Open Science Grid

The VO Services Project

Overview

- Charter & Stakeholders
- Architecture
- Deployment
- Performance
- Collaboration & Recent Focus

Don Petravick for Gabriele Garzoglio
Computing Division, Fermilab

ISGC 2007

Open Science Grid

Project Charter

- The project provides an infrastructure to manage user registration and 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.

Open Science Grid

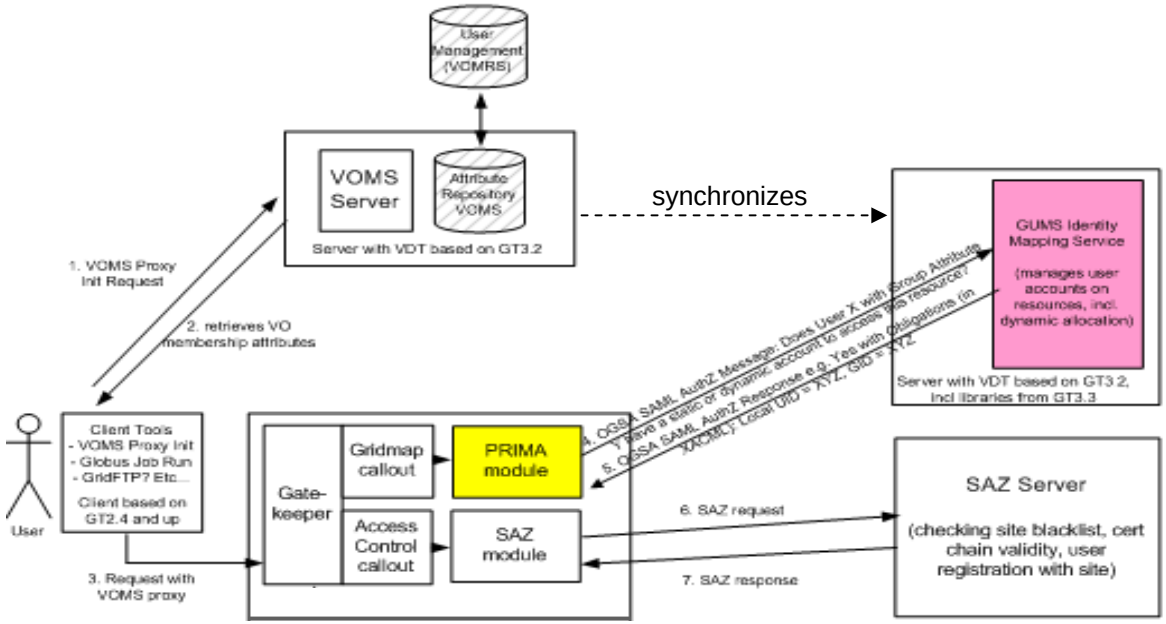
Stakeholders

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

Open Science Grid

VO Services 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/white lists
- Periodically, GUMS synchronizes with VOMS users/groups



