From VOMS to INDIGO-IAM

Francesco Giacomini – INFN-CNAF

Credit goes to the many people contributing to development, deployment and support

HEPiX Spring 2024 – Paris

Abstract

The end of life of CentOS 7 accelerates the transition from VOMS proxies to OAuth tokens as the means to convey authorization information on a Grid/Cloud infrastructure. As a consequence, the VOMS and VOMS-Admin services will be abandoned in favor of INDIGO-IAM (or equivalent products) for the management of VO membership and the issuance of proxies and tokens.

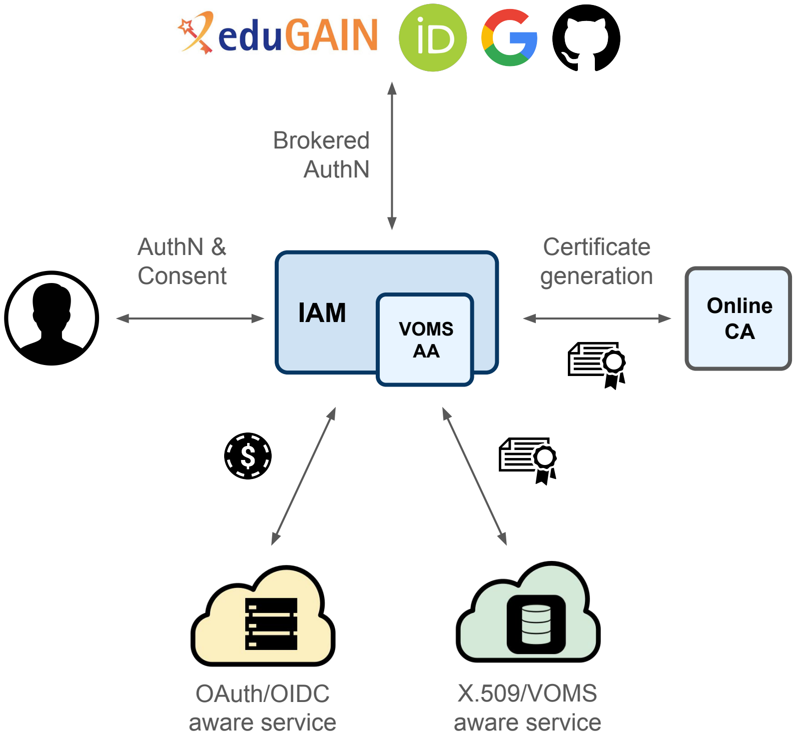
In this contribution we present the current state of affairs for the transition from VOMS to IAM, in terms of development, deployment and usage, with a peek into the future.

Outline

1. Brief intro to INDIGO-IAM
2. Existing IAM deployments
3. Performance, high-availability, scalability
4. How is the transition going?
5. Challenges
6. Development roadmap
7. Need help?

INDIGO-IAM in one slide

- Standard OAuth2 Authorization Service and OpenID Connect Provider
  - Easy integration with (web) applications
- Java application based on the Spring Boot framework
- Multiple authentication mechanisms
  - SAML, OpenID Connect, X.509, username/password
- Account linking
- Moderated and automatic user enrollment
- Enforcement of AUP acceptance
- VO membership management
- Issuance of JWT tokens and VOMS attribute certificates with identity and membership information, attributes and capabilities
- Typically deployed as a Docker container



(Some) Existing IAM deployments

- Several IAMs to control access to PaaS and SaaS services offered by INFN Cloud, to the OpenStack-based CNAF Cloud and, for small experiments, to some INFN Tier-1 services
  - On K8s or docker-compose
- One IAM for each LHC experiment
  - In OpenShift/K8s
  - Used as issuer of tokens **and** VOMS proxies, thanks to VOMS-AA
  - VO management still mostly done via VOMS-Admin, with synchronization done by a cron job
  - They all survived DC24
- Several IAMs hosted at CNAF for other collaborations: ILDG, Belle-II, HERD, JUNO, …
  - VOMS-AA is an added value

(Some) Existing IAM deployments (cont.)

