The Privilege Project and the LIGO Data Grid

Gabriele Garzoglio, Fermilab

Overview

- The Privilege Project
  - Charter, People, Architecture
- OSG Deployment
- Ideas Related to the LDG
- Conclusions

Project Charter

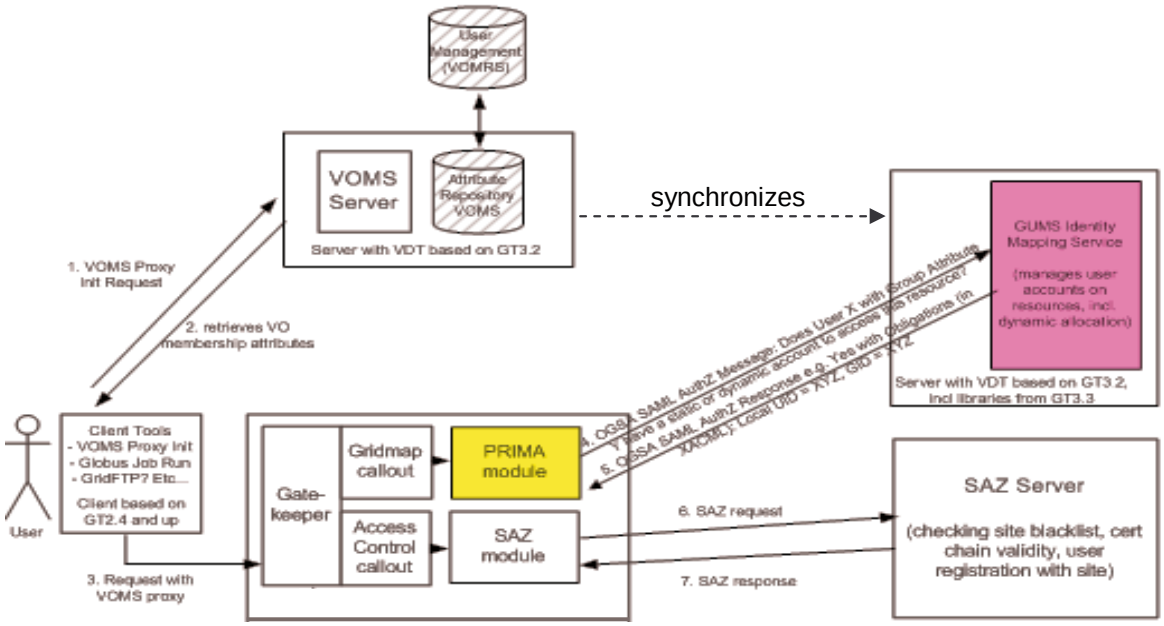
- The project provides an infrastructure to implement fine-grained authorization to access rights on computing and storage resources.
- Authorization is linked to identities and extended attributes. Mapping is dynamic and supports pool accounts. Enforcement of access rights is implemented using UID/GID 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

Ideas for the LGD I

1. There has recently been a move toward service certificates […] so that a set of users can share the load of "managing" runaway jobs and so that some jobs can be given higher priorities in the Condor queue without giving any single user a higher priority [Warren, May 31]

- Using the Privilege infrastructure, this problem can be addressed using Roles:
  - A set of users are registered in VOMS with the “production” role
  - Sites map users from this role to a special UID, with high priority in condor, access to the file sys., etc.
  - Better solution than using a service certificate because sites can still account for the user that submitted the job

Ideas for the LGD II

2. User certificates should be tightly coupled to user accounts. […] Eventually, the LIGO Computing Committee wants the signing of a certificate to automatically invoke a process which creates an LDG user account across the LIGO data grid associated with that certificate. [Warren, May 31]

- The Privilege infrastructure, supports this use case:
  - Certificates can be mapped to specific local UID through GUMS
  - If UID's are created automatically, the GUMS database can be updated as part of the process
  - This mapping can co-exist with role-based mappings

Ideas for the LGD III

3. Quick turn around on certificate revocation. […] We also want to be able to lock out users who leave the collaboration on short (< day) time scales. If accounts are tied closely to certificates, and activated automatically with certificate signing, it is natural to use certificate revocation to close access to accounts as well. [Warren, May 31]

- The Privilege infrastructure may provide an alternative solution to certificate revocation:
  - SAZ implements a certificate black-list
  - SAZ has been deployed at Fermilab for site-level black-listing
  - Would this be a Grid-level use of SAZ for LDG?
  - This way, a former LIGO collaborator can keep using his/her certificate if needed, but not be authorized to run on LDG

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.
- Some of the LDG requirements seems to be addressed by the Privilege Infrastructure.