Update Authorization Service

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

TMB Feb 11, 2009

www.eu-egee.org

Information Society and Media

Outline

- Status deployment proposal
- Global banning policy
- Update current work

Deployment Proposal

- **Received very little feedback**
- **Revised version contains**
  - Minor changes
  - Description of UID-GID mapping mechanism
- **Requested WMS use-case**
  - Provided as a separate note (in EDMS)
  - Note: We do not expect that site administrators manipulate XACML files but rather
    - Use command line interface for most common commands
    - Edit simplified notation policy files

Global Banning Policy

- **Discussed within JSPG (ongoing)**

- **OSCT operates a central banning service (CBS)**
  - Sites SHOULD use CBS
    - SHOULD or MUST?
  - Sites SHOULD give CBS priority over local policies
  - Sites SHOULD configure CBS so any ban/restore action is active in under 6 hours
    - Time period still under discussion
  - Grid Security Operations MUST inform VO manager whenever user/group access is changed (ban & restore)
- **SHOULD= Obligation with escape clause**
  - Inform Grid Security Office.

Policy for Global Banning
(Full text - currently under Discussion)

- In order to manage security threats against the infrastructure, it may be necessary to restrict the access to grid resources for certain users, groups of users or VOs. These precautionary measures need to be implemented at different levels of the Grid infrastructure, in order to enable the sites to protect their resources, the VOs to control the access of their users, and for Grid security operations to apply timely emergency access restrictions across the whole Grid.

- Each site manages its own local access policies to its resources. In addition, Grid security operations SHOULD operate a central banning service. Whenever Grid security operations bans a user or group of users, or restores their access, they MUST inform the appropriate VO Manager.

- Sites SHOULD deploy this central banning service and give it priority over local policies.

- The site implementation of the central banning service SHOULD be configured such that any ban or restore action made by Grid security operations is active at the site without a delay of more than 6 hours

Update on current work

- **authZ group revised project plan**
- **Expect now the service to enter certification in the first half of April**
  - previous estimate: second half of March
- **Meetings planned in Feb/Mar with**
  - CREAM developers
  - WMS developers
  - OSCT