- From T. Dack (STFC): *Since 2018, STFC has been operating a production instance of IAM as a multi-VO identity proxy, authorisation platform and IdP of last resort, to provide access to a broad range of services of IRIS, the coordinating body for STFC science activities*
- From M. Jouvin (IN2P3): *we are currently running three production instances. In every case, it was to provide a unified and pervasive, token-based, authN/Z service to new projects/communities where there was no pre-existing PKI-based (e.g. VOMS) federated AAI. The 3 projects are MesoNET, EURO-LABS, GRANDMA*
- Under evaluation, at different stages, in CTA, SKA, ET, …

Performance, high-availability, scalability

- Currently IAM is conceptually a centralized service and a single point of failure
- Load tests have shown that a single IAM instance can issue tokens up to a few hundred Hz, with a latency of about 1 s
  - Not enough for some scenarios
- IAM can be deployed in HA mode, with multiple instances sharing the same underlying DB and sharing session information via Redis
  - It works, but scalability is far from linear
- We have a recipe to deploy VOMS-AA in a geographically distributed way
- Main bottleneck is DB usage by IAM
  - Important improvements in the recent past (mainly adding indices), more to come

How is the transition going?

- The initial timeline for the migration to tokens foresaw “All VOs shut off VOMS-Admin” for the summer 2022
- The current timeline foresees “VOMS-Admin is switched off for one or more experiments” for March 2023, i.e. one year ago

“No plan survives first contact with the enemy”
“Plans are of little importance, but planning is essential”

- People come and go
- People need to understand how things work, implement the necessary changes in the middleware and train users
  - Flows with tokens are different than with proxies
- There are always too many things to do, wait for external triggers
- But overall the transition is going well: we keep moving data around and processing them just fine

Challenges

- As usual, too much to do, too little time to do it
    - Planning is difficult, activity is often interrupt-driven
- Specific challenges
    - Scale the system and make it more reliable and available
    - Design and implement changes that
        - address issues and requirements
        - are sufficiently generic
        - are backward and forward compatible
    - Keep pace with third-party dependencies
    - Follow, understand and address the relevant specifications
        - OAuth2, OpenID Connect, WLCG, AARC, …
    - (Contribute to) Devise the right flows for our Grid/Cloud, with a focus on usability for end users
    - Spread the knowledge
- Any help is more than welcome
    - IAM is a product for the community

Development roadmap

- In the short term the focus is almost exclusively on the transition from VOMS (Server and Admin) to IAM
  - Per the current timeline the switch over for LHC experiments should be completed by the beginning of June, in time for the EoL of CentOS 7
- We have a GitHub project with the necessary tasks. The main ones are:
  - Fewer tokens in the DB and more in the audit log
  - Support for robot certificates/users
  - Some dashboard changes to reproduce functionality available in VOMS-Admin
  - A green VOMS testsuite (at least for the combination EL9 clients – VOMS-AA)
  - Some improvements in the performance/scalability/availability area
- We expect a surge of support requests after the transition

Development roadmap (cont.)

Next:

- Integration of Multi-Factor Authentication
  - With contribution from STFC
- New dashboard, replacing Angular.js with React.js
  - PoC available
- Replace MitreID with Spring Security
  - PoC available
- Support for OpenID Federation
- Adoption of AARC (*Authentication and Authorisation for Research Collaborations*) guidelines, at the base of the Blueprint Architecture for the EOSC
- New policy engine, probably based on Open Policy Agent
  - PoC available

Need help?

- iam-support@lists.infn.it
- Channel WLCG IAM users under the “IT-dep” team in the CERN Mattermost
- Issues in https://github.com/indigo-iam/iam

- Approximately once a year we organize a hackathon
  - Next one in Bologna at the end of May https://indico.cern.ch/event/1401472/