Open Science Grid

VO Services Project
Status and Plans

Mar 2, 2007
Middleware Security Group Meeting

Gabriele Garzoglio
Computing Division, Fermilab

Open Science Grid

Overview

- VO Services Project
  - Charter
  - Stakeholders
  - Architecture
  - Deployment
- WBS
- Conclusions

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.

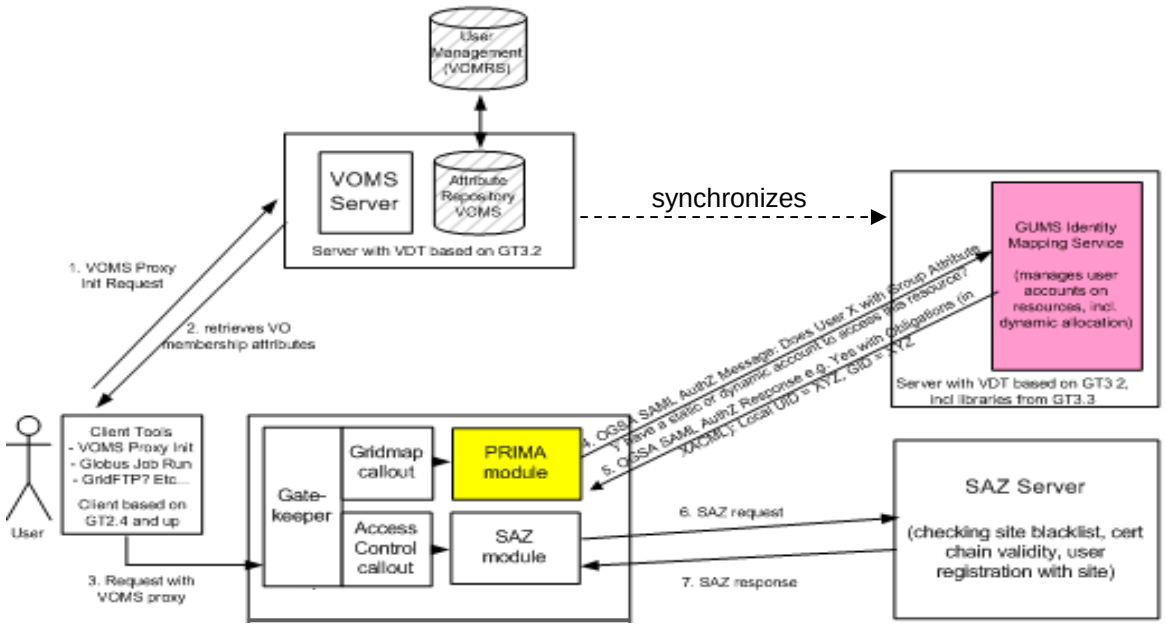
Open Science Grid

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

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 on OSG

- The authorization system (GUMS) has been deployed at O(10) sites
  - US CMS T2 centers and T1 at FNAL
  - US ATLAS T2 centers and T1 at BNL
  - FermiGrid (includes SAZ) et al.
- US CMS, US ATLAS, and DZero have defined roles that are implemented using VOMS. Sites configure GUMS (PDP) to implement local identity mapping

Open Science Grid

WBS

- The WBS was put together in late spring
- Requirements come from the stakeholders, including CMS, Fermilab, CERN
- WBS reflects work on
  - Internal components (PRIMA, GUMS)
  - Related components (gPlazma, gLexec)
  - Recent additions (VOMRS as of Sep 06)
- SAZ is logically part of VO Services, but is managed by Fermigrid

Open Science Grid

WBS - 1

1. Support and deployment
   (Ongoing ~25% FTE internal support)
   (Support need will grow with deployment)
   1. Support the PRIMA and GUMS code for 32/64 bits for GT2 and GT4 for CMS Tier 1&2. Provide best effort support for all OSG VOs. (In the past 10% effort)
   2. Support “stable” VOMRS release for Fermilab, CERN, and OSG stakeholders Ongoing. (In the past: 15% Tanya , 10% external (CERN) support)
   3. Help deploy the infrastructure to stakeholders’ sites. Ongoing (TBD)

Open Science Grid

WBS - 2

2. Improve health status reporting for key servers (Started. Remaining effort TBD)
   1. Better Gatekeeper / Prima error reporting for authorization failures (effort TBD)
   2. VOMS/GUMS health monitors (Done Aug 06)
3. Improve software validation (8 FTE weeks) (Started)
   1. Improve validation of basic functionalities (framework available in VDT)
   2. Implement validation of software dependencies
   3. Measure PRIMA / GUMS scalability (Started by John W.)
4. Improve integration of the infrastructure with dependent components as needed (Done)
   1. Improve GUMS integration with MonALISA (Done)

Open Science Grid

WBS - 3

5. Improve robustness of GUMS (Started)
   1. Fix GUMS memory management problems (3 FTE weeks) (Done at FNAL Sep 06)
   2. Improve GUMS configuration management (3 FTE weeks) (Started in Oct @ BNL)
   3. Investigate redundant servers configuration (2 FTE weeks – was 3 FTE days) (Started)
6. Improve GUMS usability (Started)
   1. Improve pool account management (1 FTE week) (Started in Oct @ FNAL: planned for GUMS v1.2)
   2. Implement history log querying interface (2 FTE week) (Not started: planned for GUM v2.0)
   3. Add web interfaces for administrative commands (Done Jan 07)

Open Science Grid

WBS - 4

7. gPlazma integration with DCache and deployment (EXTERNAL) (Started)
   1. Integrate gPlazma-enabled authorization classes with DCache doors (Done Aug)
   2. Validate DCache / gPlazma integration (Done Sep 06)
   3. Deploy gPlazma-enabled DCache (Started Sep 06 at Tier 1- externally managed)
   4. Enhance gPlazma for EGEE deployment (ext. managed)
8. Integration of gLexec with PDP (8 FTE week: Done Oct 06)

Open Science Grid

WBS - 5

9. VOMRS: implementation of “vital” features for stakeholders (Generic Attriubutes by Mar)
10. Define roadmap for long-term future (Ongoing)
    1. Interact with Globus (Security model, XACML PRIMA-equivalent, CAS, etc.) (Started)
    2. VOMRS long-term future (Ongoing)
11. Outreach (Ongoing)
    1. Understanding Requirements from new VOs and groups (e.g. LIGO)

Open Science Grid

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.
- Our current focus is to improve operations by improving robustness, usability, and validation processes
- Challenges include reliability of effort available, interactions with external groups, and defining the roadmap for the future.

Extra Slides

Open Science Grid

Effort

Name	Expertise	Recent Effort	Projected Effort
Gabriele Garzoglio	PL (Apr 06)	30%	30%
Igor Sfiligoi **	gLexec, PRIMA, GUMS	50%	50%
Vikram Andem	PRIMA	50%	0%
Tanya Levshina *	VOMRS, Roadmap	50%	50%
Valery Sergeev * (Fermigrid)	VOMRS support	0%	10%
John Hover (BNL)	GUMS	(20%)	20%
Jay Packard (BNL)	GUMS	(20%)	50%
Ted Hesselroth (dCache) ***	gPlazma	50%	0%
John Weigand (CMS)	Testing VDT	50%	(??) 0%
•VOMRS part of VO Services Since Sep 06	** Joined in Sep 06 *** gPlazma external in FY07	**320%**	**220%**