Virtual Organization Management Service Extension Project Definition

Draft

Purpose:

To facilitate the remote participation of US based physicists in effective and timely analysis of data from the LHC experiments by designing, developing, and deploying Virtual Organization management service eXtension (VOX) for US CMS

Objectives:

- Provide VO-wide reliable and easy to use registration service.
- Provide centralized storage to hold and query information (including site required identity info) about members and their authorizations.
- Collaborate with various Grid projects: iVDGL, European Data Grid and others in order to develop working relationship and converge on unified technical solution that will allow to support a true worldwide VO.
- Support application execution using Grid security infrastructure use of multiple sites, including Fermilab and other Tier-0, 1, 2, 3 institutions.

Stakeholders:

We can identify the following groups of people and organizations that have interest in the project process, outputs and outcomes

- Physicists from CMS collaboration who need to work effectively "at a distance" from CERN.
- VO administrators who need to support the physicists with timely and effective means.
- Local sites administrators responsible for register new employees and visiting scientists who need to keep track of all "remote" VO members that are using local sites
- Local grid resources administrators that need to guarantee secure access to their systems and protect against unauthorized use.
- Local site security authority that needs to guarantee that the systems at a site conform to some pre-established standard of computer security.

Introduction:

This project intends to integrate a number of components into a complete VOX. It is an extension of (and includes) the EDG VOMS effort and includes developing protocols for user, resource and site registration. It is expected that this development will proceed in close collaboration with the EDG VOMS efforts and communications are already established.

The enforcement of policy is expected to use the Globus gatekeeper callout (once available) and is currently being prototyped with the EDG LCAS code. It is expected that Globus, EDG and this effort will work toward a standard protocol and interoperable implementation(s) of the policy enforcement mechanisms. This project will implement a Site AuthoriZation service (SAZ) for FNAL as an example of a site policy enforcement mechanism.
Finally, this project will explore the issues (technical and policy management) involved in a hierarchy of VOs.

Components:

We believe that the task of creating Virtual Organization within the Grid can be divided into several autonomous yet inter-related components, namely:

1. Job Broker Service that schedules the VO member job to run on a particular grid cluster
2. Virtual Organization Service that provides user registration with VO and grid resources
3. Local Center Registration Service that provides VO member registration with local site
4. Local Resource Administration Service that provides mapping between VO member/roles/groups and local user account and creates this account
5. Site Authorization Service (SAZ) that keeps track of potential users that are allowed or banned from using site's resources.

We assume that component (1) is out of scope of the VOX project; however suitable interfaces must be maintained and documented that allow an exchange of authorization information between the VO supporting components and the actual schedulers and resource brokers that decide where jobs are executed. Component (2) is expected to be standard component. Components (3) and (4) are expected to be standard protocols with site-specific implementation as needed. Component (5) is expected to be a FNAL specific implementation using standard callout interface. In the course of the project we will either develop missing components or integrate existing components into our system.

Virtual Organization Service:

Virtual Organization Service will provide means to register user with VO, verify his/her credential, assign groups and roles, acquire confirmation from sponsor that user is approved as a member of VO.

VO Service will consists of the following parts:

