VOMS and ACLs in Light weight Disk Pool Manager

Jean-Philippe Baud, IT-GD, CERN

June 2007

Security

- All control and I/O services have security built-in: GSI or Kerberos 5
- The entries in the name space can be protected by Posix Access Control Lists
- All privileged operations can only be done with a Host Certificate on a trusted host
- VOMS integration: groups, sub-groups and roles are supported

VOMS integration

- DNs are mapped to virtual UIDs: the virtual uid is created on the fly the first time the system receives a request for this DN (no pool account)
- VOMS roles are mapped to virtual GIDs
- A given user may have one DN and several roles, so a given user may be mapped to one UID and several GIDs
- Secondary groups are now supported (1.6.4)
  - Authorization in name space is done using primary and secondary groups
  - Disk pool selection is done using primary group

VOMS integration

- Support for normal proxies and VOMS proxies
- Integration with CSEC (socket interface) and CGSI (soap services)
- Administrative tools are provided to manually update the DB mapping table if necessary
  - To create VO groups in advance
  - To keep same uid when DN changes
  - To get same uid for a DN and a Kerberos principal

Access Control Lists

- LFC and DPM support Posix ACLs based on Virtual Ids
  - Access Control Lists on files and directories
  - Default Access Control Lists on directories: they are inherited by the sub-directories and files under the directory
- Example
  - dpns-mkdir /dpm/cern.ch/home/dteam/jpb
  - dpns-setacl -m d:u::7,d:g::7,d:o:5 /dpm/cern.ch/home/dteam/jpb
  - dpns-getacl /dpm/cern.ch/home/dteam/jpb

```
# file: /dpm/cern.ch/home/dteam/jpb
# owner: /C=CH/O=CERN/OU=GRID/CN=Jean-Philippe Baud 7183
# group: dteam
user::rwx
group::r-x              #effective:r-x
other::r-x
default:user::rwx
default:group::rwx
default:other::r-x
```