The IAM VOMS importer script

Andrea Ceccanti
WLCG AuthZ WG

18/02/2021

The VOMS importer script

Migrate VO structure and users from an existing VOMS VO server

- Groups
- Roles
- Users
  - Personal information (name, surname, email)
  - X.509 certificates
  - Group and role membership
  - Generic attributes

Requires

- VOMS Admin v. 3.8.0, IAM v. 3.7.0
- VOMS proxy with admin privileges on the VOMS VO
- access token with admin privileges on the IAM VO

VOMS Groups and roles migration

Groups imported in IAM

- /atlas/production -> atlas/production

Roles are imported as IAM optional groups

- /atlas/Role=VO-Admin -> atlas/VO-Admin

Groups and roles are imported only if not already present in IAM

Users migration

IAM accounts require a username, which is a concept missing in VOMS

Solution: the username is generated concatenating the the family name and appending the VOMS user id

- This approach was favoured over the nickname as not all the VOs at CERN use the nickname and the voms importer is meant to be a generic tool (not CERN specific)

IAM requires unique email address for users

Solution: The script merges accounts sharing multiple email addresses to a single account

- The logging clearly reports when accounts are merged, so that VO Admins can take corrective actions

Linking the CERN SSO account

If the nickname in VOMS is the CERN upn, then it could be possible to link automagically the IAM imported account to the CERN SSO

A quick investigation on ATLAS seems to confirm that the nickname could be used for that purpose

- need confirmation from VO experts

CMS doesn’t use nicknames, so this is not possible

- Users can link their CERN SSO account after having logged in with their certificate

IAM changes

Extend IAM REST APIs to

- find group by exact name match
- find group by label
- find user by label/email

Increase database column size for X.509 certificate DNs

- 128 characters was NOT sufficient (VOMS uses 255)

Expose group labels in IAM dashboard group list panel

Testing

An import test was run from

- CMS
- ATLAS

to a target local IAM instance

Full import takes ~ 1 hour for ~ 3.5K users

Next steps

1. Deploying latest IAM on Openshift with changes supporting VOMS migration for ATLAS and CMS
2. Import script tuning
3. Publish script on Github repository
4. Setup periodic sync for LHC VOs on Openshift for ATLAS and CMS

Thanks for your attention.
Questions?