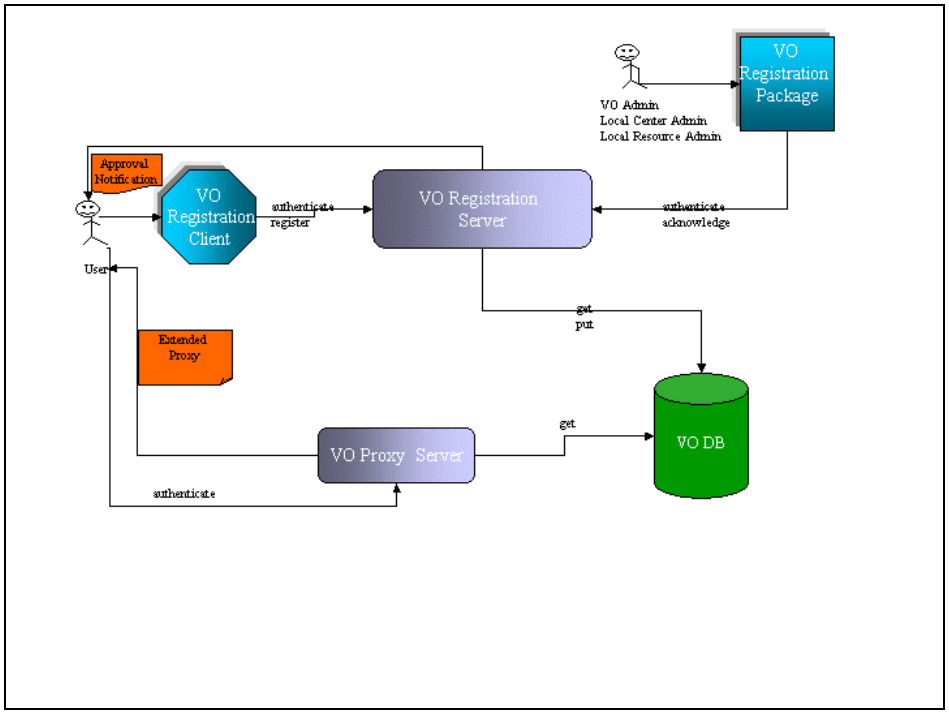
- VO Registration Client: provides GUI/Web Interface for users to apply for VO membership, modifies user information, performs limited queries.
- VO Registration Server: accepts user registration, assigns roles and groups to the user, identifies user to the local sites, allows to store/query user information.
- VO Proxy Server: authenticates user, generates user extended proxy that is valid for job submission (accepted by Gatekeeper). We are aware about at least one existing implementation of such server (EDG VOMS).
- VO DB: store information about users and sites.
- VO Registration API: allows obtaining /modifying specific information in VO DB.

Assumptions:

1. It is expected that experiment will have multiple VO Service instances (e.g. VO US CMS, VO CERN CMS) that can communicate with each other using predefined protocol. Each of VO Service instance has its own VO Proxy Server and database. VO databases are not necessarily identical.
2. VO Registration Server should be able to handle multiple simultaneous requests.
3. VO Registration Server should be able to notify Local Center Registration Service operated on each site about new potential user
4. VO Registration Server should be able to notify Local Resource Admin Service potentially operated on each grid cluster about new potential user that has been approved to use local site
5. Each VO Service has its own database. The database contains the following data:
   - Sites information
     - List of the available sites
     - Superset of requested user info for all sites
     - Sites policies

        - Sites resources (?)
        - Sites administrators and contact info
        - Sites callback actions
        - Local Resource Admin Servers locations if applicable
    - Experiment related information:
        - List of trusted spokespersons, their groups and contact information
        - List of available groups provided by spokespersons
        - List of available roles provided by spokespersons
    - User information:
        - Personal information
        - List of sites that user can potentially submits jobs
        - List of selected roles/groups
        - List of sites that allow user to submit jobs
6. VO Proxy Server should be able to handle multiple requests simultaneously
7. VO Proxy Server should be scalable (VO Proxy Server response time should be reasonably quick)
8. VO Registration Client
    - GUI/CLI/Web Interface should be provided
    - User should be able to perform the following actions via VO Registration Clients:
        - Provide subset of required personal information
        - Identify information that should not be shared with other VO Services
        - Select groups/roles
        - Perform limited queries
        - Modify provided information
    - Administrator should be able to perform the following actions via VO Registration Clients:
        - Add/Modify site/experiment/user information
        - Query VO database, create reports
9. VO API will be used by
    - VO Registration Client
    - VO Administrate to populate VO database
    - Local Center Administrates and Local Resource administrators to acknowledge user inclusion to the local site.

Figure 1: VO Service Architecture



Local Center:

Assumptions:

We assume that Local Centers have the following features or provide services:

1. Provides grid resources.
2. Can host multiple unrelated VOs (VO US CMS, VO SDSS)
3. Cooperates VO administrate.
4. Has full control on local resources allocation
5. Has full control on local resources usage

Local Center Registration Service:

Local Center Registration Service provides means to register VO member with the local site and get sufficient credential to access this site directly.

