User Management in sPHENIX

It only sounds easy

What's the problem we are trying to solve?

- Scale and frequency of changes
  - sPHENIX has hundreds of collaborators
  - New collaborators show up, others leave at a rate of a few per week

- Authentication + Authorization
  - Access to sPHENIX computing resources (cpu, disk, tape)
  - Access sPHENIX web pages and services (gitea, invenioRDM, email lists, indico,...)
    - Outside BNL: github
  - We do need fine grained access controls (e.g. various roles in InvenioRDM, email admin, indico,...)

sPHENIX Approach

- sPHENIX decided from the beginning that every collaborator has to have an sdcc account to access services and work on sPHENIX.
  - Basic access permissions based on the sphenix unix gid
  - Initially sphenix gid was added to existing RHIC user accounts
  - Later separate sPHENIX accounts were required
  - Now we are back to being able to add the sphenix gid to existing accounts

- scdf run services (gitea, wiki, access to protected web pages) work for us
  - That took a lot of behind the scenes effort by scdf which is appreciated
  - sphenix gid provides default access permissions
  - Other authorizations (e.g. gittea repo write, wiki admin) handled separately for each service
    - rarely changes

- Hpss uses separate accounts
  - There are some good reasons for this

- Removal of access automatic when account expires (or user account gets blocked on request)

Authorization issues

- Services not run by sdcc are not hooked up into this
  - Indico
    - Every user has their own account
    - Access control done via adding accounts to indico roles
      - Adding accounts as collaborators join is done by whoever gets the mail, removal of collaborators who have left – not so much
  - Mailing Lists
    - Every list is its own universe, admins get notified of subscription request
    - No removal of collaborators who have left (though undeliverable addresses get purged after many tries)
  - Github
    - Authorization maintained by hand
    - Only PRs by collaborators are allowed to trigger Jenkins which runs in scdf
      - You don’t want random code compiled and run inside scdf, even if it’s inside a sandbox

InvenioRDM

- sPHENIX's central document repository
- Needs fine grained roles and groups (admin, review committee member, paper preparation group member,...)
- Groups and their membership should be controlled by the collaboration (just not practical to do this via tickets)
- That's where the phone book comes in
  - Though the principal access is still via the sphenix gid, if the account is locked that collaborator won't have access

Quick Summary

- We have come a long way, I can remember when I had 4-5 accounts for various rcf services
- In general the unix gid based authorization works well for us
- ltd run services are not integrated, InvenioRDM needs attention

- Being able to centrally remove access for a given user can is important
  - It is rare – happened once. But it took about a week to remove the access to PHENIX internals for them.