VOMS status

IT GD Group Meeting
2003-12-05

Maria Dimou IT/GD

Why migrate out of LDAP(I)

- Unfriendly mass-updates via the ldap[add|search|delete] commands or the LDAP browser.
- CN name clashes within a given VO.
- Currently the LCG User Registration procedure allows a user to become a member of only one VO at a time.

Why migrate out of LDAP(II)

- Added functionality in *voms-proxy-init* as opposed to *grid-proxy-init*, i.e. credentials from the guidelines & from VO's VOMS server checked at the resource (i.e. LCAS/LCMAPS, edg-java-security etc). Pending:
  - voms-proxy-info command under development.
  - Proxy renewal in case of long jobs needs to be tested.
- Additional VOMS' attributes:
  - The user's working **Group** (e.g. registration, integration, testing)
  - The user's **Roles** (within a given "Group" i.e. inheriting the Group's privileges, e.g. production manager, user).

VOMS admin pending issues (I)

- The user registration information is not yet decided. DN,CN,CA,CA URI,Email,Groups and Roles are the only fields foreseen so far. Today, (ldap) lcg-registrar contains the Institute and the PhoneNumber in addition. USA sites require more information (see 2003-11-07 meeting with the VO managers and notes from the VOX web interface demo).

VOMS admin pending issues (II)

- The procedure ensuring a user's compliance to the Guidelines before acceptance in the VO is not yet clear. The LCG security group discussed the issue on 2003-11-03 but postponed the decision to the VOMS Workshop of 2003-12-15.
- The VOMS (web) interface for users to submit requests to the VO administrators is not yet available.

Done so far

- We submitted a number of enhancement suggestions with Bugzilla after playing with the test installation.
- We are in phase 0 migration scenario, i.e. importing data from LDAP into VOMS (on tbed0152.cern.ch). Periodic synchronisation LDAP-VOMS (cron job) is active (every 6 hours).
- Proceeding to phase 1 i.e. generating the gridmap file from VOMS, is possible today but requires C&T availability to test impact on the service (after LCG-2).

Benefit(?) for the rest of LCG service

- As long as we use the gridmap file:
  - even if user registration allowed users to belong to multiple VOs, only **one** of the entries present for a given user can be considered.
  - VOMS' enhanced functionality in terms of fine-grain categorisation of users in Groups and Roles cannot be exploited.

To Do (I)

- A use case on how experiments name their directories and arrange access permissions is needed to write down the potential contents of LCMAPS (exact mapping mechanism of VOMS Roles to Unix groups).
- LCG has to give feedback to EDG/WP1 and WP4 on the proposed service developments. Namely:

To Do (II)

- A VOMS-aware *gridftp* by EDG/WP4 (D.Groep) Development and testing time: 2 weeks. VDT integration not counted.
- For the job to map the site-specific Unix group name on the WN to the VOMS Group/Role name:
  - EDG/WP4 (O.Koeroo) is currently developing the JobRepository, a database containing:
    - □ User certificate chain
    - □ Job info
    - □ Job status
    - □ VOMS info. per user, per job
    - □ Active UID, GID(s) for a Job.

To DO (III)

- EDG/WP4 shall provide a kind of *id* command that gets from the JobRepository the UNIX groupname for a given VO Group/Role.
- EDG/WP4 (D.Groep) produced a VOMS-aware CE InfoProvider from today's GlueCEAccessControlBaseRule: VO:dteam to contain complete VO/Group/Role information as Fully Qualified Attribute Names (FQAN) for publication in the GlueSchema :
  - /VO[/group[/subgroup(s)]][/Role=role][/Capability=cap]
- EDG/WP1 (M.Sgaravatto) has to change the RB.

Conclusions

- There is some remaining development in the VOMS admin. part for user registration. With our good relation with the developers these can be smoothly planned and get done.
- There are dependencies from EDG/WP1 and WP4 where help is needed from the :
  - Experiment VO managers (for FQANs).
  - Globus VDT contacts (for integration checking).
  - LCG C&T and Infrastructure experts (for gridmap-to-lcmaps migration deployment).