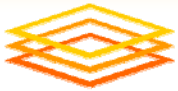


VOMRS/VOMS-Admin Convergence and VO Services Project Status

Tanya Levshina
Computing Division, Fermilab

Outlines

- VOMRS
  - Purpose
  - Scope
  - Deployment
  - Convergence with VOMS-Admin
  - Place in Grid World
- VO Services:
  - Gums
  - gPlazma
  - SAZ
  - Authorization Interoperability
  - SVOPME Project
- Conclusion

Virtual Organization Management Registration Service (VOMRS)

- VOMRS was developed to address the end-to-end needs for VO membership registration and groupings of common interest within the Fermilab and WLCG contexts.
- Initiated on 1/24/03, first production release - 3/1/2004.
- Some of the collected requirements were incorporated into Joint Security Policy Group (JSPG) VO Membership Management Policy document.
- The implementation is in compliance with JSPG requirements.

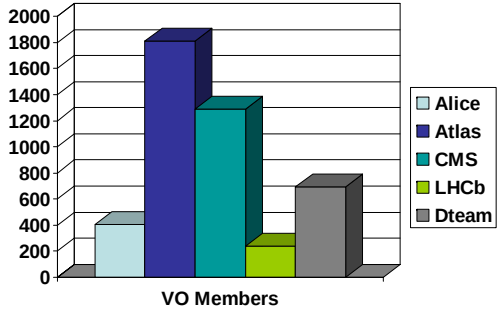
VOMRS Scope

VOMRS offers a comprehensive set of services that facilitates secure and authenticated management of VO membership, grid resource authorization and privileges:

- implements a registration workflow
- supports management of multiple grid certificates per member
- permits VO-level control of member's privileges
- provides email notifications of selected events
- supports VO-level control over its trusted set of Certificate Authorities
- permits delegation of responsibilities within the various VO administrators:
  - VO Admin
  - Representative
  - Group Owner/Group Manager
- manages groups and group roles
  - Group/group role definition
  - Group/group role access
  - Group role are linked to a specific group
  - Group/group role assignment request
- is capable of interfacing to third-party systems
  - CERN and Fermilab HR databases
  - DZero SAM
  - VOMS

VOMRS Deployment

- VOMRS is a part of VDT
- Multiple production installations:
  - Fermilab:
    - 11 instances. Total number of registered users > 5,000
  - CERN:
    - 11 instances. Total number of registered users >4,000



  - Also installed at
    - BNL
    - Texas Tech University
    - APAC - University of Melbourne
    - Desy
    - Forschungszentrum Jülich

VOMRS and VOMS-Admin Convergence (I)

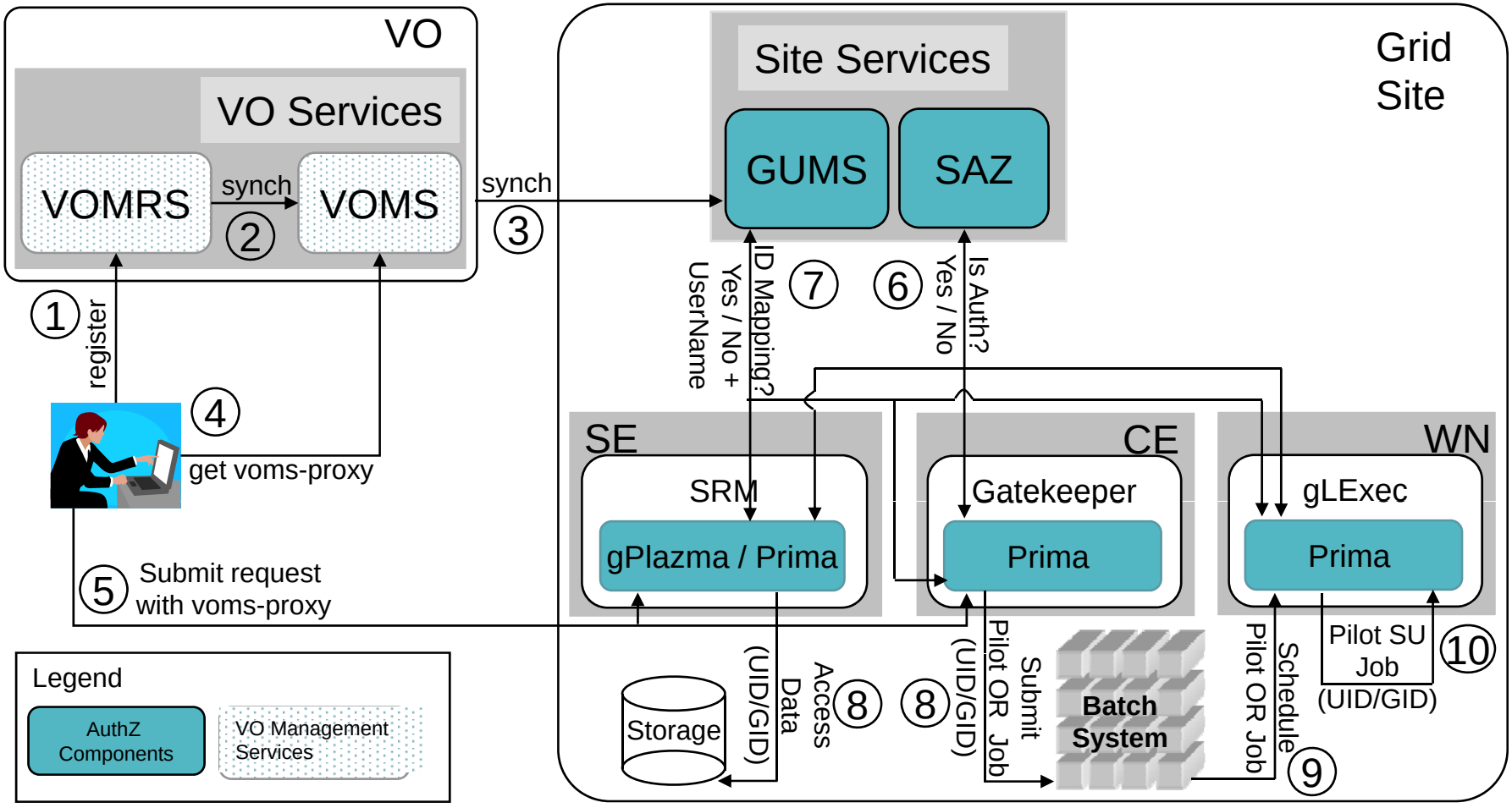
- VOMS-Admin is emerging:
  - 2.5 version will have a lot of new features.
  - This raises the possibility of rationalizing the support and converging on a single solution by continuing and extending our current collaboration.
- There are several crucial features that should be implemented in VOMS-Admin in order to do so:
  - Persistent member's status
  - Member's institutional expiration
  - Enhance handling of groups and group roles:
    - Group and group role definitions
    - Opened/Restricted access
    - Possibility to attached a particular role to a specified group

