Authorization in Data Management

Ákos Frohner on behalf of the Grid DM Team
CERN – JRA1 All Hands meeting, 2007-10-25

DPM/LFC: POSIX permissions

POSIX style file and directory permissions

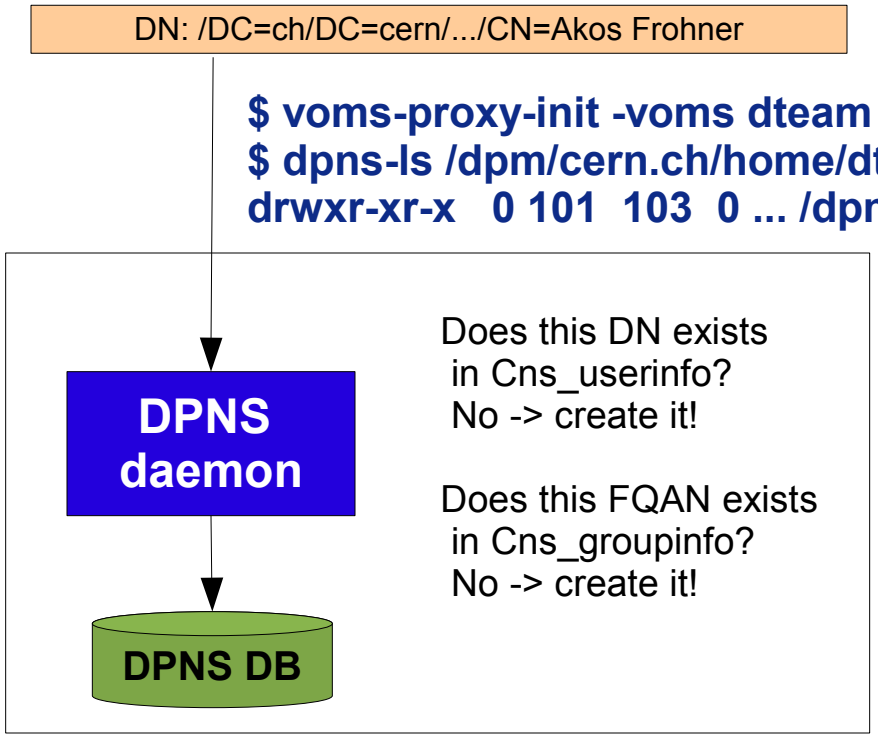
- **owner = DN of the creator**
- **group = first VOMS FQAN of the creator**
  - except, with set-group-id directories, where the group is inherited
- **basic read/write/execute permissions for user/group/others**
- **POSIX ACL:**
  - Access ACLs: set permissions for other users and groups
  - Default ACLs on directories: they are inherited by each entry created within.

Exact match: any of the user's DN or VOMS FQANs has to match exactly one of the permissions on a file.

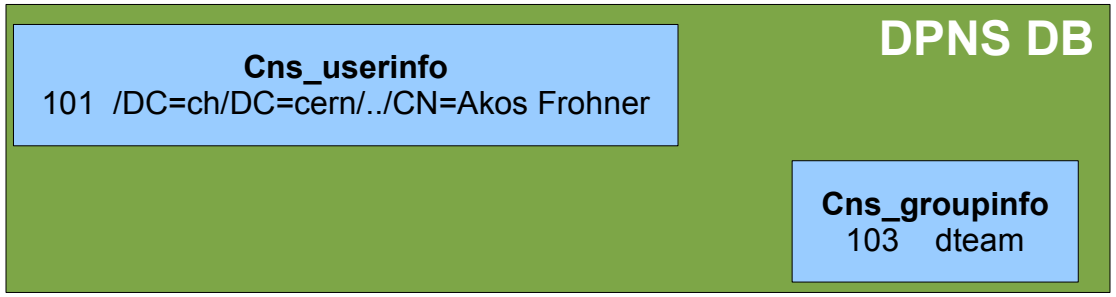
DPM/LFC: examples

```
$ dpns-mkdir /dpm/cern.ch/home/dteam/akos
$ dpns-chmod 0755 /dpm/cern.ch/home/dteam/akos
$ dpns-setacl -m d:u::rwx,d:g::r-x,d:o:- /dpm/cern.ch/home/dteam/akos
$ dpns-setacl -m 'g:biomed:r-x,m:rwx' /dpm/cern.ch/home/dteam/akos
$ dpns-setacl -m \
    'u:/DC=ch/DC=cern/.../CN=Remi Mollon:rwx,m:rwx' /dpm/cern.ch/home/dteam/akos
$ dpns-getacl /dpm/cern.ch/home/dteam/akos
# file: /dpm/cern.ch/home/dteam/akos
# owner: /DC=ch/DC=cern/.../CN=Akos Frohner
# group: dteam
user::rwx
user:/DC=ch/DC=cern/.../CN=Remi Mollon:rwx  #effective:rwx
group::r-x                  #effective:r-x
group:biomed:r-x        #effective:r-x
mask::rwx
other::r-x
default:user::rwx
default:group::r-x
default:other::---
```

