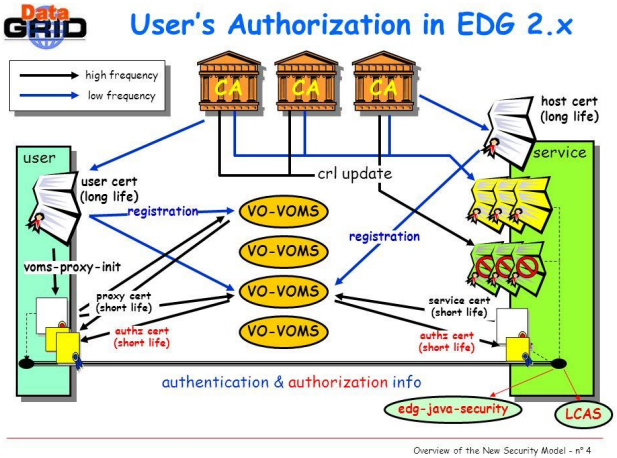
Importare utenti VOMS in INDIGO IAM tramite il voms-importer

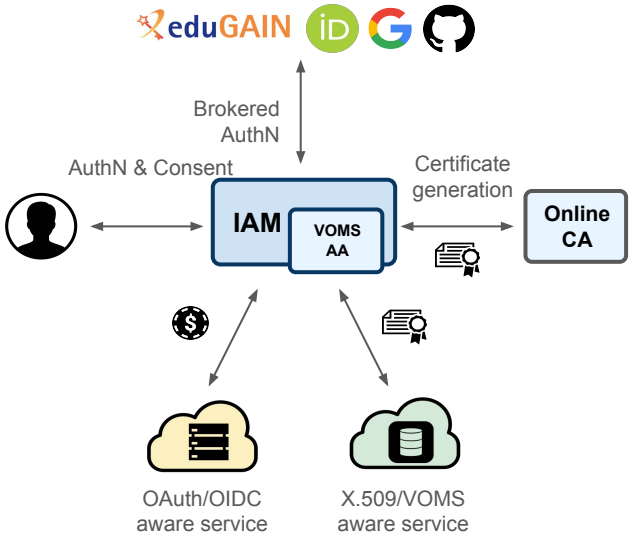
Corso di formazione “Panoramica su OAuth2/OpenID Connect e sue applicazioni tramite il servizio INDIGO IAM”, 12-14 Maggio 2025, LNF

Federica Agostini, INFN CNAF

Evolution of the WLCG AAI beyond X.509

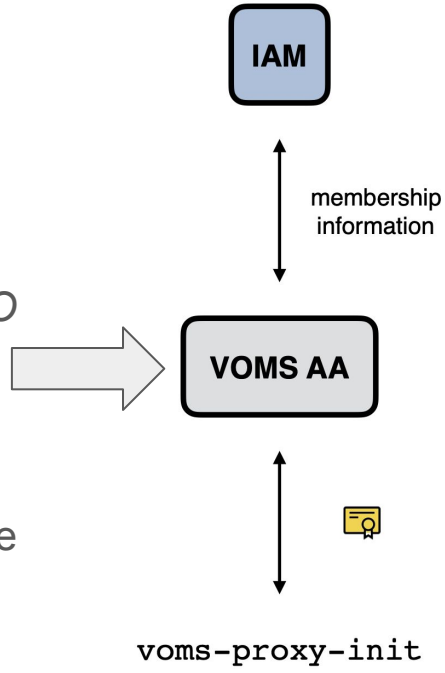


Move beyond X.509



VOMS → IAM

- Knowing that the transition from X.509 to tokens will take time, IAM was designed to be **backward-compatible** with our existing infrastructure
- IAM provides a VOMS endpoint (VOMS-AA) that **can issue VOMS credentials understood by existing clients and libraries**
- A voms-importer migration script has been developed to *import the VO structure and users* from VOMS to INDIGO IAM
  - **users will NOT have to re-register in mass** to IAM, and their IAM account will be automatically linked to their X.509 certificate
  - the script will keep IAM in sync with the VOMS instances until the VO registration process is migrated to IAM
- At some point **IAM will be the only authoritative VOMS server** for the infrastructure



The VOMS importer script

The VOMS information that are imported into IAM include

- VOMS Groups
- VOMS Roles
- VOMS Users
    - Group and role membership
    - X.509 linked certificates
    - Generic attributes
    - Other info with options

Useful details

Documentation here

Source code here

Also available as docker image as indigoiam/voms-importer (from CentOS7)

It requires (all available in the docker image)

