institution
  • [externalUserId] userId@institution.suf

• External users do not show in results for groups which do not allow external users

• Demo
Group sync with another Grouper

• Grouper can sync a group with a group in another grouper
• Map the folder/group on one grouper to the folder/group on another grouper
• Only one side needs to make configurations
• Both groupers need to use external member identifier (e.g. eppn)
Group sync with another Grouper
(continued)

• Three types of sync’ing:
  – Push (full cron)
  – Pull (full cron)
  – Push_incremental (full cron and diffs real time)
  – The source needs WS credentials to the destination, also rights to read/update the group
  – Only external members are sync’ed (not subgroups or internal subjects)
Group sync with another Grouper
(continued)

• Example on the Grouper demo server
• Two instances of Grouper 2.0 running, publicly updatable groups, can see it sync across
Atlassian – Grouper connector

• Penn using in production since Dec 2010, requires Grouper 1.6
• Implements the OpenSymphony osuser interfaces:
  – Credentials provider (optional?)
  – Access provider
  – Profile provider (optional?)
Atlassian – Grouper connector (continued)

• Map a root folder for Confluence or Jira
• Groups (unnamespaced) are in that folder
• Can create/delete groups from atlassian, though sometimes there are issues... we just create/use from Grouper
• XMPP messaging from Grouper to Atlassian for real time updates
• Fail-safe cache so if Grouper is down, Atlassian is up
Atlassian – Grouper connector (continued)

• If you have LDAP groups with memberOf and member, you can use Atlassian LDAP groups
• If not, you can use this
• Two-way editing is nice (if it works)
• If no anonymous access, there is a REMOTE_USER authenticator too