Table of Contents

Virtual Ids / VOMS

The LFC and the DPM support virtual Ids and VOMS : each user/group is internally mapped to a "virtual Id".

This allows Access Control Lists (ACLs) to be fully supported.

Note : thus, your rights may then differ, depending of your credentials at a given time !

Comment

The virtual ids and VOMS are supported in LFC version >= 1.4.0 and DPM version >= 1.5.4.

The virtual ids are not backwards compatible, in the sense that an LFC client prior to 1.4.0 (or DPM client prior to 1.5.4) doesn't recognize the virtual ids. It will still print the unix id of the user/group that exists on the client machine.

Virtual Ids

Each user and each group is internally mapped to a "virtual Id".

The mappings are stored in :

- the `Cns_userinfo` table, for the users
- the `Cns_groupinfo` table, for the groups

For instance :

```
mysql> use cns_db;

mysql> select * from Cns_groupinfo;
+-------+-----+-----------+
| rowid | gid | groupname |
+-------+-----+-----------+
|   1   | 101 | dteam     |
|   2   | 102 | atlas     |
|   3   | 103 | cms       |
|   4   | 104 | babar     |
|   5   | 105 | infngrid  |
+-------+-----+-----------+

mysql> select * from Cns_userinfo;
+-------+--------+-------------------------------------------------------------+
| rowid | userid | username                                                    |
+-------+--------+-------------------------------------------------------------+
|     1 |    101 | /C=CH/O=CERN/OU=GRID/CN=Sophie Lemaitre 2268          |
|     2 |    102 | /C=CH/O=CERN/OU=GRID/CN=Sophie Lemaitre 2268 - geant4 |
|     3 |    103 | /C=CH/O=CERN/OU=GRID/CN=Jean-Philippe Baud 7183       |
+-------+--------+-------------------------------------------------------------+
```

The user and group ids are completely **independant** from the UNIX uids/gids.

Each user is represented by his DN and each DN is mapped to a different internal uid. Each group is represented by a string, and each of these strings is mapped to a different internal gid.

For performance reasons, when using `lfc-ls -l`, only the internal user id and group id appear :

```
$ lfc-ls -ld /grid/dteam/tests
drwxrwxr-x   0 18947    2688   0 Feb 15 18:40 /grid/dteam/tests
```

You can see the actual DN / group name by using `lfc-getacl` :

```
$ lfc-getacl /grid/dteam/tests
# file: /grid/dteam/tests
# owner: /C=CH/O=CERN/OU=GRID/CN=Sophie Lemaitre 2268
# group: dteam
user::rwx
group::rwx              #effective:rwx
other::r-x
default:user::rwx
default:group::rwx
default:other::r-x
```

The arguments for the `lfc-chown` and `lfc-setacl` commands can be either the internal uid/gid, or the actual DN/group name :

```
lfc-chown "/C=CH/O=CERN/OU=GRID/CN=Sophie Lemaitre 2268":dteam /grid/dteam/tests/hosts1

lfc-chown 18947:2688 /grid/dteam/tests/hosts
```

If you use different certificates, you will be mapped to a different DN, and thus a different uid (and maybe gid).

On different LFC servers, you will be mapped to a different virtual id.

The group you are mapped to is :

- either your VOMS group (when using "voms-proxy-init -voms")
- or the group in lcgdm-mapfile (when using a simple "grid-proxy-init")

VOMS

Depending on your VOMS credentials/role, you will be mapped to different virtual gids.

This is why a user might not be able to write in a directory he/she created before with another VOMS role.

To handle that situation, you should use ACLs (see `man lfc-setacl` or `man dpns-setacl`) to grant privileges to the different gids corresponding to the different VOMS roles.

See the slides attached below.

---

lcgdm-mapfile

The `/opt/lcg/etc/lcgdm-mapfile` file is needed.

It contains DNs to group name mappings :

```
"/C=CH/O=CERN/OU=GRID/CN=Jean-Philippe Baud 7183" dteam
"/C=CH/O=CERN/OU=GRID/CN=Sophie Lemaitre 2268" dteam
"/C=CH/O=CERN/OU=GRID/CN=Sophie Lemaitre 2268 - geant4" geant
```

This file is used when the user issues a `grid-proxy-init` or `voms-proxy-init` without VOMS parameters.

Then, `/opt/lcg/etc/lcgdm-mapfile` allows the software to know to which group the user should be mapped.

It is not used when the user possesses VOMS credentials.

`/opt/lcg/etc/lcgdm-mapfile` is populated thanks to the `/opt/lcg/etc/lcgdm-mkgridmap.conf` configuration file, which contains the VO names to which entries should be mapped.

For instance :

```
more /opt/lcg/etc/lcgdm-mkgridmap.conf

#############################################################################
#
# lcgdm-mkgridmap.conf generated by YAIM on Thu Mar 16 10:22:10 CET 2006
#
#############################################################################

group vomss://lcg-voms.cern.ch:8443/voms/atlas?/atlas/Role=lcgadmin atlas
group vomss://voms.cern.ch:8443/voms/atlas?/atlas/Role=lcgadmin atlas
group vomss://lcg-voms.cern.ch:8443/voms/atlas?/atlas/Role=production atlas
group vomss://voms.cern.ch:8443/voms/atlas?/atlas/Role=production atlas
group vomss://lcg-voms.cern.ch:8443/voms/atlas?/atlas/lcg1 atlas
group vomss://voms.cern.ch:8443/voms/atlas?/atlas/lcg1 atlas
group ldap://grid-vo.nikhef.nl/ou=lcgadmin,o=atlas,dc=eu-datagrid,dc=org atlas
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=atlas,dc=eu-datagrid,dc=org atlas
group vomss://lcg-voms.cern.ch:8443/voms/dteam?/dteam/Role=lcgadmin dteam
group vomss://voms.cern.ch:8443/voms/dteam?/dteam/Role=lcgadmin dteam
group vomss://lcg-voms.cern.ch:8443/voms/dteam?/dteam/Role=production dteam
group vomss://voms.cern.ch:8443/voms/dteam?/dteam/Role=production dteam
group vomss://lcg-voms.cern.ch:8443/voms/dteam?/dteam dteam
group vomss://voms.cern.ch:8443/voms/dteam?/dteam dteam
group ldap://lcg-vo.cern.ch/ou=lcgadmin,o=dteam,dc=lcg,dc=org dteam
group ldap://lcg-vo.cern.ch/ou=lcg1,o=dteam,dc=lcg,dc=org dteam
auth ldap://lcg-registrar.cern.ch/ou=users,o=registrar,dc=lcg,dc=org
gmf_local /opt/lcg/etc/lcgdm-mapfile-local
```

Note : In this file, only VO names should appear, and no "pool accounts" (like `.dteam` or `dteamsgm`)...

Troubleshooting

IMPORTANT

When using `grid-proxy-init` or a simple `voms-proxy-init`, a user **belonging to several VOs with the same DN** will sometimes be mapped to one VO, and sometimes to another VO (depending in which order the mappings appear in the `lcgdm-mapfile`).

To prevent this, use VOMS credentials.

-- SophieLemaitre - 07 Nov 2007

This topic: LCG > VirtualIds
Topic revision: r10 - 2009-09-21 - MariaDimou

or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback