Current LCG User Registration, VO management and Authorisation Procedures

VOMS workshop
2003-12-15

last update 12/12/2003 16:25

What "getting on LCG" means

As explained in the User Introductory page the basic steps are:

- authentication (by means of a personal digital certificate),
- registration,
- authorisation to use LCG resources (via a limited-in-time proxy) and
- job submission

LCG Registration procedure today

Read the LCG Usage Rules. If you agree to adhere to these rules, then proceed to:

1. Obtain a valid digital certificate from your CA.
2. Load your certificate onto your browser.
3. Fill the LCG Registration Form

In this form you will:

- Choose the VO you are affiliated with.
- Confirm your adherence to the LCG Usage Rules = Guidelines.

Complete registration

Additional information on that web form:

- Family Name
- Given Name
- Institute
- Email Address
- Telephone Number

The Email Address is mandatory as it is used to check the authenticity of the request, by automatically emailing back a URL for the user to open, which launches the completion of the registering process.

What happens behind the scenes

- Successful registrations are added in an LDAP directory for the Guidelines and a separate LDAP directory for the VO.
- The Guidelines' LDAP and the DTEAM VO LDAP are physically at CERN, the experiments' VOs are on an LDAP server at NIKHEF.
- The addition of the user in the Guidelines' LDAP is automatic and ends by an email request to the relevant VO manager to include the user in the VO.

New VO member

- The VO manager checks with the Institute (security?) contacts whether the user should be accepted and whether his/her data are correct.
- (S)he uses a set of EDG scripts and/or the LDAP commands and browser to add the new member to the VO. (Procedure)
- (S)he notifies the user and all site contacts about the admission of a new member in the VO (continue?) A set of mailing lists facilitates communication between sites and VO managers.

Finally "on the Grid"

Once the user is as a valid LDAP entry in a given VO (s)he will automatically appear in the grid-map file a few hours later, e.g.:

"/C=CH/O=CERN/OU=GRID/CN=Maria Dimou 7577" .dteam

The user should be present in, both, the Guidelines' and the VO LDAP as checked by the /opt/edg/etc/ edg-mkgridmap.conf

```
# LCG Standard Virtual Organizations
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=alice,dc=eu-datagrid,dc=org .alice
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=atlas,dc=eu-datagrid,dc=org .atlas
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=cms,dc=eu-datagrid,dc=org .cms
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=lhcb,dc=eu-datagrid,dc=org .lhcb
group ldap://lcg-vo.cern.ch/ou=lcg1,o=dteam,dc=lcg,dc=org .dteam

##### AUTH: authorization URI
auth ldap://lcg-registrar.cern.ch/ou=users,o=registrar,dc=lcg,dc=org
```

Why would anyone wish to change this procedure?

- Unfriendly mass-updates via the ldap[add|search|delete] commands or the LDAP browser.
- Can't handle 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.
- There is no mechanism to tell the local resources what this user is authorised to do with(out) priviledges.

The VOMS alternative 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 in VOMS. Today, (ldap) lcg-registrar contains the Institute and the PhoneNumber in addition.
The GDB decided which are the mandatory fields for LCG user registration.

The VOMS alternative 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 discussion to this Workshop. Who/when will take the decision?
- The VOMS (web) interface for users to submit requests to the VO administrators is not yet available.

Conclusions for registration

- The present procedure doesn't scale and doesn't cover the needs of service from the Authorisation point of view, i.e. we need the VOMS Groups/Roles' values.
- The issue of separate (or not) Guidelines/VO database(s) must be decided (in this workshop?)
- The minimum mandatory amount of information as decided by the GDB must be available on all user registration tools (VOMS, VOX, …).

Hint for the authorisation slot

VOMS' enhanced functionality in terms of fine-grain categorisation of users in Groups and Roles cannot be exploited as long as we keep the grid-map file, where we have no indication to which Unix group(s) the user's job must belong.

It would be a pity to only use VOMS for its better administration interface because of unclear mechanisms to extract, match and exploit VOMS and LCMAPS information.