INDIGO IAM Hackathon

9 & 10th February 2023

Attendees!

- Federica Agostini
- Enrico Vianello
- Roberta Miccoli
- Hannah Short
- Berk Balci
- Michel Jouvin
- Tom Dack
- Petr Vokac (Remote)

Topics Covered

- Group Management
- Key Rotation
- Admin Privileges to API
- Review and “solving” of Open Issues

Group Management

- Understanding of how Group Management can be implemented to fit notably different deployments
  - EG: WLCG with IAM per VO and IRIS with Multi-VO IAM

- Decisions made:
  - There should be a setting per group to control if managers are able to remove members from that group, with a default global value defined in config
  - CNAF will look at implementing parent group membership cascading deletes on subgroup membership deletion
  - Group managers should have managerial rights of subgroups below their group
  - Addition to subgroups should not require approval of parent group manager – delegated trust

Key Rotation – solved!

- The issue of rotating signing keys in a transparent manner, and not invalidate previous signing keys completely (thus invalidating tokens)
- With testing, it was found that IAM could show multiple signing keys, with a variable declaring which key is currently used to sign
- During this process a misconfiguration was found and we had to do an emergency key rotation for all IAM instances apart from LHCb. This went very smoothly and the process has now been tested in production.
- Currently undocumented, but will be detailed later in the INDIGO IAM documentation

Admin access to API

- Issue was that without any specific scope, an IAM admin could perform any desired action within the IAM with a regular token
- The proposal is to restrict the user roles which can access the endpoints
  - If a token is provided, only the token will be evaluated based on its scopes – the user’s roles are ignored
  - If no token is provided, the access is via the dashboard, and the roles are evaluated as usual

Open Issues

- Local account access – the ability to hide the username/password from the login form *without* breaking a redirect flow
- Password complexity – currently only a minimal length-check is made for password complexity, this will be updated
- User Suspension oddities: A suspended user can refresh tokens, if they can log into IAM (ie via X.509), though cannot get VOMS proxy extension
- Bug in Suspension Synchronisation – mismatch between CERN HR DB and Indigo IAM
- Refresh Token Lifetime Default – currently infinite, should default to WLCG recommended minimum (1 day), without changing existing clients

New in IAM 1.8.1…

- Full release notes: https://github.com/indigo-iam/iam/releases/tag/v1.8.1
- Add scope management to IAM dashboard by @enricovianello in #500
- Fix /devicecode endpoint in cors endpoint matchers by @rmiccoli in #535
- Do not raise exception when incorrect scope policy by @rmiccoli in #526
- Fix bug when updating user fields by @rmiccoli in #512
- Do not allow IAM to issue RT to users with expired AUP by @rmiccoli in #503
- Remove orphans from database due to issue #481 by @enricovianello in #547
- Prevent VOMS aa from issuing ACs when AUP has expired by @enricovianello in #552
- Support for AARC-G069 guideline by @enricovianello in #553
- Add the groups view for the group managers by @rmiccoli in #536

- The CNAF team is aiming to target more frequent, smaller releases rather than infrequent larger ones.
  - This serves to benefit both developers and admins!

Next Steps

- IAM 1.8.1 deployed for the WLCG test instances, with experiments to follow
- Plans for a second hackathon later this year (~July), focussing on High Availability and Incident Response