WP4 Security

Planning for Release 2.1

David Groep, NIKHEF
davidg@nikhef.nl

WP4 Gridification Task
Martijn Steenbakkers
Gerben Venekamp
Oscar Koeroo
Wim Som de Cerff

http://hep-proj-grid-fabric.web.cern.ch/

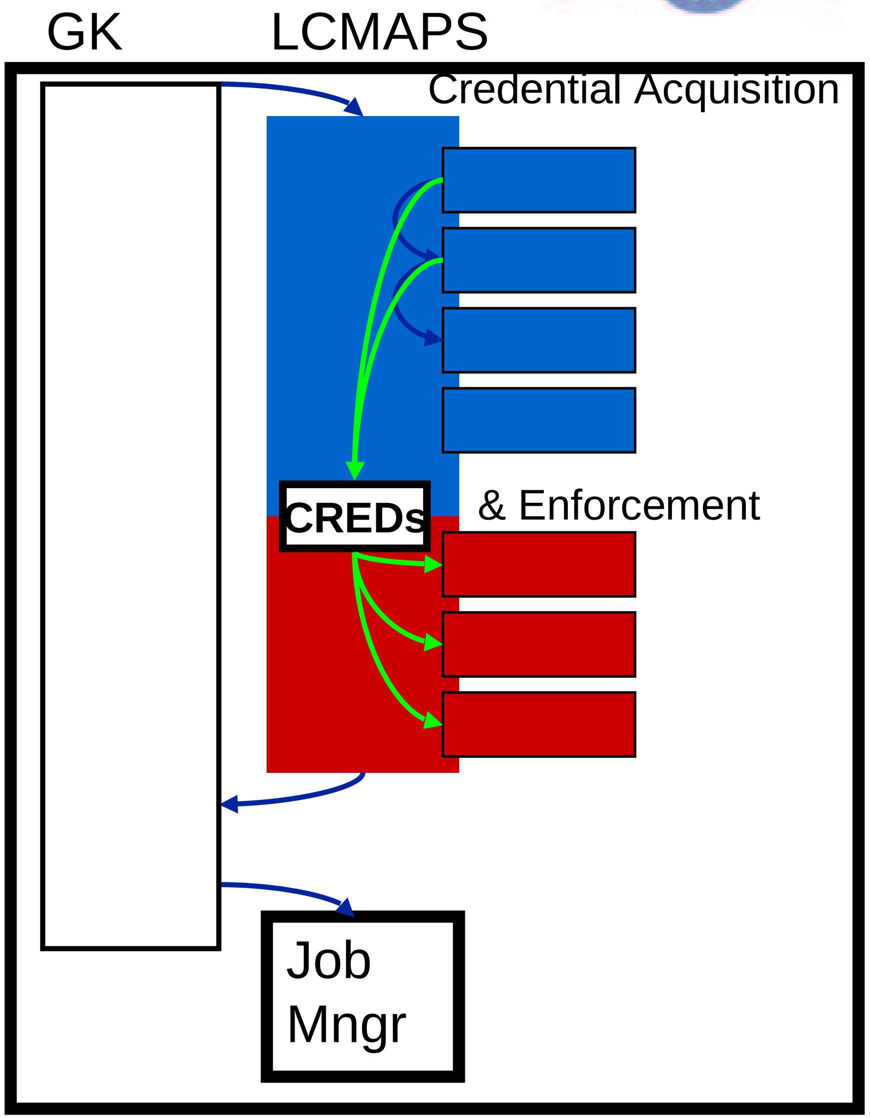
Components

- **2.5.1** **LCMAPS “framework”**
  COMPLETED NOW (slot July 11th)
- **2.5.2** **AFS and Kerberos5 LCMAPS plugins**
  for 2.1 (integration slot in August)
- **2.5.3** **Job Repository**
  there, but limited in 2.1…
- **2.5.4** **VOMS, POSIX-local, PoolAccounts plugins**
  2.1 (integration slot Monday, July 11th)
- ***2.5.5*** ***LCAS server***
  2.1
- ***2.5.6*** ***FLIdS***
  ‘optional’ component
- ***2.5.7*** ***FabNAT***
  ‘optional’ component

LCMAPS framework

- New API to get to VOMS attribs
- Legacy API gss_assist_gridmap()

- Cred Acquisition plugins
  - (VOMS) PoolAccount
  - PoolGroups
  - VOMS
  - LocalAccount
  - AFS/Kerberos
- Enforcement plugins
  - POSIX-LDAP
  - POSIX-in-process



Status of plugins

- ‘Equivalence’ functionality is there today
- VOMS attributes can be acquired, minor mods being done
- AFS needs new design of interaction with KDC
  - No plaintext password files anymore
  - Minimal interference with KDC
  - Preferred
    - no ‘patched source’ for KDC (hard to make really robust)
    - X509 to ticket service next to KDC, with access to the shared secret
- Enforcement in central user directories is there today
  needed for support of VOMS in the fabric
  - Out-of-the-box support for LDAP
  - But YP is very hard, and plain files almost impossible

Local authorization issue

- User/group management on a cluster

IF you want to use VOMS-based authorization
AND you have a cluster as an execution system
THEN you **must** run a distributed user administration
and for this release such a user directory **must** be based on LDAP

- Edg-lcfg-authconfig is there

Map files

New in /etc/grid-security/grid-mapfile

```
"/VO=wilma/GROUP=*“   .test
"/VO=fred/GROUP=*"    .fred
“/*”                 .pool
```

/etc/grid-security/group-mapfile

```
"/VO=fred/GROUP=fred/ROLE=husband“ bogus1
"/VO=fred/GROUP=fred/mstest"       bogus2
"/VO=fred/GROUP=fred*"             .pool
#"/VO=fred/GROUP=fred*"            bogus2
"/VO=wilma/GROUP=wilma/pebbles"    bogus3
"/VO=wilma/GROUP=wilma*"           bogus4
"/VO=wilma/GROUP=*"                .pool
```

Issues

Site policy configuration and thinking is needed

- How to handle poolaccounts in the wake of >1 role/user?
- Job accounting issues (primary group membership)
- Group explosion on a site
  due to changes in VOMS database made by a VO admin
- Really needs a Grid-aware file system (/grid)!

  … *which in turn needs the JobRepository*

Other components

- LCAS server implementation
  - Effort available only for “minimal” separation
  - Target should be SAML, *will not be in 2.1*
  - VOMS AuthZ as discussed yesterday (XACML/GACL)
    but tight on effort, must be able to re-use much stuff

- JobRepository
  - “Ambiguous” information based on uid *will be there in 2.1*
  - Retrieve credentials/RSL/etc based on current process context
    might be post 2.1…