INDIGO IAM & VOMS updates

Andrea Ceccanti
INFN CNAF

EGI Conference
November 2nd, 2020
Agenda

INDIGO IAM updates & planned activities

VOMS updates & planned activities
INDIGO IAM
INDIGO Identity and Access Management Service

A VO-scoped authentication and authorization service that

- supports multiple authentication mechanisms
- provides users with a persistent, VO-scoped identifier
- exposes identity information, attributes and capabilities to services via JWT tokens and standard OAuth & OpenID Connect protocols
- can integrate existing VOMS-aware services
- supports Web and non-Web access, delegation and token renewal
INDIGO Identity and Access Management Service

Selected by the WLCG MB to be the core of the future, token-based WLCG AAI

Sustained by INFN for the foreseeable future, with current support from:

- EOSC-hub
- ESCAPE
- IGTF
- ID
- eduGAIN
- Google
- CERN

Brokered authN

AuthN & Consent

Certificate generation

Online CA

OAuth/OIDC aware service

X.509/VOMS aware service
IAM as a service offering

INFIN provides IAM as a service to partner research communities. In this scenario, a dedicated IAM instance is deployed on the INFIN infrastructure and configured according to the community needs.

INFIN takes care of keeping the service operational and up-to-date, while administrative control on the IAM instance is granted to the community.

To request the deployment of an IAM service instance for your community, write to our support list.
IAM deployment model

An IAM instance is deployed for a community of users sharing resources, the good old Virtual Organization (VO) concept.

Client applications and services are integrated with this instance via standard OAuth/OpenID Connect mechanisms.

The IAM Web appearance can be customized to include a community logo, AUP and privacy policy document.
IAM deployment model

An IAM instance is deployed for a community of users sharing resources, the good old Virtual Organization (VO) concept.

Client applications and services are integrated with this instance via standard OAuth/OpenID Connect mechanisms.

The IAM Web appearance can be customized to include a community logo, AUP and privacy policy document.
IAM deployment model

An IAM instance is deployed for a **community** of users sharing resources, the good old **Virtual Organization (VO)** concept.

Client applications and services are integrated with this instance via **standard OAuth/OpenID Connect** mechanisms.

The IAM Web appearance can be **customized** to include a **community logo**, **AUP** and **privacy policy** document.
IAM v. 1.6.0 (latest release)

This release introduces new core functionality in IAM:

• Multiple token profiles
• Basic account lifecycle management
• Improved registration configurability
• Local authentication can be disabled to rely completely on external identity providers

For the full list of changes, see the release notes:

https://github.com/indigo-iam/iam/releases/tag/v1.6.0
IAM v. 1.7.0 (in development)

Update Spring framework dependencies to a recent version (2.2.x)

- Port to Java 11
- Requires some refactoring of the code

And other bug fixes and enhancements. For more details see the Github Milestone

ETA: December 2020
IAM NG: moving to Keycloak

Good progress in the first half of 2020 thanks to collaboration with STFC

- [https://github.com/indigo-iam/iam-ng](https://github.com/indigo-iam/iam-ng)
- Initial incarnation of IAM APIs for registration and requests management and dashboard in place

Efforts currently focused on extending Keycloak to better support Identity federations

- SAML and OpenID Connect federation
- Joint collaboration with GRNet
IAM users workshop

https://indico.cern.ch/event/970568

Kindly organised by Tom Dack from STFC

January 27th - 28th 2021 with provisional times of 14:00 - 17:00 (UTC) each day (depending on number of talks, and scheduling)

The aim of this workshop is to facilitate user led discussion around best practice, administration and deployment experience between the different communities who utilise the INDIGO IAM Authentication and Authorization service.
VOMS
The VOMS 10-20 release


Provides updates for all VOMS components

- VOMS Admin server 3.8.0, VOMS Admin client 2.0.20
- VOMS 2.0.15
- VOMS Clients 3.3.2, VOMS API Java 3.3.2

VOMS GDPR-compliance changes

CERN HR db integration refactoring

CENTOS 7/SystemD porting

Bug fixes and enhancements
VOMS Admin 3.8.0: GDPR compliance

GDPR-compliance changes: GGUS ticket

Remove all data for users who have been in status EXPIRED for more than a configurable period (default: 1 month)

- Users that failed to sign the AUP are not removed

Restrict what can be seen by any authenticated user: only the list of certificate subject DNs for a given VOMS group or role shall be exposed to any authenticated user, because that functionality is needed for constructing grid-mapfiles.
VOMS Admin 3.8.0: HR db integration refactoring

VOMS Admin used to integrate directly with the Oracle HR DB for experiment membership checks.

The HR integration has been refactored to call out to the HR DB API, a thin REST layer in front of the new HR DB VOMS views.

The same API is used by IAM WLCG deployments.
VOMS Admin 3.8.0: CENTOS 7/SystemD porting

VOMS Admin daemon lifecycle now managed with SystemD

Dedicated utility to enable/disable active VOs:

- `voms-vo-ctl deploy atlas`
- this was previously done by the init-script, difficult to port to SystemD
VOMS Admin 3.8.0: MySQL connector update

MySQL connector updated to version 8.0.16

Requires timezone set in the database or in the database URL or the connection to the database will fail and the service will not start

voms-configure utility updated to allow setting the timezone URL at VO configuration time
VOMS Admin client 2.0.20: CENTOS 7 porting

No significant code changes

Requires python-zsi package, no longer in EPEL

Package provided in our VOMS-external repo
VOMS 2.0.15: CENTOS 7/SystemD porting

Move to SystemD instantiated services

```
systemctl start|stop|status voms@atlas
```

To run commands on all configured VOs:

```
systemctl start|stop|status voms@'*'
```
VOMS 2.0.15: OSG patches merged upstream

Patches by B. Bockelman and M. Selmeci merged upstream:

- Github commit

Validate top-level VOMS group

Make RFC proxies by default for legacy VOMS clients

Disable TLS1.1 and older

Disable Weak ciphers
Bug fixes and improvements:

- [https://issues.infn.it/jira/browse/VOMS-876](https://issues.infn.it/jira/browse/VOMS-876): VOMS Java APIs authorityKeyIdentifier AC extension validation is not aligned with C/C++ VOMS APIs (more on this later)
- [https://issues.infn.it/jira/browse/VOMS-878](https://issues.infn.it/jira/browse/VOMS-878): Update to CANL 2.2.6
- [https://issues.infn.it/jira/browse/VOMS-877](https://issues.infn.it/jira/browse/VOMS-877): Make fallback to VOMS legacy protocol optional
A word about legacy VOMS clients support

The supported VOMS clients are the Java ones, but **we have no plans to break interoperability with the legacy clients**

- No active development is foreseen but contributions/patches from the community are welcome

In support of this statement

- legacy clients interoperability testing is being included in our CI testing pipeline
- the IAM VOMS implementation has been modified to support VOMS legacy clients
Thanks for your attention.
Questions?
References

IAM @ GitHub: https://github.com/indigo-iam/iam

IAM documentation: https://indigo-iam.github.io/docs

IAM in action video: https://www.youtube.com/watch?v=1rZlvJADOnY

VOMS website: http://italiangrid.github.io/voms/

Contacts:

• andrea.ceccanti@cnaf.infn.it
• indigo-iam.slack.com