VOMS and ACLs in Storage Services: summary of the GSSD discussions

Flavia Donno, IT-GD, CERN

June 2007

Summary

- Presentations from J.-P. Baud about DPM, P.Fuhrmann on dCache, and L. Magnoni on StoRM.
- The implementation existing in DPM at the moment has been taken as a proposal for others.
- We focused on functionality offered to end-users and site administrators. We tried to ensure that the same functionality is offered by all SE implementations.
- LHCb (N. Brook) declared to be satisfied with the current functionality offered by DPM.

Security

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

VOMS integration

- For **DPM** 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). **dCache/StoRM** use a pair UID/GID. If CASTOR creates Unix UID/GIDs ahead of time, it can use the same logic as DPM and solve the problem with LSF that has to operate with UNIX UIDs.
- VOMS roles are mapped to virtual GIDs (DPM) or to a set of UID/GID pairs (dCache/StoRM)
- **DPM** A given user may have one DN and several roles, so a given user may be mapped to one UID and several GIDs or **dCache/StoRM** several UID/GID pairs.
- **DPM** 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

- **DPM** ACLs can also be establishes on pools (sets of filesystems). Such ACLs are used only when:
  - the default space is used,
  - during the pool selection process when dynamic reservation takes.
- It was asked to:
  - In case of ACLs/DN mismatch, it was asked to check on secondary groups and to possibly provide a fallback pool (configurable option)
  - Allow for “negative” ACLs (to disallow usage from a specific group/subgroup/role)
- **dCache** same functionality could be provided.
- **StoRM** at the moment a filesystem is a storage area or storage component and ACLs can be enforced at the filesystem level using group id mapping. JiT vs. AoT ACLs.

VOMS integration: DPM specific

- Support for normal proxies and VOMS proxies (DPM, dCache and StoRM).
- 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: DPM specific

- 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
```