continued on the next slide …

VOMRS and VOMS-Admin Convergence (II)

- List of required features：
  - Interfacing third-party services during registration and membership validation
  - Dynamic list of collected personal information
  - Registration workflow and event notification
  - Web UI improvements
    - Online help
    - Sortable, selectable output
    - Ability to execute actions for multiple users simultaneously
- Required effort estimated by VOMS-Admin developers is about 8-10 FTE months + 2 months for customer feedback and deep testing
- This effort is coordinated by LCG VO Registration Task Force

VO Services Architecture



VO Services Project

- VO Services project provides user registration to VO and fine-grain access authorization to resources.
  - Gabriele Garzoglio (Fermilab) is project leader.
- VOMRS forms part of a set of VO services implemented in accordance to the OSG blueprint and targeted to meet the needs of the OSG:
  - Certificate to User Account Mapping (GUMS)
  - Authorization for Storage and Compute Services (gPlazma, glExec)
  - Site Banning Tool (SAZ)
- Working with Globus, EGEE/gLite and INFN to provide interoperability and consolidate the implementations in the future (Authorization Interoperability Project)
- Participating in the SVOPME project that provided the prototype tools for automating the process of managing role-based privileges over the Grid, from VOs to Grid sites
- Adapting VO services to new use cases (e.g. LIGO, Shibboleth based identity management).

GUMS

GUMS (Grid User Management System) maps users' grid credentials to site-specific identities in accordance with the site's grid resource usage policy

- Replaces the Globus grid-mapfile.
- Retrieves membership information from a VO server such as LDAP or VOMS.
- Currently the focus is on operational properties of the tools, such as monitoring, status/availability checks, validity of the authz configuration at a site, etc.

gPlazma

gPlazma (Grid-aware PLuggable AuthoriZation MAnagement) provides the authorization decision and site-specific user information relevant to user's credential when requested by storage cells (gridFtpdoor, SRM)

- Retrieves username from GUMS by providing user's DN and FQAN.
- Retrieves storage-privilege set {uid,gid, permitted storage area, r/w permissions} form Storage Meta Data Service.
- Returns a User Authorization Record (a SAML response format) to gPlazma.

SAZ

SAZ (Site Authorization Service) allows security authorities of the grid site to impose sitewide policy and to control access to the site.

- Allows administrators to control user access to the site resources.
- Provides means to retrieve the information about users and their access.
- Authorizes user by checking
  - user's certificate chain
  - status of VO FQAN provided in extended certificate
  - user's access status

OSG is interested in this technology to implement a Grid-wide banning tool.

Authorization Interoperability Activity

- Started in Oct 2006 as a collaborative effort between the OSG VO Services Project, EGEE, Globus and Condor (joined later)
- Goal: To provide interoperability between middleware and authorization infrastructures.
- The common protocol is used by resource getaways, or Policy Enforcement Points (PEP) to interact with Policy Decision Points (PDP)
- For each access request, the PDP informs the PEP on whether access is granted or denied and, what obligations need to be enforced if access if granted.
- Obligations are used as a mechanism to restrict privileges at Grid resources.
- The final design document: “An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids”

  http://cd-docdb.fnal.gov/cgi-bin/ShowDocument?docid=2685

SVOPME Project

- SVOPME – A Scalable Virtual Organization Privileges Management Environment.
  - Joint Project : Tech-X Corporation and Fermilab financed by Small Business Innovation Research
  - Phase I is completed in March 2008
- Goal to develop tools and services for automating the process of managing role-based privileges over the Grid, from VOs to Grid sites.
- Prototype tools were developed to facilitate the automatic propagation of privilege data
  - VO Policy Editor – generates VO policies and verification queries
  - VO/Grid Policies Comparer - produces a report on which VO policies are honored by the Grid site and which are not
  - VO/Grid Policies Advisor - advises the Grid administrator on what amendments needs to be performed on the Grid; such that the Grid site complies with the VO policies
- XML schema for specifying role-based privilege policies was defined and used to assist documenting and converting policies among VOs and Grid sites.
- Proof of concept: Use standard policy languages (XACML) to express site and VO policies for our use cases.

Summary

- VOMRS and VOMS were developed to address the end-to-end needs for VO membership registration and groupings of common interest within the WLCG and Fermilab contexts.
- Fermilab is committed to the support and maintenance of VOMRS in the short and longer term.
- The recent development of new features in VOMS-Admin raises the possibility of rationalizing the support and converging on a single solution by continuing and extending our current collaborations.
- VO Services Project is constantly evolving and adapting for new use cases.