Deploying the gPLAZMA authorization framework in dCache.

gPLAZMA

grid-aware PLuggable AuthoriZation MAnagement

dCache Authorization -legacy

- SRM
  - Receives delegated proxy from srmcp
  - Looks up DN in dcache.kpwd
  - Forms UserAuthRecord: username, uid, gid, rootpath
  - Checks request against rootpath before transfer
- gridftpdoor
  - Receives delegated proxy from SRM
- dcap

dcache.kpwd:

```
# Mappings for 'cmsprod' users
mapping "/DC=org/DC=doegrids/OU=People/CN=Ted Hesselroth 898520" cmsprod
mapping "/DC=org/DC=doegrids/OU=People/CN=Shaowen Wang 342981" cmsprod

# Login for 'cmsprod' users
login    cmsprod    read-write    9811   5063    /    /pnfs/fnal.gov/data/cmsprod    /pnfs/fnal.gov/data/cmsprod
      /DC=org/DC=doegrids/OU=People/CN=Ted Hesselroth 898520
      /DC=org/DC=doegrids/OU=People/CN=Shaowen Wang 342981
```

gPlazma

- Invokes plugins for authorization methods
  - kpwd
  - grid-mapfile
    - Maps DN to username from grid-mapfile
    - Second lookup (from storage-authdb) for uid,gid,rootpath
  - gplazmalite-vorole-mapping
    - Maps DN and Role to username from grid-vorolemap
      - "/cms/uscms/Role=cmsuser/Capability=NULL"
    - Second lookup (from storage-authdb) for uid,gid,rootpath
  - saml-vo-mapping
    - Maps DN and Role to username from GUMS
    - Second lookup (from storage-authdb) for uid,gid,rootpath

storage-authdb:

```
authorize    cmsprod    read-write    9811   5063    /    /pnfs/fnal.gov/data/cmsprod    /pnfs/fnal.gov/data/cmsprod
```

gPlazma Cell

- Runs as gPlazma@gPlazmaDomain
- Takes authorization requests from other cells
  - SRM
  - gridftpdoor
  - dcap (future)
- Invokes gPlazma authorization method, which
  - Tries methods specified in policy file
  - Acquires UserAuthRecord
- Sends UserAuthRecord to requesting cell
- dcachesrm-gplazma.policy
    - Which authentication plugins to try
    - Order in which to try plugins
    - GUMS url for saml-vo-mapping plugin

Deploying gPlazma Cell

- Included in 1.7 release candidate
  - Turned off by default
- To turn on
  - Prepare configuration files consistent with your site's uid, gid, and rootpaths
  - Edit gplazma policy file.
  - Set GPLAZMA=yes in node_config
  - In srm.batch and gridftpdoor.batch
    - -use-gplazma-authorization-cell=true \
  - Restart cells
- If using saml-vo-mapping
  - Deploy GUMS server
- https://srm.fnal.gov/twiki/bin/view/SrmProject/GPlazmaHowTo
- GPLAZMA@fnal.gov

Future Work

- Test deployment
- dcap support
  - Call with DN and Role rather than delegation
- Improvements to storage-authdb file
  - Database
  - Maintain consistency with CE
    - Common database with GUMS
    - VOMS
  - Storage Authorization Service
    - Web service
  - Dynamically assign
    - Create root path per username