- python 2.7
- ldap module
- voms-admin-client
- an executable `dn_converter` (source here)

VOMS groups and roles migration

The VOMS importer creates new IAM groups, if not existing, as

- `/test.vo/G1` (VOMS group) → `test.vo/G1` (IAM group)
- `/test.vo/Role=VO-Admin` (VOMS role) → `test.vo/VO-Admin` (IAM optional group)

In IAM, a VOMS *role* (also called *optional group*) is represented by the `voms.role` and `wlcg.optional-group` labels

Note the missing leading “/” in the IAM representation of groups with respect to VOMS

- still preserved in VOM FQANs

Groups and roles can be created directly in IAM without any corresponding group or role in VOMS

- they will not be removed

User migration

The importer script migrates

- group and roles membership
- user’s email address
- AUP signature time (*optional*)
    - ignored if the IAM VO has not defined any AUP
- linked X.509 certificates
- generic attributes
    - they will appear in the proxy if a VOMS AA server is in place

By default, it synchronizes only active VOMS users

- do not expect that a user suspended by a VO Admin in VOMS is suspended also in IAM

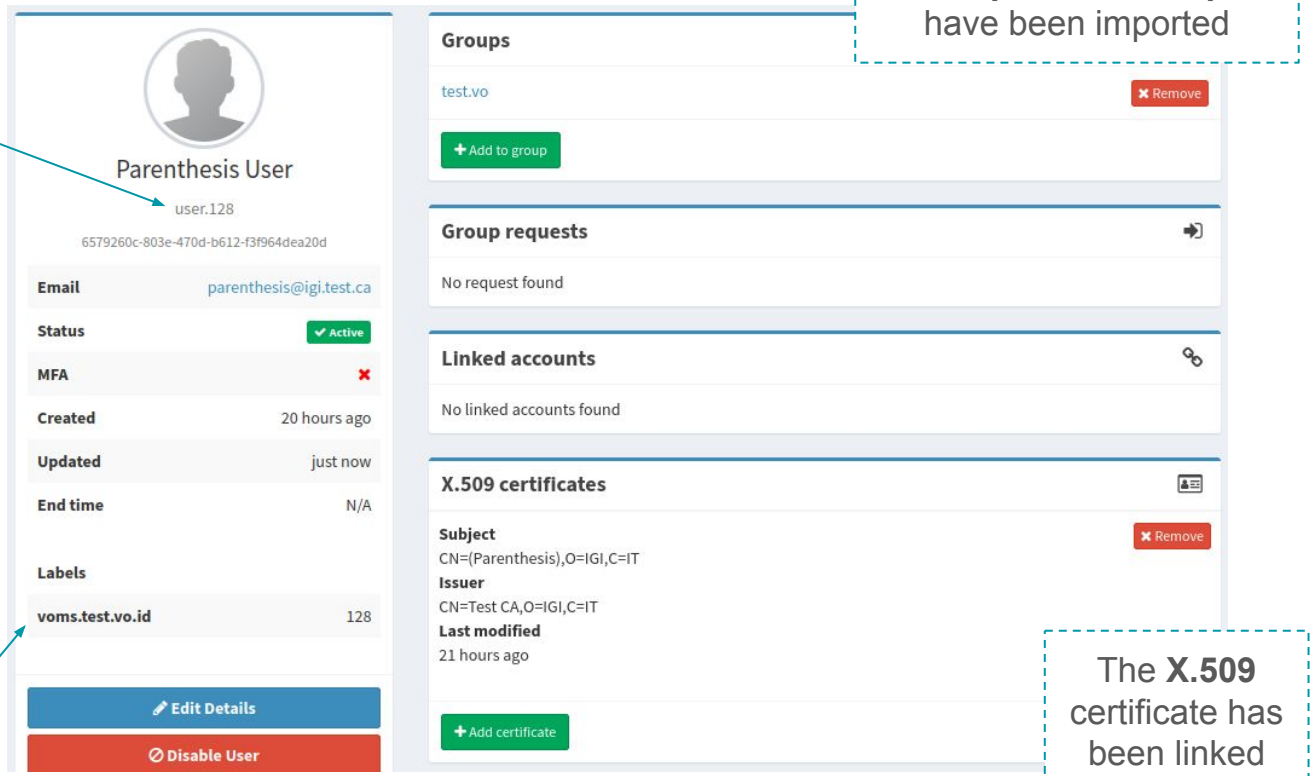
Newly created IAM accounts

The **username** is set to `user.<voms userid>` (VOMS accounts didn't have username)

The **given name**, **family name** and **email address** is the one registered in VOMS

