The OSG Privilege Project

HPDC Workshop – Management of Rights in Production Grids
June 19, 2006
Paris, France

Gabriele Garzoglio, Fermilab

Overview

- The Privilege Project
  - Charter, People, Architecture
- OSG Deployment
- Activities
  - Current Focus and Future Directions
- Conclusions

Project Charter

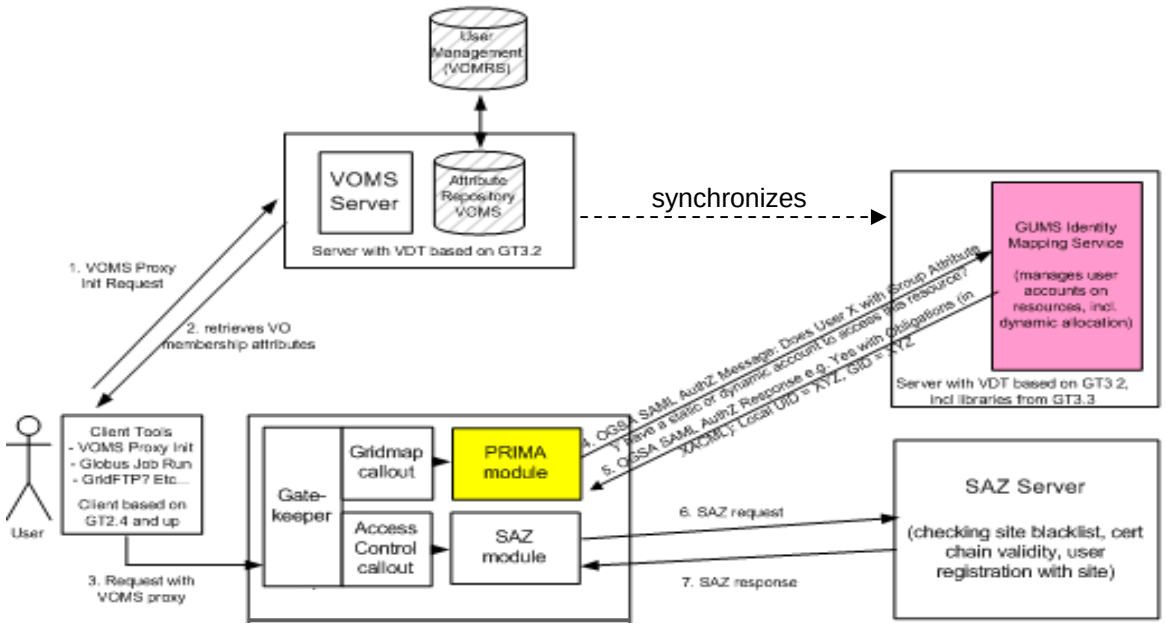
- The project provides an infrastructure to implement fine-grained authorization to access rights on computing and storage resources.
- Authorization is linked to identities and extended attributes. Mapping is dynamic and supports pool accounts. Enforcement of access rights is implemented using UID/GID pairs.
- The infrastructure aims at reducing administrative overhead. Authorization service is central at the site.
- The project is responsible for the development and maintenance of the infrastructure and for assisting with the deployment and support on the OSG.

Project Collaboration

- Stakeholders giving requirements: US CMS and US ATLAS.
- Joint Project of Fermilab, BNL, PPDG, Virginia Tech, UCSD, OSG
- Different institutions are responsible for the maintenance of different components
- Project started in 2003
- Core software distributed via VDT

Privilege Architecture

- User identity and attributes are maintained in VOMS through VOMRS
- Users interact with VOMS to get attribute-enhanced credentials
- Gateway software (**CE and SE**) performs
  - identity mapping call-out through the PRIMA module
  - access control call-out through the SAZ module
- GUMS server maintains identity / attribute mapping **for all the gateways at a site**
- gPlazma server (not shown) enhances UID/GID mapping with service-specific parameters (e.g. root path for SE).
- SAZ checks black lists / CRL
- Periodically, GUMS synchronizes with VOMS users/groups



Deployment on OSG

- The authorization system (GUMS) has been deployed at O(10) sites
  - all US CMS T2 centers and T1 at FNAL
  - US ATLAS T2 centers and T1 at BNL
  - FermiGrid (includes SAZ) et al.
- US CMS and US ATLAS have defined roles that are implemented within VOMS. Sites configure GUMS (PDP) to implement local identity mapping
- VOMS extended proxy is parsed by the callout and given to GUMS for authentication

Current activities 1

- Maintenance of call-out modules for GT2 / GT4 on 32bit / 64bit platforms
  - Stress test of GT4 call out
  - So far light operations: maintenance at 2 “easy” tickets / month
- Integration / Deployment of dCache / gPlazma for CMS T1 & T2
- Improve robustness of the infrastructure
  - Memory management, configuration management, reliability/redundancy

Current activities 2

- Implement health monitoring for key components
- Improve software validation processes
- Integrate new software with privilege PDP
  - gLexec SAML call-out to GUMS / SAZ (“pilot-style” job management)
  - Condor-C

Future Directions

- **Publication of role-based privilege policies: can we collaborate on this ?**
- Simplify / Aggregate architecture
  - Streamline gPlazma infrastructure (direct connection to GUMS)
  - Reorganization of PDP services (GUMS talking to SAZ)
  - Update communication protocols (from extended SAML v1.1 to SAML v2.0)
  - Improve PRIMA build process
- Extend privilege enforcing to network management
- Long term directions
  - Investigate direct DN rights enforcement (no UID mapping)
  - Integrate Privilege Project with Policy Discovery Services
  - Extend privilege enforcing to include privacy
  - Executable integrity

Conclusions

- The privilege infrastructure provides role-based fine-grained authorization for access to grid-enabled resources.
- It is used on the OSG by US CMS, US ATLAS, et al.
- Current focus:
  - pushing the deployment of the SE authorization infrastructure
  - improve operations by improving robustness, usability, and validation processes
  - integrate new software with the privilege infrastructure