VOMS deployment

- Extent of VOMS usage in LCG-2
  - Node types
- gLite 3.0
- Issues
- Conclusions

LCG node types aware of VOMS

- UI
- RB
  - To small extent
- CE
- Classic SE
- LFC
  - Version 1.4.5 (in LCG 2_7_0)
  - Native, no user accounts needed
- DPM
  - Version 1.5.x (code tested and tagged, rpms not yet available)
  - Native, no user accounts needed

- Work in progress (ties in with SRM v2.1 ACLs):
  - dCache
  - CASTOR

Resource Broker

- RB itself does not distinguish groups/roles/...
  - Jobs just passing through
- Proxy renewal daemon also renews VOMS extensions
- Other components ignore VOMS extensions
  - E.g. Condor-G
    - Will launch a single grid_monitor per CE per DN
- But the CE does not!
  - VOMS proxies and normal proxies will be mapped to different pool accounts
  - Each set of FQANs has a different mapping
  - A grid_monitor for one UID cannot handle jobs for other UIDs
- Users cannot quickly switch between groups/roles
  - Must wait for old grid_monitor & grid_manager instances to exit...

- Is this problem avoided in the gLite WMS?

Computing Element

- LCMAPS first tries VOMS mapping
  - Fall back on standard grid-mapfile
    - Derived from VOMS (and LDAP) servers
      - Take most priviliged mapping per DN
- VOMS plugin grid- and group-mapfile default contents
  - Before LCG 2_7_0:
    - Only distinguish sgm from normal users
      - But no VOMS proxy needed for that
  - With LCG 2_7_0:
    - Also distinguish production manager
    - Start to distinguish groups
      - Currently only CMS have supplied content (see next page)
- VOMS already used more in other VOs and partner grids
  - GridIt/INFNGrid, GridIreland, ...
- Each set of FQANs gets a different pool account
  - May need many more accounts than DNs!
    - Pool accounts should *not* be recycled quickly

LCG 2_7_0 grid- & group-mapfile

- Grid-mapfile

```
“/VO=cms/GROUP=/cms/ROLE=lcgadmin” cmssgm
“/VO=cms/GROUP=/cms/ROLE=production” cmsprd
“/VO=cms/GROUP=/cms/HeavyIons” .cms
“/VO=cms/GROUP=/cms/Higgs” .cms
“/VO=cms/GROUP=/cms/StandardModel” .cms
“/VO=cms/GROUP=/cms/Susy” .cms
“/VO=cms/GROUP=/cms” .cms
```

- Group-mapfile

```
“/VO=cms/GROUP=/cms/ROLE=lcgadmin” cms
“/VO=cms/GROUP=/cms/ROLE=production” cms
“/VO=cms/GROUP=/cms/HeavyIons” cms01
“/VO=cms/GROUP=/cms/Higgs” cms02
“/VO=cms/GROUP=/cms/StandardModel” cms03
“/VO=cms/GROUP=/cms/Susy” cms04
“/VO=cms/GROUP=/cms” cms
```

CE group-mapfile usage

- Set primary GID based on first VOMS group/role that matches
  - User will always pick up at least the standard GID for the VO
    - Possibly as secondary GID
  - Order of entries important in grid- and group-mapfile
- Batch system to set scheduling priority also based on primary GID
  - Not only UID
- No recipes for LCG 2_7_0 yet
  - Some batch systems may need work to support this model
    - Custom submit wrappers could be developed where needed
- How to advertize such queue behavior in the information system?
  - A queue may look full, but certain groups/roles might find their jobs run immediately

VOMS capabilities

- How can a VO centrally affect scheduling of groups/roles?
  - Use case:
    - The Higgs group needs to run many jobs now for next week's conference
- All site admins could be asked to change their queue parameters
  - Practicable for the short term
    - Only a few groups/roles, priority changes very infrequent
- A VOMS capability could be mapped to a high-priority queue
  - Capability would be set by VOMS server
  - Users would only ask for groups and roles in their proxies
  - VO admin would associate capabilities with certain groups/roles
    - E.g. move high-priority capability to group/role that currently needs it
- Work in progress?

VOMS server host certificates

- VOMS-aware services need host certs of all trusted VOMS servers
  - Currently typically distributed via rpms
    - Some VOs use insecure web servers or unsigned e-mail
      - Security vulnerability
  - Maintenance problem
    - Old host cert for voms.cern.ch expires today (!)
      - Needed “emergency” rpm update providing both new and old certs

- New model being worked on
  - Services only need host DNs of all trusted VOMS servers
  - VOMS proxy will carry copy of VOMS host cert

VOMS versions in LCG-2_7_0

- gLite voms 1.6.10
  - Latest officially released version (gLite 1.4.1, 1.5)
  - In use on voms.cern.ch and lcg-voms.cern.ch
  - Needed for DPM gridftpd
    - Because of retrieve() symbol clash in older versions
  - LFC cannot use it because of:
    - Thread-safety problems
    - Memory leaks
  - Client issues mostly fixed in 1.6.15 (tested)

- EDG voms 1.5.4
  - EDG build of gLite voms 1.5.4
  - Introduced in LCG-2_6_0
  - Some minor problems with work-arounds were reported
  - Default choice
    - PATHs have $EDG_LOCATION earlier than $GLITE_LOCATION

Conclusions and plans

- Services are becoming really aware of VOMS
  - Good news, but also puts constraints on VOMS API changes
  - Standard grid-mapfile may be needed for legacy components
- Important improvements being worked on

- Plan for gLite 3.0:
  - Certify gLite voms 1.6.x where x >= 15
    - Both client and server
    - Try and fix only critical issues
  - Remove the old EDG voms