INDIGO IAM
Community Meeting

February 23rd, 2024

INFN
CNAF
Istituto Nazionale di Fisica Nucleare

(Almost) Post Data Challenge summary

- (cit. WLCG Authz meeting)
  - *From the token perspective, a good success*
  - *~hundreds of thousands of files moved using only tokens across Atlas, CMS, and LHCb*
- IAM services stayed always up and available
  - although we observed some slowness (expected)
- Fixes during DC:
  - Configuration tuning: increased db connections
  - Added index on `refresh_token.token_value`
- Performance bottlenecks identified:
  - On deleting access tokens (mitigated with the increased db connection pool size)
  - On refreshing tokens with thousands of refresh tokens without the mentioned index
  - On dashboard accessing tokens page

Looking forward (1)

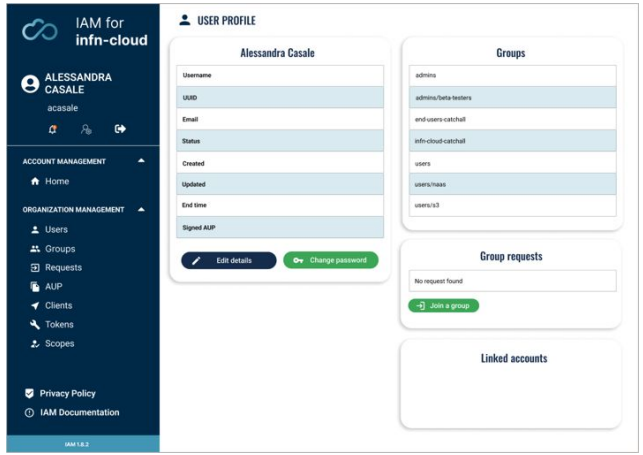
- We could avoid storing access tokens in the database
  - logging who got that token with details on token content is enough to have no security issues (discussed with our security expert)
  - how to mitigate the potential slowness on accessing introspection and APIs endpoints?
    i. caching the decrypted token received
    ii. how much is this use case relevant w.r.t. the benefits of not storing access tokens?
  - the idea is to introduce this behavior during the migration to Spring Authorization Server as base library in place of MitreID

Looking forward (2)

- Even if it wasn't an evidence during the DC, great amounts of scope policies means a significant decrease in performance
  - We're testing a migration to an external OPA (Open Policy Agent) engine in order to filter the requested scopes using the same policies defined on IAM
    i. first results are very encouraging (10k policies currently means getting a 30s timeout error using oidc-agent, few hundreds of millisecs to get the filtered scopes using OPA engine)
    ii. first step is to provide a "rego" file that applies the same policies already defined in INDIGO IAM

Looking forward (3)

- Dashboard issues or MitreID user interface problems
  - We won’t invest particular time if not really necessary
  - A new dashboard is in development
    i. decoupled from IAM (login-service) logic



INDIGO IAM v1.8.4 status and beyond

https://github.com/orgs/indigo-iam/projects/6

- The idea is to include what's in progress here and release it soon as 1.8.4 (as RC, later promoted to official)

Other main ongoing developments:

- OPA integration
- Spring Authorization Server evaluation
- IAM new dashboard development
    - unrelated to the "login-service" release roadmap
- MFA integration

Other activities to be started soon:

- geographically distributed VOMS-AA
- support for PostgreSQL?
- disabling clients

Of course, maintenance of current code base mainly focused on garbage collection optimization

INFN CNAF
Istituto Nazionale di Fisica Nucleare

Next IAM Hackathon

- Where?
  - Probably Bologna
- When?
  - May 29-30

CERN - 2023 February 9-10

Abingdon - 2023 July 25-26

CNAF

Istituto Nazionale di Fisica Nucleare

Next meeting

Friday 8th March

https://agenda.infn.it/event/40050/

INFN CNAF
Istituto Nazionale di Fisica Nucleare