IRIS Identity and Access Management

Edinburgh IRISathon
12 January 2023
Jens Jensen, UKRI-STFC

If the goals of IRIS IAM are

- Let users authenticate with existing IdPs
  - Particularly home organisation
- Proxy users' existing credentials through to all services
- Harmonise attributes and LoA
- Single account management for user and infrastructure for all services
- Single point of attribute management
- User friendly
- Everything is secure
- Good performance and scalability
- Everything standards compliant and interoperable

… then what is missing?

Authenticate to all services

- IRIS IAM gives acces to IRIS cloud
- Not to DiRAC
  - This is D-FED: trialled at Cambridge (Matt R-B) and Durham (Alastair B)
- Not to GridPP?

Use existing IdPs

- Relatively easy to add new IdP to Indigo-IAM
  - Traditionally the problem is with orgs not in eduGAIN
- Need to pass user attributes through
  - Do services see enough attributes from community IdPs?
- What about low assurance IdPs?
- What about MFA support?

Science and Technology Facilities Council

Assurance Levels

- Controlling a telescope remotely is not the same as editing a wiki
- Increasingly hostile online environment
  - Protect infrastructure/reputation against bad people
  - What protection do we have against compromised credentials?

Proxy credentials through

- Indigo IAM supports only OIDC, acting as the OP
- For services that need SAML, Satosa is needed
  - Or use EGI CheckIn
  - Or EUDAT B2ACCESS
  - Or keycloak
- Need delegated credentials
- We can generate X.509 certificates on demand
  - Useful as delegated credentials
  - Users need not know they have them

High Availability IAM

- Goal: set up HA IAM with single access endpoint
- Use technologies developed by EOSC Future for RCauth
  - Three sites host peer Indigo IAM instances
  - Sites synchronise state with Galera over private VPNs
  - HA is achieved through HA Proxies
  - Single access endpoint is achieved with ANYCAST
    - Or alternatively using DNS failover (Särimner by SUNET)
- Needs two other sites (Glasgow, Cambridge)
  - Each site is a full, live peer – no single point of failure anywhere
  - Needs BGP which is the blocking and delated ar RAL

UKRI Science and Technology Facilities Council

User Friendly

- IRIS IAM asks for password on the front page
  - Password should only be used for users with no usable IdP
  - Or for low assurance accounts for testing
- IdP discovery has too many options
  - Though the proxy will remember the most recent selection
  - Potentially multiple redirects
- Notify user of session expiry
- Different logins SHOULD lead to the same accounts
  - E.g. SAFE => DiRAC vs SAFE => IRIS-IAM => DiRAC

Usability
appint (standards and interop)

- Née AARC(2) JRA1, appint provides a means for community techies to define protocols
- Proposals are reviewed by AEGIS
  - Which has representatives from infrared
- How to express community membership/roles
- How a service can provide hints to a proxy
  - Narrowing IdP selection
  - Service AUPs
- Emerging standards still need implementation

Token-based access

- Need delegated credential
  - Allow jobs to act with user's (possibly restricted) abilities
- Need renewal for long-running jobs
  - We can issue refresh tokens
  - But who (what) renews access tokens?
  - Same problem as renewing GSI credentials via MyProxy
  - Except that GSI proxies live much longer (typ $10^6 s$) than tokens (typ $10^4 - 10^5 s$)

Token-based access - PAM

- PAM module should cache login locally (on client side)
  - Can the client save a token into the user's (local) workspace?
  - (There is also KIT's OIDC agent)
- Allow forwarding credentials?
  - Can the module save a token into the user's (remote) workspace?
  - Different from login token as scope is probably different
  - The user would need to authorise tokens twice…?!
  - (Note the sshd is the OIDC *client*)
- We could do all of the above with MEG in NGS
  - MEG = MyProxy-Enhanced GSISSH
  - Kerberos can do it too
  - ssh keys/agent mostly do the same though forwarding is limited to ssh (and the user cannot close their session)

Community AAI

- Some “communities” have their own AAI
  - Example: SAFE
  - Example: SKA prototype AAI, SRC AAI
- Can be linked to IAM as an IdP
- IAM needs to pass authorisation attributes

Scalability and Performance

- Indigo IAM
  - HA-IAM will aid scalability
    - Users go to their nearest available IAM instance
  - Account creation: Still need to approve users individually
  - Delegated group/role management helps scale authorisation

Authorisation

- Are groups/roles sufficient?
- Authorisation still needs to be done by the service
  - In SAML-speak, the service is the PEP
  - There is no PDP
  - There is no policy repository. There is no policy.
- Fine grained authorisation is not possible
  - Without more/better tools
- Time limited delegation is not possible
- Delegation of authorisation is not possible
- The case for dteam (= people in IRIS who Make Things Work™)
  - Support staff with (temporary) permissions of communities

Science and Technology Facilities Council

Discussion

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council

Upstairs Downstairs

- Downstairs users = IaaS management
  - People who *manage resources* and *deploy stuff* on our clouds
- Upstairs users = SaaS/PaaS users
  - People who *use* resources running on IRIS cloud
- When should we authenticate upstairs users? And how?
  - It is possible to authenticate them through IRIS IAM though it needs to be documented

Towards Zero Trust Architecture?

- A compromised credential has access to everything…
  - Different LoAs in eduGAIN
- Any authenticated user can set up an OIDC client
  - Which is probably what we want but…
  - If we support upstairs users on IAM
- Quite a lot of security-through-obscurity in our environments

Can we improve acct mgmt.?

- Indigo IAM authentication to GridPP
  - Can generate (GSI) certificates on demand
    - Even IGTF accredited ones (in principle), though they would be IOTA
- Sign up/approval process in Indigo IAM
  - We probably need different assurance levels