Follow-up on Authorization

Christoph Witzig, SWITCH
(christoph.witzig@switch.ch)

MWSG March 27, 2008

www.eu-egee.org

Information Society and Media

Outline

- Introduction
- Status of recommendations
  - Feedback received
  - Proposed action and timeline
- Summary

Goal of the Study

- **Task by C.Grandi to look into authorization (authZ) in gLite from end-to-end with the goal to**
  - Make recommendations for changes in existing authorization mechanisms and
  - specify design for “authorization service” work item in EGEE-III
- **Should specify the work in 2008 / early 2009**
  - Comment: should be fully deployed within lifetime of EGEE-III

Timeline

- September / early October: requirement gathering
- mid-October - late Nov: working out the recommendations and a proposal of the design
- Discussion at MWSG meeting in December
- Presentation and decision in TCG in January
- Follow-up presentation in TCG March 12, 2008

Priorities

List of priorities in order (as approved by TCG):

1. **Should fix some of the limitations of the current authZ framework**
2. **Introduce new features to the extend that they are needed by the**
   1. Experiments / VOs
   2. Sites / SAx
   3. JRA1
3. **Interoperability**
4. **Use of standards if possible**

Focus

- **The priorities as well as the JRA1 budget determined the focus of the study, namely**
  - Rather improving and gently extending the current authorization framework than proposing a new, radically different authorization solution
- **Note:**
  - Recommendations reflect my impressions and to a certain degree also my personal preferences

Outline

- Introduction
- **Status of recommendations**
  - **Feedback received**
  - **Proposed action and timeline**
- Summary

Recommendations

- **Recommendations for**
  - Pattern matching rules
  - User Interface
  - CE
  - WMS
  - New Authorization Service
  - Data Management

Pattern Matching Rules (1/2)

- **Recommendations:**
  - **A standard library and a test suite should be developed, which implements the FQAN pattern matching rules. They should become part of the standard gLite distribution. Existing code should be modified to use this library wherever possible. Where this is not possible, the existing implementation should be tested against the test suite.**
    - **Note: a first version of this library already exists and is in use**
  - **The only supported wildchar should be the asterix character ("*"). The initial implementation should restrict the wildchar usage to**
    - ***In the group string after the trailing slash***
    - ***The "role=" string to denote all possible roles***
  - **A command line tool, available on the WMS and CE, should print the authorization decisions for every package in the CE and WMS. The input parameter of this debugging utility can either be the primary FQAN or a proxy certificate.**

Pattern Matching Rules (2/2)

- **Examples for patterns**
  - /VO1/analysis/* OK
  - /VO1/analysis/*/role=production OK
  - /VO1/analysis/*/role=* OK
  - /VO1/*/higgs NOT OK
  - /VO1/analysis/?iggs NOT OK
  - Note: /* as pattern to denote all VOs is not allowed

- **Feedback received is positive or neutral**

- **TCG decision:**
  - All three recommendations accepted
  - Timeline:
    - short term (<6 months)