A `voms.<vo>.id` label with the VOMS user's id is added, to track back which user has been created

Group memberships have been imported



The **X.509** certificate has been linked

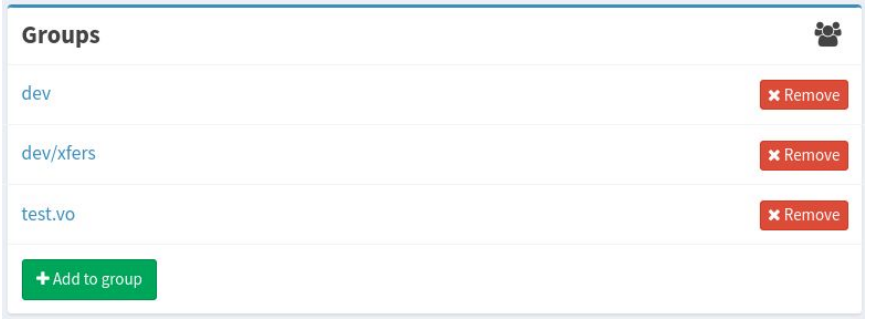
Also generic **attributes** are imported

Existing IAM accounts

- **Name**, **last name**, **username**, **email** address and **nickname** are unchanged
- **group memberships** retired from VOMS are also removed from IAM, but
- memberships to *IAM groups without a VO parent group* NOT considered in the account synchronization

dev and **dev/xfers** are IAM groups not defined in VOMS

test.vo is a group imported by VOMS



- new **X.509 certificates** defined in VOMS are appended to the existing ones in IAM
- also **generic attributes** are appended to the existing ones

User’s email address

IAM requires an *unique* e-mail address for users, while VOMS allowed different users to share the same address

By default, the importer prints the duplicate e-mail addresses, but import only the first user in the run

What to do with duplicate email addresses?

- manually remove the not needed VOMS accounts with a duplicated e-mail address
- use dedicated service account email address for service accounts
- set a new email address for a specific account
    - `--email-mapfile </path/to/file>` option allows to source from a file with *vomsid;email@address* content, to enable a duplicate email overwrite mechanism

For newly created IAM accounts !

```
2025-05-07 19:24:50,419 INFO : Importing VOMS user: 128 - Parenthesis User
2025-05-07 19:24:50,419 INFO : Overriding email for VOMS user: 128 : apostrofe@igi.test.ca => parenthesis@igi.test.ca
2025-05-07 19:24:50,706 INFO : No IAM account found matching VOMS user id 128 found, will create a new one
```

Setup credentials

Register into **VOMS**

- ask to give you Admin privileges

Register into **IAM**

- ask to give you Admin privileges
- link the same *valid* X.509 certificate you have in VOMS
- load a long-lived plain proxy certificate (or you will have to refresh it once it is expired)
    - create a proxy with `voms-proxy-init -valid 8760:00`
    - click on IAM button *Add managed proxy certificate* and paste the contents of your grid proxy
- Register an oidc-agent Client with at least the following scopes allowed: `openid iam:admin.read iam:admin.write scim:read scim:write proxy:generate`
    - may require RHEL distros

Run the script

This example allows to import users, groups and roles from meteora (VOMS) to iam-dev (IAM)

Initialize the required credentials

```
export OIDC_AGENT_ALIAS=<alias>
export OIDC_AGENT_SECRET=<secret>
export IAM_ENDPOINT=https://iam-dev.cloud.cnaf.infn.it
init-credentials.sh
export X509_USER_PROXY=/tmp/x509up_u$(id -u)
```

Basic options to run the script

```
vomsimporter --vo test.vo --voms-host meteora.cloud.cnaf.infn.it --voms-port 8443
--iam-host iam-dev.cloud.cnaf.infn.it --skip-duplicate-accounts-checks
```

Here `--skip-duplicate-account-checks` (which does not check if an email is duplicated in VOMS) is used to bypass a known importer error in the current version

Some useful option

`--username-attr <attribute-key>` sets the username of a newly created IAM account as the VOMS attribute (if present) identified by the attribute key

`--synchronize-activation-status` imports users suspended in VOMS and sets them in IAM as *disabled*. It also synchronizes the VOMS user's activation state

`--id-file <file>` allows to import in IAM the VOMS users whose id is listed in the file (one id per line)

`--skip-users-import` does not synchronize users

`--insecure` disables a SSL certificate verification when interacting with VOMS server

