

# XaaS Challenges for (federated?) ID Management

Warren G Anderson (LIGO)

16th FIM4R Workshop & TAGPMA

# XaaS in Research

- Researchers depending increasingly on “X-as-a-Service” (XaaS) offerings
  - Cloud services (e.g. AWS) for “hardware” (cycles, storage, ...)
  - Code repositories (e.g. GitHub) for development and deployment
  - Office application suites (e.g. Google Workspace) for communication and collaboration
  - Data sharing (e.g. Zenodo) for dissemination of results
  - ...
- Upsides - many, but include
  - Quality of service often better than research organizations can provide internally
  - Free/cheap for individuals or small groups
  - Let researchers focus on the research problem
- Downsides - many, but include
  - Creates challenges for identity management

# Case study #1 - AWS, keys and scaling

- Multi-institutional research group developing infrastructure on AWS
- Using COmanage for identity management
- OIDC authentication to AWS console
- Onboarding through COmanage enrollment.
- Offboarding in COmanage:
  - AWS account not expired
  - However, no more OIDC authentication
- But ...

# Case study #1 - AWS, keys and scaling

- Researchers use CLI tool to develop and deploy (Terraform)
- These tools use the AWS API interface
- Developers create long-lived API keys to authenticate
- Offboarding now requires
  - Notification of AWS admin when offboarding occurs
  - Manual action of AWS admin to revoke API keys
- Manageable when there ~ 10 researchers, but ...
  - ~ 100 researchers?
  - ~ 1000 researchers?
- Is there tooling for handling this that I just don't know about?

## Case study #2 - The medium-sized collaboration

- NSF project involving ~ 10 universities with about 30 scientists
- Developing proof-of-principle cyberinfrastructure for astronomers
- Two years to get community buy-in and seek funding for a permanent virtual facility
- Astronomers and computer scientists from various external projects contributing
- Too big and ambitious to not leverage enterprise tools
- Too small to stand up infrastructure internally or purchase enterprise licenses
- So ....

## Case study #2 - The medium-sized collaboration

- Even though there is a CILogon subscription for federated identity management
  - Code development in “personal” GitHub accounts
  - Documents in “personal” Google Drives
  - Messaging in free Slack instance
  - Mailing lists in Google Groups
  - ...
- Onboarding requires involvement of a half dozen people
- Offboarding never happens from half of the XaaS tools
- Is federated identity management the “right” approach for medium sized (> 10 but < 100) people?
- Is migration to a more traditional federated identity environment feasible when this approach isn't scalable anymore?

# Conclusions

- XaaS tools are becoming standard for researchers
- Free/inexpensive versions are aimed at individuals or small groups
  - Don't support external identity sources
  - Actually vying to be the identity provider for other service (GitHub, Google, ...)
- Enterprise licenses aimed at commercial companies
  - Usually support external identity sources
  - Often too expensive for research budgets
- Researchers will use whatever helps them get through the next grant cycle
  - And they will jump through some hoops in the process
- Is there any way to give researchers the benefits of modern XaaS that is economical, scalable and supports FIM?