Table of Contents

VOMS and ACLs in Data Management

Author : Jean-Philippe Baud

VOMS mapping

All groups for the VO selected are present in the proxy. Only the role selected is present in the proxy. Groups can be ordered in the proxy on user request.

The first group selected by voms-proxy-init (group ordering or explicit role) is called the primary group. If no group ordering nor explicit role is selected, the primary group will be the voname.

There are 2 methods used for VOMS mapping:

- **LCMAPS :**

LCMAPS provides site dependant mapping between DNs and/or roles and local Unix uid/gid. Currently at CERN:

- "gridmapfile" maps a VOMS group or role to a local or pool user account,
- "groupmapfile" maps a VOMS group or role to a local group.

LCMAPS does a setuid/setgid (primary group) and a setgroups to set the secondary groups.

This is used by the Workload Management System. The job runs under this primary group but also uses the secondary groups to access files local to the Worker Node. The accounting is done on primary group.

- **Virtual Ids :**

They are site independant and do not require any administrator action. A DN is mapped to a Virtual uid and a VOMS group o role is mapped to a Virtual gid.

They are used by Data Management components like LFC and DPM.

Currently only the Virtual Uid and the primary Virtual Gid are used to control access to the File Catalogue entries or the files in the Storage Elements.

File ownership in LCG Data Management tools

Unless changed with chown the files are owned by the DN of the user who created the file.

The group ownership of a file depends on the S_ISGID of the parent directory: if it is set, the file group ownership is the same as the parent one, if not the primary group of the user is used.

Posix ACLs

Base ACLs map directly to standard Unix permissions: owner, group owner, others.

Extended ACLs correspond to lists of supplementary users/groups. Please note that if there is a list of supplementary users/groups, an acl mask must also be defined.

There are 2 types of extended ACLs: access and default.

- access ACLs can be set on both directories and files and are used to control access.
- default ACLs can be set on directories. These ACLs are inherited as access ACLs by every file or sub-directory underneath unless explicitely changed. The default ACLs are also inherited as default ACLs by every sub-directory.

LFC and SE with SRM v2 interface and also HPSS support Posix ACLs

---

File deletion

Permission to delete a file depend on S_ISVTX bit in parent directory:

- one always needs to have write permission on the parent directory,
- if the `S_ISVTX` bit in parent mode is set, one needs to be the owner of the file or to have write permission on the file itself.

User files

We suggest to set:

- the `S_ISVTX` bit on parent directory
- the mode of the file to `0644`, or `0600` if the file must only be seen by the owner (DN) itself

---

Production files

We suggest to set:

- the `S_ISVTX` bit on parent directory
- the mode of the file to `0664`

Support of secondary groups in LCG Data Management tools

Note : this is not available yet...

Why is it useful? Let's take an example: "collective" files are owned by group "lhcb".

- case 1 : secondary groups are not supported

If these files are not world readable, an LHCb user coming with a role "production" cannot read those files unless you have an access ACL giving "lhcb/Role=production" as supplementary group.

- case 2 : secondary groups are supported

Then, any LHCb user will get "lhcb" as one of his/her groups and you do not need to set the ACL.

Experiment admin and file/directory permissions

Note : this is not availaible yet...

Let's assume that a role "vodataadmin" is defined in VOMS.

There are 2 solutions:

- An ACL entry is added to every file/directory to give the role "vodataadmin" all permissions on them.
- "vodataadmin" is recognized by all LCG Data Management services as being a special role to get all permissions on files/directories owned by the VO without having to set the ACL entry.

Accounting and quotas in LCG Data Management tools

- A file will be accounted to the owner DN and to the group owner but please see the remark about `S_ISGID` above.
- soft quotas will be implemented for users and primary groups.

-- SophieLemaitre - 12 Apr 2006

This topic: LCG > VomsAndAcls
Topic revision: r1 - 2006-04-12 - unknown