LHCb and VOMS

GDB March 2006

Slides prepared by Ricardo Graciani

Use Cases

1. Individual use of the GRID.
2. A number of users want to share the task of running on the GRID:
   - Some are in charge of creating jobs
   - Some are in charge of submitting jobs
   - Some are in charge of monitoring job
   - Some are in charge of retrieving outputs
   - Some are in charge of cleaning
   - …
   - This is already the case for MC production, but will be a similar case for most sub-detector activities, alignment, calibration, group-analysis,…
3. The VO managers with "root" like privileges:
   - A user has filled some SE, causing problems to other users.
   - …

VOMS Groups and Roles

- Philosophy.
  - Maximum simplicity
- All lhcb users are assigned to:
  - /lhcb
- VOMS Groups are created for users that need to share resources:
  - /lhcb/production
  - /lhcb/…
- VOMS Roles required for different MW behaviours.
- Short user VOMS "Alias" used to assign a simple (e.g. CERN AFS account) unique name to each VO user.
- VOMS proxy holds a selected Group/Role if needed.
  - Only the first Group/Role held in the proxy matters.

VOMS and LCG Services (I)

- Middleware uses information in VOMS proxy to assign the user to a given Group/Role
- By default "lhcb:/lhcb" is used. But …
  - The user fully keeps the identityi.e. user is owner of jobs & data.
  - He/she is the only one allowed to access to his/her jobs.
  - He/she is the only one with write access to his/her data.
- If a given group is selected in the proxy:

```
# voms-proxy-init -voms lhcb:/lhcb/production/Role=Group
```

  - The group becomes the owner of jobs and data.
  - Other group members have full access to jobs and data.
  - The default user proxy has no longer full access.

VOMS and LCG Services (II)

- The "User" Role: lhcb:/lhcb[/Role=User]
- The "Group" member Role: lhcb:/lhcb/XXXX/Role=Group
- The "Manager (=Admin?)" Role:
  - Middleware uses information in VOMS proxy to assign the user to a given Group/Role.
  - One or more Manager users for the VO and for each group.

```
# voms-proxy-init -voms lhcb:/lhcb[/xxxx]/Role=Manager
```

  - The VO Manager must authorize the registration of new users in the VO (lhcb:/lhcb).
  - The VO Manager is responsible of creating new groups (+ Group Manager).
  - The Group Manager must authorize users entering the group.
  - The VO Manager has full access to jobs and data.

Summary

Groups	Roles		
	User	Group (Member)	Manager
/lhcb	Allowed	Not Allowed	Allowed
/lhcb/production	Not Allowed	Allowed	Allowed
/lhcb/xxxx	Not Allowed	Allowed	Allowed

- Group/Role is selected using the voms proxy.
- Mapping to local user is dynamic (not based on DN).
- In all cases, by default, any VO member has read access to data.
- LHCb needs Groups to share tasks in the GRID.
- Higher priority to data management m/w with respect of workload management m/w.