DPM/LFC: Virtual uid and gid

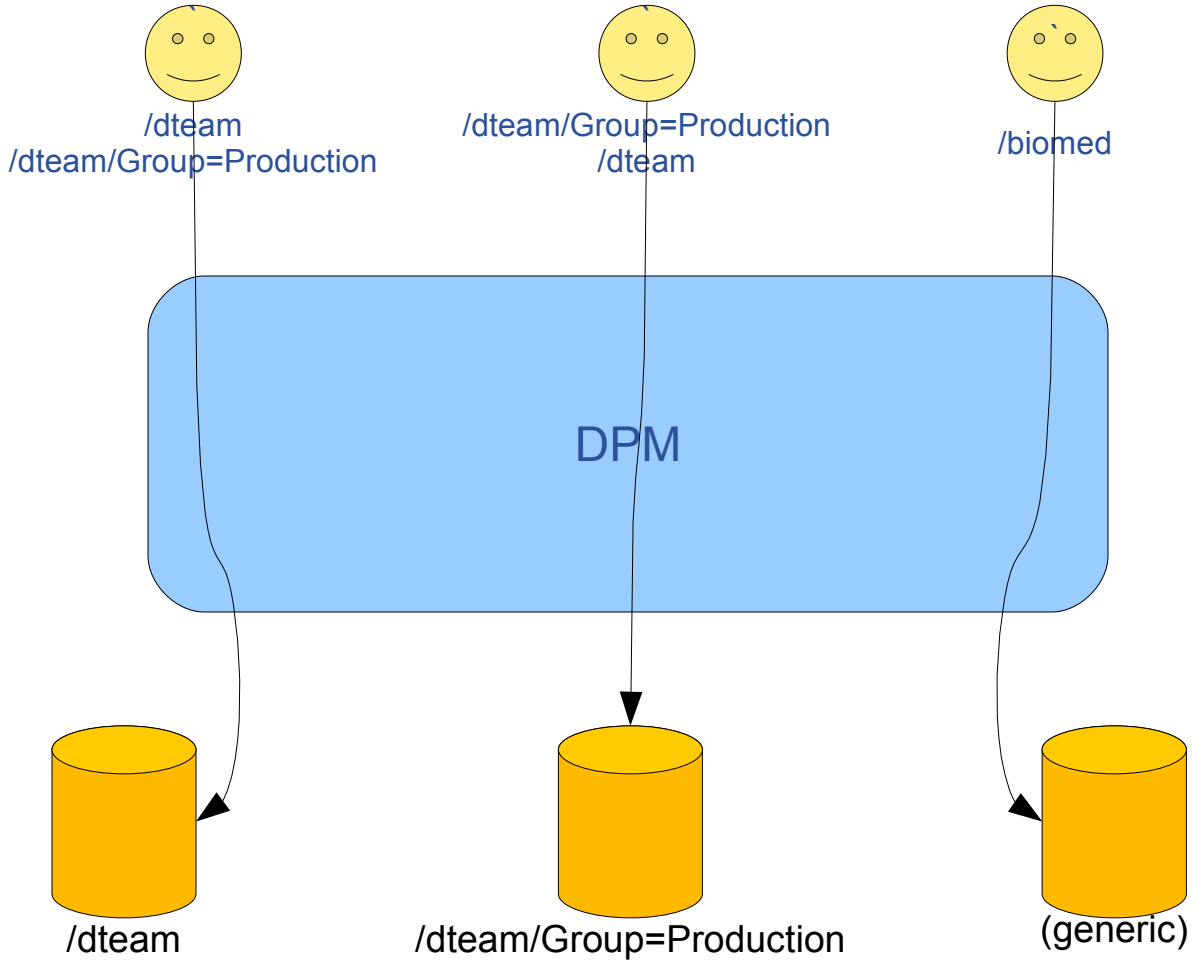


- no need to create pool accounts
- no need to change the /etc/passwd file
- faster check on ACL than with string/pattern matching on DN/FQAN



DPM: pool selection

Pool selection when creating a new file in DPM



- exact match based on the first FQAN
- match pool with enough space
- otherwise match with the generic pool

Hydra permissions

Hydra keystore permissions is almost like POSIX, but

- **there is no hierarchy or there is no directory permission (follows the Windows model)**
- **creating an entry is protected by a global VOMS FQAN i.e. like a toplevel directory permission**
- **owner = DN, group = first VOMS FQAN on a new entry**
- **operations on a key:**
  - get key content
  - set key content
  - change permission
  - delete the key

Exact match: any of the user's DN or VOMS FQANs has to match exactly one of the permissions on a file.

Hydra: examples

```
# create restricted to '/biomed'
$ voms-proxy-init -voms biomed
$ glite-eds-key-register /some/file
$ glite-eds-get-acl -v /some/file
        ...
        Base perms: user pdrwl-gs, group --------, other --------
$ glite-eds-chmod g+g /some/file
$ glite-eds-get-acl -v /some/file
        ...
        Base perms: user pdrwl-gs, group ------g-, other --------
$ glite-eds-set-acl -m '/DC=ch/DC=cern/.../CN=Remi Mollon:g' /some/file
$ glite-eds-get-acl -v /some/file
        ...
