Access Lists Management in LDG MDC

D. Pleiter, D. Melkumyan

12 May 2006

For the MDC the following privileges are foreseen:

1. Administrator privilege
2. Manager privilege (bound to project)
3. Group privilege (bound to ensemble)

A higher level privilege implies all lower level privileges. Administrator privilege is the highest privilege.

1 Table `certmap`

certID	cid
varchar(255)	int

Table maps a certificate identified by a certificate subject string to an unique numerical identifier.

2 Table `prjmap`

collaboration	prjName	prjid
varchar(255)	varchar(255)	int

Table maps tuple (collaboration, project name) to an unique numerical identifier.

3 Table `grpmap`

grpName	prjid	gid
varchar(255)	int	int

Table maps the tuple group name and project identifier to an unique numerical identifier. The project identifier is needed to restrict groups to a project.

4 Table ensemblemap

ensembleURI	eid	prjid
varchar(255)	int	int

Table maps the ensemble URI to the unique numerical identifier `eid` and defines the project to which the ensemble belongs to. It is assumed that part of the `ensembleURI` depends on the project name to avoid name clashes and the possibility to obtain privileges on ensembles of another project.

The following rules apply:

1. The entries in column `ensembleURI` are unique.
2. For each `ensembleURI` there is one and only one `eid`.
3. For each `prjid` there may exist several `ensembleURI`.

This rules may be enforced in a database by defining `ensembleURI` as an unique primary key and `eid` an unique secondary key.

5 Table adm

cid
int

Owners of the certificates listed in this table have administrator privilege, i.e. read/write access to all tables.

6 Table manager

prjid	cid
int	int

This table defines the managers identified by `cid` of a project identified by the `prjid`. Project managers have

- Read access to all tables;
- Right to add/modify/delete entries in table `prjensemble` with matching entries in column `prjid`.
- Right to add/modify/delete entries in table `grp` for an ensemble referenced by `ensembleURI`[1] which according to table `prjensemble` belongs to the project `prjid`.
- Right to add/modify/delete entries in table `acl` for an ensemble referenced by `ensembleURI` which according to table `prjensemble` belongs to the project `prjid`.

Only owners of certificates in table `adm` can modify this table.

[1] For LDG: `ensembleURI` == `markovChainURI`.

7 Table `grp`

gid	cid
int	int

This table allows to define groups of people identified by their certificate subject strings. Note that groups are restricted to a project.

8 Table `acl`

eid	gid	writeRight
int	int	bool

Each entry defines group privileges, i.e. the rights of all members of group identified by `gid` with respect to the all documents and files which belong to the ensemble identified by ensemble ID `eid`. This includes the ensemble XML document, the configuration XML document and the binary files.

Read: For each entry in this table read privileg is assumed implicitly. For ILDG read privileges only affect the SEs as the metadata documents are required to be world-readable. If no entry exists with `writeRight` equal to false, the binary files are world readable (the XML documents are always world readable).

Write: Write privileges allow modification of both, documents in the MDC and files in the SE. By default, write access is not granted.

9 Update via WS

Table	Operation	Privilege	Webservice	Comment
certmap	insert	group	doAdmInsert, ...	Automatic insertion
	update	admin.	doCertMapUpdate	Only updates certID, not cid
	delete	admin.	doCertMapDelete	Only successfull if cid not in use
prjmap	insert	admin.	doPrjMapInsert	prjid is automatically assigned by MDC
	update	admin.	doPrjMapUpdate	Only updates prjName, not prjid
	delete	admin.	doPrjMapDelete	Only successfull if prjid not in use
grpmap	insert	manager	doGrpMapInsert	gid is automatically assigned by MDC
	update	manager	doGrpMapUpdate	Only updates grpName, not prjid or gid
	delete	manager	doGrpMapDelete	Only successfull if gid not in use
ensemble-map	insert	manager	doEnsembleMapInsert	eid is automatically assigned by MDC
	update	manager	doEnsembleMapUpdate	Only updates ensembleURI, not eid or prjid
	delete	manager	doEnsembleMapDelete	Only successfull if eid not in use
adm	insert	admin.	doAdmInsert	certID must be in VO
	update	—	—	No update operation
	delete	admin.	doAdmDelete	
manager	insert	manager	doManagerInsert	
	update	—	—	No update operation
	delete	manager	doManagerDelete	
grp	insert	manager	doGroupInsert	
	update	—	—	No update operation
	delete	manager	doGroupDelete	
acl	insert	manager	doAclInsert	
	update	—	—	No update operation
	delete	manager	doAclDelete	

10 Dependency graph