VOMS importer log

```
2025-05-07 18:25:04,609 INFO : VOMS importer run id: aab2a8a1-3d9f-4fd6-892e-58e4dafe6d3f
2025-05-07 18:25:04,609 INFO : Importing VOMS groups
2025-05-07 18:25:05,181 INFO : Group /test.vo already present
2025-05-07 18:25:06,230 INFO : Group /test.vo/G1 already present
2025-05-07 18:25:07,276 INFO : Group /test.vo/G1/G4 already present
2025-05-07 18:25:08,110 INFO : Group /test.vo/G1/G4/G5 already present
2025-05-07 18:25:09,031 INFO : Group /test.vo/G1/R1 already present
2025-05-07 18:25:09,990 INFO : Group /test.vo/G2 already present
2025-05-07 18:25:11,049 INFO : Group /test.vo/G2/G3 already present
2025-05-07 18:25:11,747 INFO : Importing VOMS roles
2025-05-07 18:25:12,472 INFO : Importing VOMS role: Role=Group-Manager as optional group: test.vo/Group-Manager
2025-05-07 18:25:12,638 INFO : Optional group test.vo/Group-Manager already present
2025-05-07 18:25:12,949 INFO : Importing VOMS role: Role=R1 as optional group: test.vo/R1
2025-05-07 18:25:13,094 INFO : Optional group test.vo/R1 already present
2025-05-07 18:25:13,391 INFO : Importing VOMS role: Role=R2 as optional group: test.vo/R2
2025-05-07 18:25:13,550 INFO : Optional group test.vo/R2 already present
2025-05-07 18:25:13,870 INFO : Importing VOMS role: Role=R3 as optional group: test.vo/R3
2025-05-07 18:25:14,033 INFO : Optional group test.vo/R3 already present
2025-05-07 18:25:14,350 INFO : Importing VOMS role: Role=VO-Admin as optional group: test.vo/VO-Admin
2025-05-07 18:25:14,511 INFO : Optional group test.vo/VO-Admin already present
2025-05-07 18:25:14,830 INFO : Importing VOMS users
2025-05-07 18:25:15,272 INFO : VOMS users count: 12. Starting from index 0
2025-05-07 18:25:15,469 INFO : Importing VOMS user: 147 - Federica Agostini
2025-05-07 18:25:15,950 WARNING : IAM account found matching VOMS user 147 - Federica Agostini email: federica.agostini@cnaf.infn.it. Will import informati
on on that account
2025-05-07 18:25:16,109 ERROR : Failed AUP synchronization for account d331b9e3-c5bd-4e1c-a519-c9b93a093d0b with error: {"error":"AUP is not defined for th
is organization"}
2025-05-07 18:25:16,110 INFO : Syncing group/role membership for user fagostin (d331b9e3-c5bd-4e1c-a519-c9b93a093d0b)
2025-05-07 18:25:16,110 INFO : Importing fagostin (d331b9e3-c5bd-4e1c-a519-c9b93a093d0b) membership in VOMS FQAN: /test.vo
2025-05-07 18:25:16,270 INFO : Importing fagostin (d331b9e3-c5bd-4e1c-a519-c9b93a093d0b) membership in VOMS FQAN: /test.vo/Role=VO-Admin
2025-05-07 18:25:16,420 INFO : Syncing generic attributes for user fagostin (d331b9e3-c5bd-4e1c-a519-c9b93a093d0b)
2025-05-07 18:25:16,420 INFO : Importing certificate {u'suspended': False, u'creationTime': u'2024-03-29T12:30:04', u'subjectString': u'/DC=org/DC=terena/D
C=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Federica Agostini fagostin@infn.it', u'issuerString': u'/C=NL/O=GEANT Vereniging/CN=GEANT TCS Authent
ication RSA CA 4B'} for user fagostin (d331b9e3-c5bd-4e1c-a519-c9b93a093d0b)
2025-05-07 18:25:16,440 INFO : Converted certificate info: 'CN=Federica Agostini fagostin@infn.it,O=Istituto Nazionale di Fisica Nucleare,C=IT,DC=tcs,DC=te
rena,DC=org', 'CN=GEANT TCS Authentication RSA CA 4B,O=GEANT Vereniging,C=NL'
```

Demo

- Create a new user in VOMS (https://meteora.cloud.cnaf.infn.it:8443/)
- Set a *nickname* attribute equal to `importer_demo`
- Run the importer
  - assign the user a nickname equal to its attribute with `--username-attr nickname`
  - run the import just for this user with `--id-file <file>` (the file contains a VOMS user's id)
- Disable the user from VOMS and run the importer again
  - use the `synchronize-activation-status` option

More examples are available in this repo