Open Science Grid

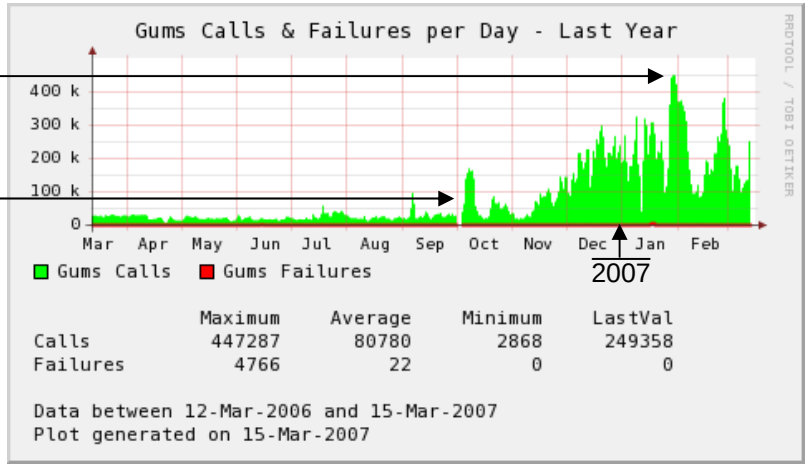
Deployment

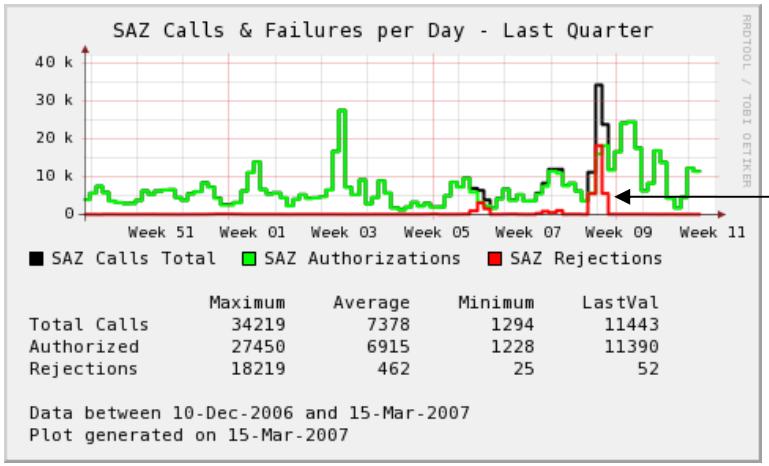
- The authorization system (GUMS) has been deployed at O(10) OSG sites
  - US CMS T2 centers and T1 at FNAL
  - US ATLAS T2 centers and T1 at BNL
  - FermiGrid (includes SAZ) et al.
- VOMRS deployed at
  - Fermilab: 14 VO with > 5,000 users
  - CERN: 9 VO with >2,500 users
  - BNL: 2 VO
  - Evaluations: 2 VO @ TTU & 2 VO @ U. of Melbourne

GUMS & SAZ at FermiGrid

GUMS scales well to ~480,000 calls/day (20k calls / hours).

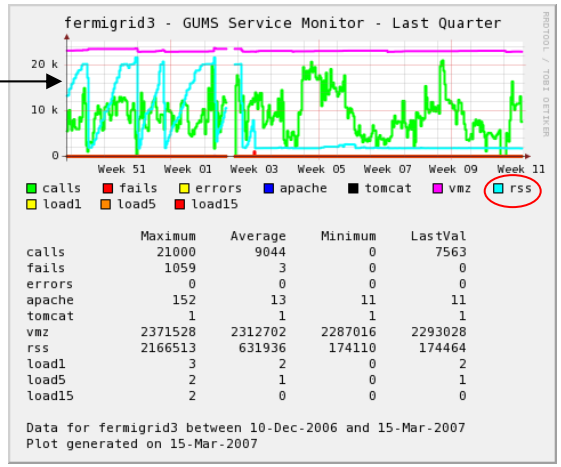
Turn ON SE call-out (gPlazma).
SE callout > 80% Total callout.





Fixed GUMS memory leak

Access denied to non-VOMS proxy.



Open Science Grid

Collaboration with Globus and EGEE

- Current AuthZ call-out library (PRIMA) is based on SAML v1.1 + XACML extensions
  - Standardization was tough to achieve.
- Now working with Globus and EGEE to introduce a common/standard AuthZ call-out library for PRIMA/GUMS/SAZ (OSG) & LCAS/LCMAPS (EGEE).
- Globus AuthZ library is based on SAML2 / XACML2.
- Planned integration with Globus: Apr 2007. OSG and EGEE AuthZ services thereafter.

Open Science Grid

Recent Focus

- Improve operations by improving
  - robustness: configuration management
  - usability: user interface
  - validation processes across components
- Helping LIGO with AuthN/Z requirement for the OSG
- Supporting site security for late-binding job using gLexec
- Working with SE groups to refine mapping policies

Open Science Grid

Conclusions

- The privilege infrastructure provides user registration and role-based fine-grained authorization for access to grid-enabled resources.
- GUMS is deployed on the OSG by US CMS, US ATLAS, et al.
- VOMRS is deployed at FNAL, BNL, CERN for 25+ VOs
- We promote the adoption of standards for AuthZ Services