VO Authorization in EGEE

Erwin Laure
EGEE Technical Director

Joint EGEE and OSG Workshop on VO Management in Production Grids
HPDC 2008
Boston, USA

Authorization in EGEE

- **Gaining access to EGEE resources is governed by VO membership**

- **EGEE does not own or manage resources**
  - Resource centers are independent and allow certain VOs to access their resources
  - Resource centers govern the usage policy
    - Set quotas, priorities, shares etc. for VO members
  - EGEE provides mechanisms for VOs and resource centers to negotiate usage (out of band)

- **Users are identified via X.509 proxies**
  - VO membership via VOMS
  - VO information can be passed inside proxy or is used implicit when generating gridmap files

Separation of Concerns

- **VOs manage their membership and associated information (groups, roles, etc.)**
- **Resource Centers ensure fulfillment of their commitments to VOs using their own policies**
  - E.g. fair share, fixed quota etc.
- **Problem:**
  - VOs want to have ways to control how their allocation at a resource center is being shared among the VO members

Use case: ATLAS Experiment

- **Atlas wants to guarantee shares for production and analysis activities**
  - At some centers 80% of CPU resources allocated to Atlas should be guaranteed to production, at other sites 50%
  - Those values are rather static (may be need to change them O(1year))

- **Many national grids want to ensure shares to users of the same country**
  - Hierarchy already explicit in ATLAS VOMS.
  - Sites do not want to deploy separate queues in batch system

Different Strategies

- **Late binding**
  - A VO scheduler decides what to do with the resource once the resource was allocated to the VO
  - aka pilot-job, glide-in, etc.

- **Provide hooks in middleware to allow VOs to express their policies**
  - Atlas use-case:
    - Even if pilot systems are used, job priority mechanism is still needed
      - *Simplifies scheduling of production and analysis pilot jobs*
        - Submission relative ratio does not need to be throttled by the VO
      - *Analysis in ATLAS can be performed via pilot jobs but also in push mode.*

Current Situation in EGEE

Problem:

- static mapping FQAN/gid/share
- change of VO policy requires site intervention
- one gid per VO/share

