WP1 Plans for Security

Daniel Kouřil

CERN, July 9–10, 2003

Logging and Bookkeeping Service

- *Collects events associated with jobs into a LB database and provides access to them*
- *Events enter the LB infrastructure through 'local-logger', passed to 'interlogger' and transfered to 'LB server' and stored in LB db.*
- *All the LB components use GSI authentication*

Authorization in the LB

Access to information about jobs

- *allow job owners to control access to information about their jobs stored in the LB*
- *allow owners to change ACL's arbitrarily*
- *keep ACL's close to job events and let the EDG components processing the events (R-GMA) evaluate and enforce the ACL rules*
- *use a standardized format of the authorization information*

Authorization of LB components

- *control which componentst are allowed to log events to the LB (currently, everyone with a valid certificate is allowed to store arbitrary events to the LB)*

Implementation

– *each job in LB assign an ACL and check it on each query about the job.*

– *ACL = { (cred:action:type), . . . },*
cred:

* *X.509 DN (/O=CESNET/O=Masaryk University/CN=Daniel Kouril)*
* *VOMS information (group or role membership, posession of capability)*

action:

* *Read (job status, job-log)*
* *Write allow to log events (e.g. user tags)*
* *Admin allow to change ACL itself*
* *Export (?) allow to export from the LB to another EDG service (e.g.R-GMA)*

type:

* *allow, deny*

– *Create a simple layer exporting*
bool CheckUser(cert_chain, ACL, required_action)

ACL management

- *current ACL for a job may be get as part of job status (returned by edg_wll_JobStatus())*
- *changes to ACL may be done by means of a new event; a new call to the API: ChangeACL(jobid: JobId, operation: int, ACLaction: int, ACLcred: *void),*
  - *operation – add, remove entry to/from ACL*
  - *ACLaction – read, write, admin / (allow, deny)*
  - *ACLcred – DN, VOMS information (pointer to a structure containing encoded authorization information (DN, VOMS groups, etc.)*
- *default ACL used during job registration: (<owner's subject name>: <all>)*

R–GMA

- *Add an corresponding ACL to each job propagated to R-GMA and let the R-GMA infrastucture handle them independetly.*
- *Propagate a complete ACL on each change.*
- *the ACL format should be easily readable by the R-GMA authorization routines (use e.g. GACL format).*

Component authorization

- *Utilize VOMS information for services (e.g. create VOMS group "logging")*
- *LB server would only accept events from authorized services*
- *The logging components (interlogger) run with a host proxy, generated by periodical use of grid-proxy-init*
- *replace grid-proxy-init with edg-voms-proxy-init*