OSG Security

Mine Altunay

25 September, 2009

Open Science Grid

Current Work

- Security Operations
  - Incident response,
    - ssh incident, coordinating with EGEE, building a incident sharing community, joined Ren-ISAC
  - Moving CA distribution out of VDT
    - VDT is out of CA business. GOC distributes a recommended set of CAs.
    - VDT CA distribution will slowly fade out.

Open Science Grid

Current Work

- Operational (Contd)
  - Policy work: VO AUP and VO user management templates are sent out and discussed at User's meeting
  - Training/Education: 0.25 FTE devoted to solely security education/training materials/work

Open Science Grid

Current Work

- Middleware/Infrastructure
  - Command Line Tools:
    - CA mgmt tool. A site admin tool for easily managing certs
    - refreshCAPackage | fetchCRL | setDistributionURL [--url] | add [--dir] --hash | remove --hash
    - showDistributionURL | listCA [--dir] [--pattern] | verify [--hash] | diffCAPackage | show [--certfile | --hash] | showChain [--certfile | --hash]

- CA mgmt tool
  - Interface developed with EGEE
  - OSG puts high priority
  - Work scheduled to end mid-November
- Logging and forensics work
  - Interfaced gratia records with Splunk (indexing tool for log files). Generates records from raw XML data and emails per user usage data to the users

Open Science Grid

What is Next

- Next site admin tool:
  - Banning tool: for banning user, VO, proxy
  - Job removal after banning
- RSV Monitoring for security
  - More security oriented probes. Currently only two probes.
- VDT security examination (end-end)
- Top-down OSG Registration Policy
- Keeping eye on other authN methods, shibboleth,openID