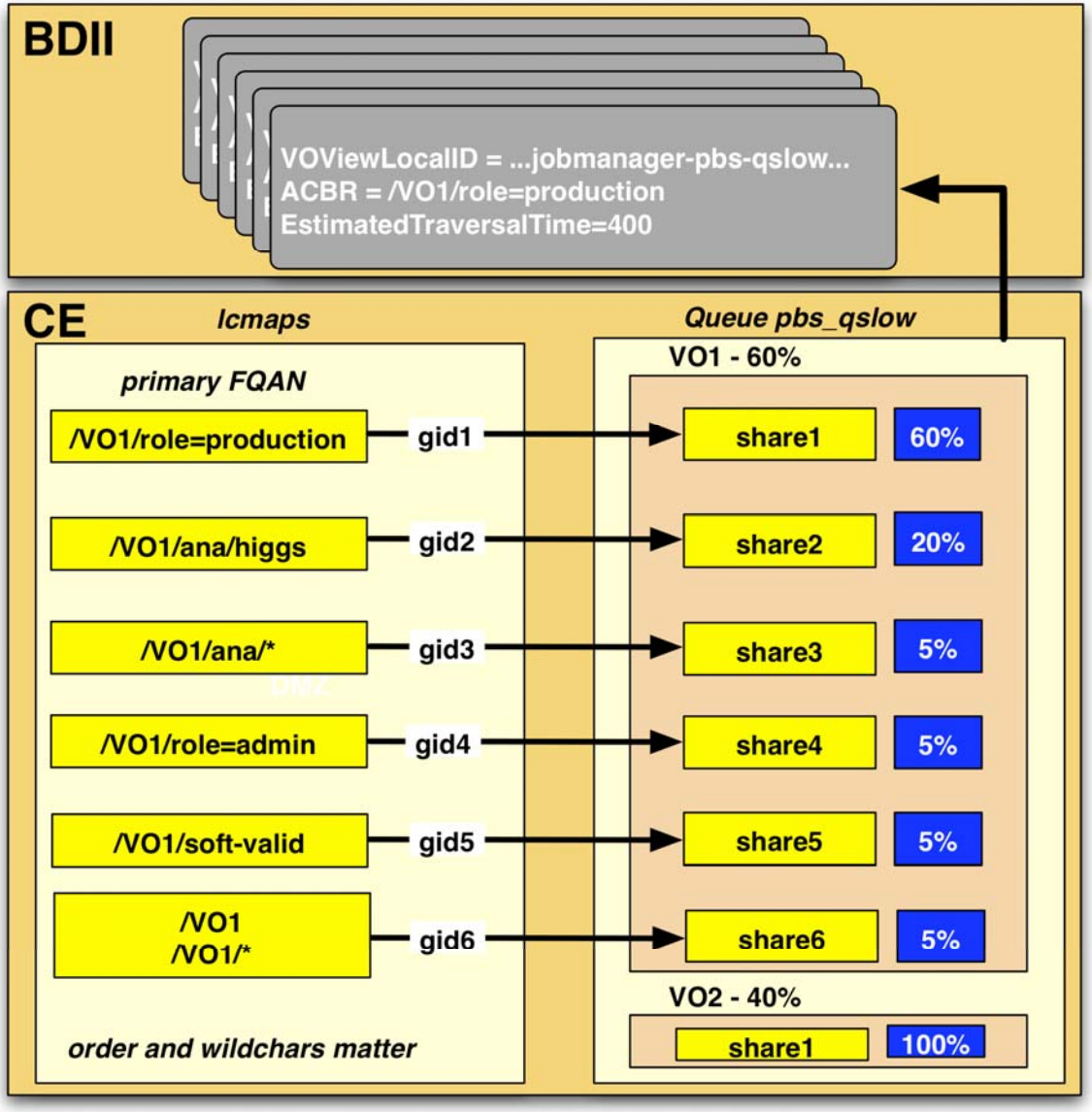
JOB 1
/VO1/role=production
/VO1

JOB 2
/VO1/role=admin
/VO1/ana/higgs
/VO1/

JOB 3
/VO1/ana/higgs
/VO1/ana/
/VO1

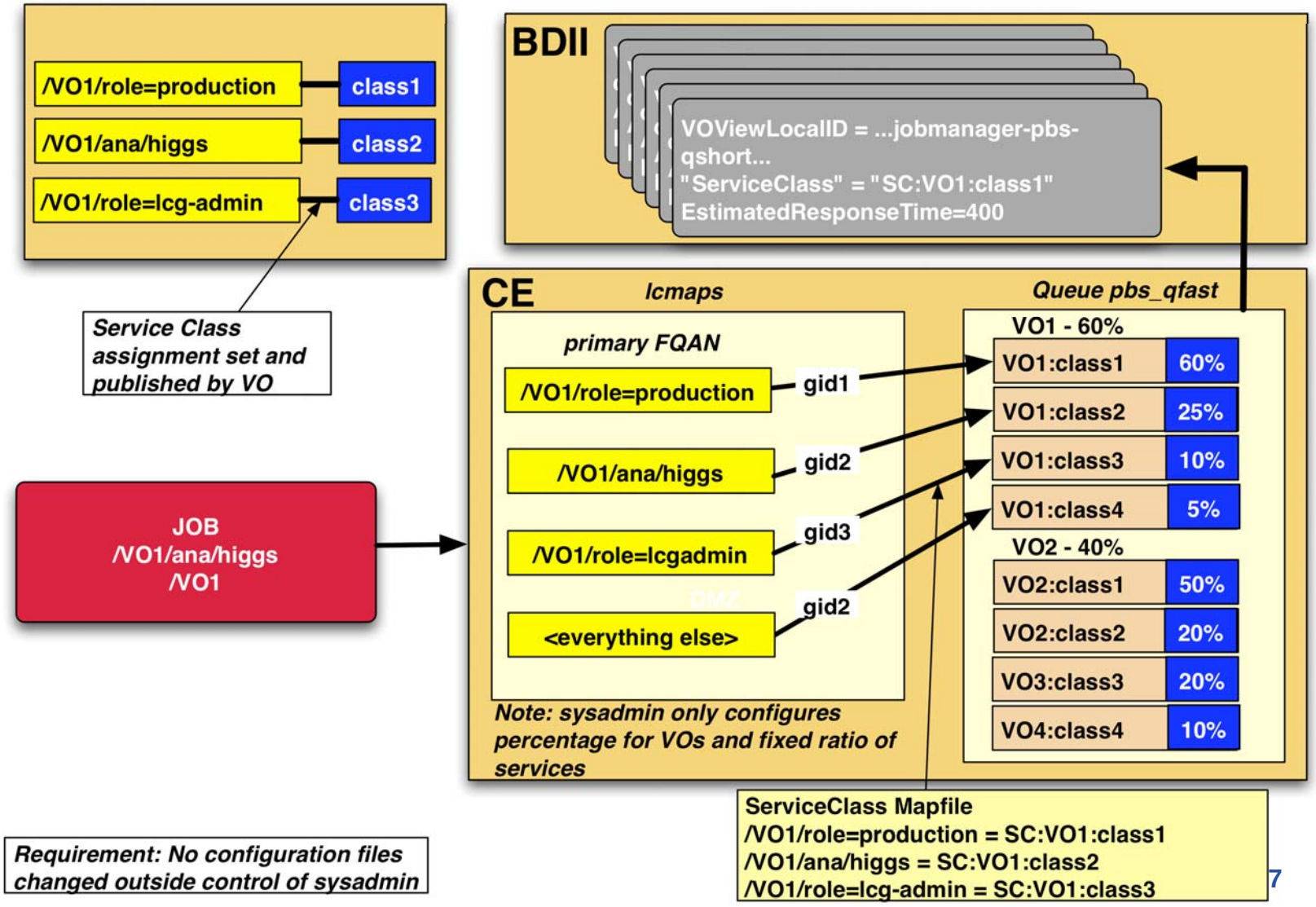
JOB 4
/VO1/
/VO1/ana/mesons

JOB 5
/VO1/ana/mesons
/VO1



Proposed changes

Decouple FQAN/gid/share mapping -- No link gid scheduling decision any more
Still service class share needs to be fixed



Long term strategy

- **EGEE is revising its authorization framework**
  - Requirements:
    - Uniform authorization and policy management in gLite
    - Compatible with SAML and XACML standards
    - Built on the experience of previous systems
      - *LCAS/LCMAPS, SCAS, G-PBox, gJAF*
    - Usable with different authentication mechanisms
      - *X.509 proxies, uid/password, shibboleth, kerberos tokens …*
  - Preserve separation of concerns
    - But provide hooks in policy decision point together with flexible ways of specifying the execution environment (virtual machine, uid/gid, …)
- **Provide a generic VO scheduler framework with reference scheduler?**

Summary

- **Clear need for a separation of concerns:**
  - Inter-VO policies: sites
  - Intra-VO policies: VOs
- **VOs are struggling expressing their intra-VO policies and have them implemented on the infrastructure**
- **Two strategies have been followed:**
  - Late binding and VO schedulers
  - Hooks in middleware
- **Both need to be continued in the mid term**
- **Harmonization of compute and data policies needed**