PennGroups Intro / HA / UI

May 2014
Agenda

• Introduction to PennGroups (Grouper)
• Recent use cases
• Recent improvements in availability
  – Architecture
  – Client failover between WS and LDAP
  – New readonly WS server offsite
  – DNS failover for readonly WS
  – Client failover between WS onsite and offsite
• New UI
  – Description
  – Bake-off
Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify and make consistent by using the same group or role in many places

**Physics 101 Course Group**

- Email Group
- Wiki Access
- Lab Reservations
Additional benefits of access management

• Empower the right people to manage access. Take central IT out of the loop.

• See who can access what, with a report rather than a fire drill
Grouper: core concepts

- Folders in hierarchies
- Group
  - Direct members
  - Subgroup
    - Indirect members
  =  \( \mathbf{\cap} \)
  - Composite groups
Security & delegation

- Create groups
- Create subfolders
- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation
Beyond groups

- Attributes
- Roles
- Permissions

Attribute definition
Permission definition

Role inheritance
Delegation model extends that for Groups
Grouper integration

Identity Management
- Shibboleth IdP
- Persons Orgs
- LDAP

Application
- SAML
- LDAP
- Grouper Client
- SOAP
- REST
- Web Services
- UI

Grouper
- Java API
- Grouper Loader
- Grouper Database
- Grouper Shell
- XML script

JDBC Source Adapter
- JNDI Source Adapter

Systems of Record
Recent use case - Canvas

- Needed to lock out half of the users of canvas during maintenance
- Created two large ad hoc groups by importing CSV’s of pennids or pennkeys
- The WebLogin team configured Shibboleth to make this happen based on the group
- The service owners could edit the group memberships
Recent use case – License change

• An application needed to change its user base
• Used to be all IT staff
• Now should be IT staff minus 3 centers
• Orgs and centers were previously loaded into grouper
  – Created a new overall group for application
  – Marked it as “include/exclude” type
  – Added itstaff to the includes
  – Added 3 centers to excludes
  – The WebLogin team changed the application Shibboleth configuration to point to the new group
PennGroups access options

• WS
  – Full featured, lots of queries
  – Real time up to date
  – Read/write

• LDAP
  – Updated nightly
  – hasMember and getMembers (not memberOf)
  – Readonly
  – Fast

• SQL
  – Not typical
  – Large exports

• SAML
  – At user login time
  – Only hasMember for groups which are allowed to be sent to SP
  – One hour delay, locally cached in authn system, highly available
Client failover between WS and LDAP

Try WS or LDAP, if error or timeout use the other one.
Client failover between WS and LDAP

- The FAST framework from ISC has done this for years
- Never had an outage
- The logic only does failure failover, not timeouts, need to change that
New read-only offsite WS

![Diagram of WS server 1 connected to Main Grouper R/W DB, ISC data center, one-way replication to WS server 2 in readonly mode, and Grouper readonly DB in Sungard.]
Client failover between WS’s

Try primary connection first

If there is a timeout or error on primary, and if it is a readonly query, then try this connection

One-way replication

1. WS server 1
2. Main Grouper R/W DB
3. ISC data center
4. One-way replication
5. WS server 2 in readonly mode
6. Grouper readonly DB
7. Sungard
Discovery

- Grouper high available client has discovery
- Allows the service operator to configure which servers are available
- Penn is not currently doing this, but we could
Discovery

Hi! optional discovery web server every 5 minutes to get WS server configs.

Secondary discovery web server

Try primary connection first

If there is a timeout or error on primary, and if it is a readonly query, then try this connection.

WS server 1
Main Grouper PAM DB

One-way replication

Datacenter 1

Grouper readonly DB
Datacenter 2

WS server 2 in readonly mode
Grouper client

- One java jar with no dependencies
- Can be used as library or command line
- Does LDAP and WS
- Failover between WS on failure or timeout
Failover comparison

• LDAP or WS
  – Single points of failure, manual fixes might be required for outages

• LDAP/WS failover
  – Only works for LDAP queries, LDAP has daily update and might have stale data, need logic in app

• DNS based failover
  – Few minutes of failover for polling and TTL, secondary server could have stale data though is generally real-time

• Client based failover
  – Readonly queries, need logic in app, 2nd server could have stale data though is generally real-time
Failover demo

• Try the client for each server in test env
• Try the DNS name
• Turn off primary
• Try DNS, see error
• Try client for each (see one down)
• Try client failover (see warning)
• Try DNS (is it done yet?)
Failover summary

- Make sure you are on penngroups-users listserv
- Email penngroups-help and let us know you are doing it
- 2\textsuperscript{nd} offsite WS is new, experimental, might change
- DNS load balancing is new, experimental, might change
- Data is generally real-time up to date, but replication could fail for some time
New PennGroups UI

- Penn uses Grouper 2.1
- Grouper 2.2 will be released soon
- Has a new UI
- Admin and Lite UI still shipped
- New UI does not completely contain all logic in the admin and lite UI (maybe it will in 2.3?)
- Accessible and mobile friendly
- Lot of UX design and studies
New UI features

• Tree control
• Dashboard
• Favorites
• Recently used
• Services
• Analyze membership
• Bulk assign
• Ajaxy (but bookmarkable and backbutton friendly)
New UI vs old

- Add group to user
- View/assign privileges
- Deprovision quickly
Fin

- Thanks
- Email penngroups-help@lists.upenn.edu for info
- This pres will be on the penngroups page (google it)
- http://www.upenn.edu/computing/penngroups/