        /DC=ch/DC=cern/.../CN=Remi Mollon:------g-
$ glite-eds-encrypt /some/file local.file local.file.encrypted
```

Operations in 3 category:

- global: submit, query, cancel, administrate
  authz: VOMS FQAN or gridmap file per type of operation
- channel specific: set/get attributes
  authz: list of DN or FQAN in DB
- VO specific: set/get per-VO attributes
  authz: list of DN or FQAN in DB

The client's DN and the set of FQANs are compared by string equality with the authorization attributes above.

In case of the first match the operation is authorized.

Exception is the cancel operation, which only the submitter or the global administrator can call.

FTS: examples

```
# submit VOMS FQAN: /org.acme
$ voms-proxy-init -voms org.acme
$ glite-transfer-submit -d srm://a.example.org/a srm://b.example.org/b
      ... <jobid>
$ glite-transfer-cancel <jobid>
# admin VOMS FQAN: /org.acme/Role=fts-admin
$ voms-proxy-init -voms org.acme -role /org.acme/Role=fts-admin
$ glite-transfer-channel-add AB A B
$ glite-transfer-channel-addmanager AB "/DC=ch/DC=cern/.../CN=Akos Frohner"
$ glite-transfer-channel-listmanagers AB
      ...
      /DC=ch/DC=cern/.../CN=Akos Frohner
$ glite-transfer-channel-setvoshare AB /org.acme 100
$ glite-transfer-addvomanager /org.acme "/DC=ch/DC=cern/.../CN=Akos Frohner"
$ glite-transfer-listvomanagers /org.acme
      ...
      /DC=ch/DC=cern/.../CN=Akos Frohner
$ glite-transfer-channel-setvoshare AB /org.acme 50
```