User Interface

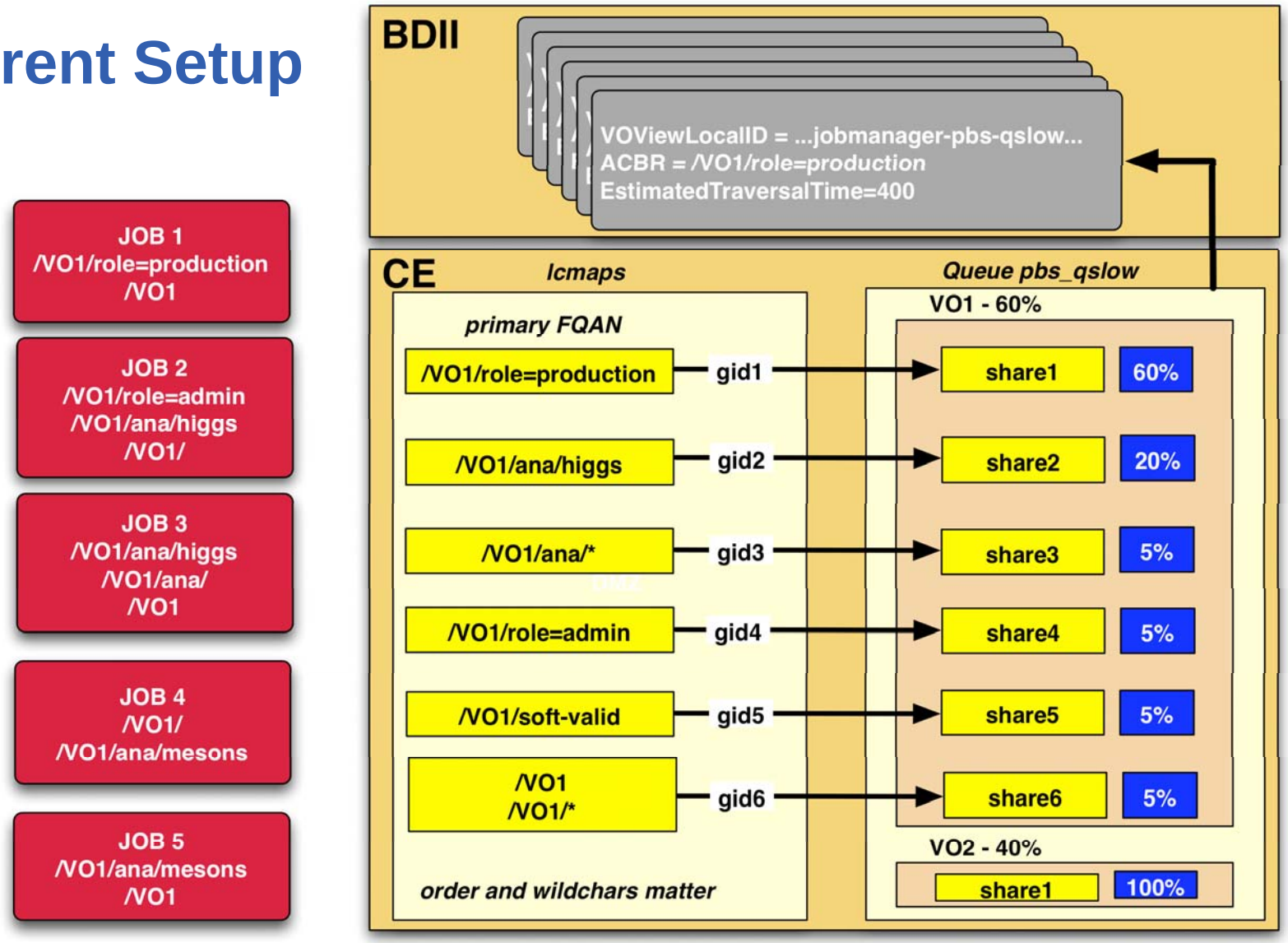
- **Recommendation:**
  - **We recommend that the user shall be able to specify the FQAN to be used in the job submission either as a parameter in the JDL file or as a variable in scripts.**

- **Background:**
  - **Currently only one primary FQAN for job handling and data management**
  - **Allows to submit jobs with one primary FQAN while another primary FQAN is taken for the data management**
  - **Implementing a flexible way to set the primary FQAN is hard (DM interfaces)**

- **TCG decision:**
  - Work on pre-ws-GRAM CE needs evaluation
  - Implement in CREAM CE
  - Make feature available to user once CREAM CE is deployed in a sizeable fraction of the sites
    - Possibly by Tier

CE Setup

Current Setup



CE (1/2)

- **Recommendations FQAN handling in WMS - CE**
  - **Instead of taking the first match, LCMAPS should return the GID corresponding to the most specific match. The most specific match is the match, which matches the most characters excluding any possible wildchar.**
  - **The WMS should only consider one VOView per CE for a given primary FQAN. The selected VOView should be the one, whose ACBR is the most specific match for the primary FQAN.**

CE (2/2)

- **Feedback received:**
  - Generally judged positive
  - Can be done with available manpower in JRA1
    - Only localized changes in middleware
- **TCG decision:**
  - Implement in the short term
- **Benefits:**
  - Will remove ambiguity between CE and WMS and guarantees that the same algorithm by both
  - No DENY tags

Data Management

- **Recommendation**
- All storage element implementations should adopt the DPM authorization model.

- Comment:
  - This has already been decided.

- **Proposed action:**
  - none

Summary Recommendations (1/2)

- **Implement some of the recommendations in the near term**
- **Move some of the recommendations into the new authorization service**
  - Make pFQAN user selectable for job management
  - Linking FQAN - UID/GID - shares and enabling VO to set FQAN - share assignment
  - Time horizon of 1 1/2 years
- **No mid-term work**

Summary (2/2)

- **Short term solution:**
  - Implement recommendations on pattern matching
  - Implement recommendations for FQAN handling in WMS and CE to guarantee a consistent job handling between them as soon as possible
- **Benefits:**
  - Simpler pattern matching (less error prone)
  - Consistent pattern matching in code
  - Consistent job handling between WMS and CE
  - Modest amount of work
- **But: This is a short term fix**
  - Long term issues addressed within the context of the new authorization service