Assumption:

1. Development of such Service is out of scope of the VOX Project. We assume that this service already exists in some form.
2. Local registration administrate uses VO pre-defined protocol that allows VO Registration Service to notify it when a new user requested access to the local site.
3. Local registration administrate uses VO Registration package that allows it to notify VO Registration Server about approval/rejection of user access.

Local Resource Administration Service:

Local Resource Administration Service associates VO member with the local account based on the user group and role, creates local account(s) on the appropriate grid cluster(s), notifies VO Registration Server that local site is ready for user to submit jobs. This service allows local resource administrators to manage fine grain access control to local resources.

The local resource administrators have to define how to detect new potential VO members who want to use local resources and how to map him to the local accounts. VO project will provide VO registration package, so local resource administrators can notify VO Registration Server when user account has been created.

This project will provide Local Resource Administration Service package. It is up to local administration to install/use it.

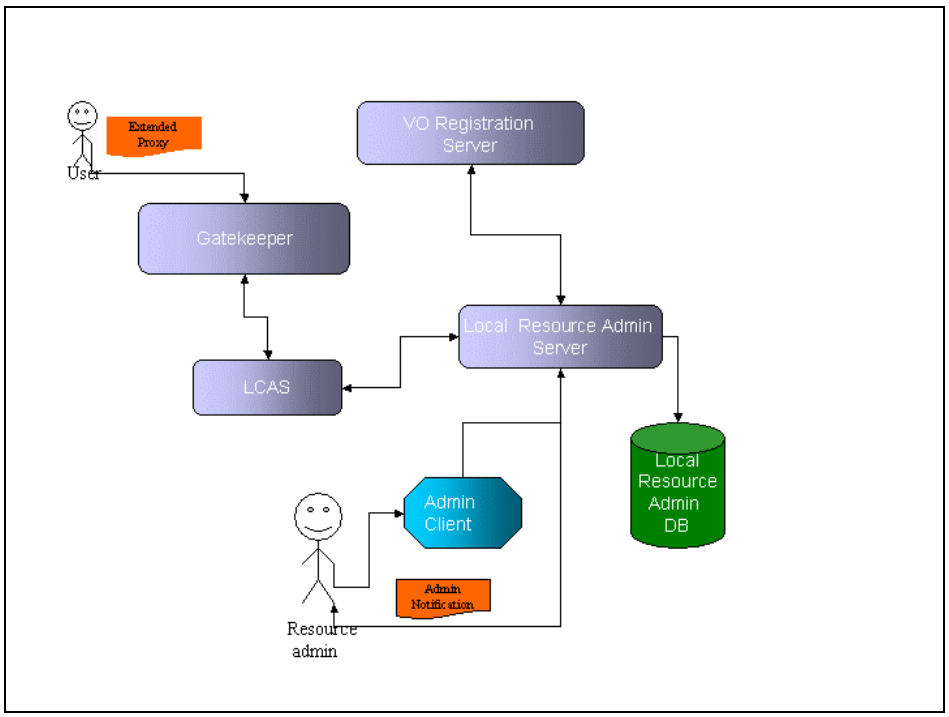
Assumptions:

1. It will be at least one Local Resource Admin Service per VO on each site (could be one per grid cluster)
2. VO Registration Server will notify Local Resource Admin Service when the registered user get approval to submit jobs from Local Center Registration Service
3. Local Resource Admin Service consists of the following parts:
   - Local Resource Admin Server: communicates with VO, handles modification/query of the local database, notify sys admin about new users
   - Local Resource Admin Client: GUI/CLI for system administrator to query/modify local database
   - Local Resource Database contains the following data:
     - User
     - Roles
     - Groups
     - Local accounts
     - Local grid cluster

- Denied/Allowed access
- Timeslots of allowed access

LCAS will query database in to get user account and access information

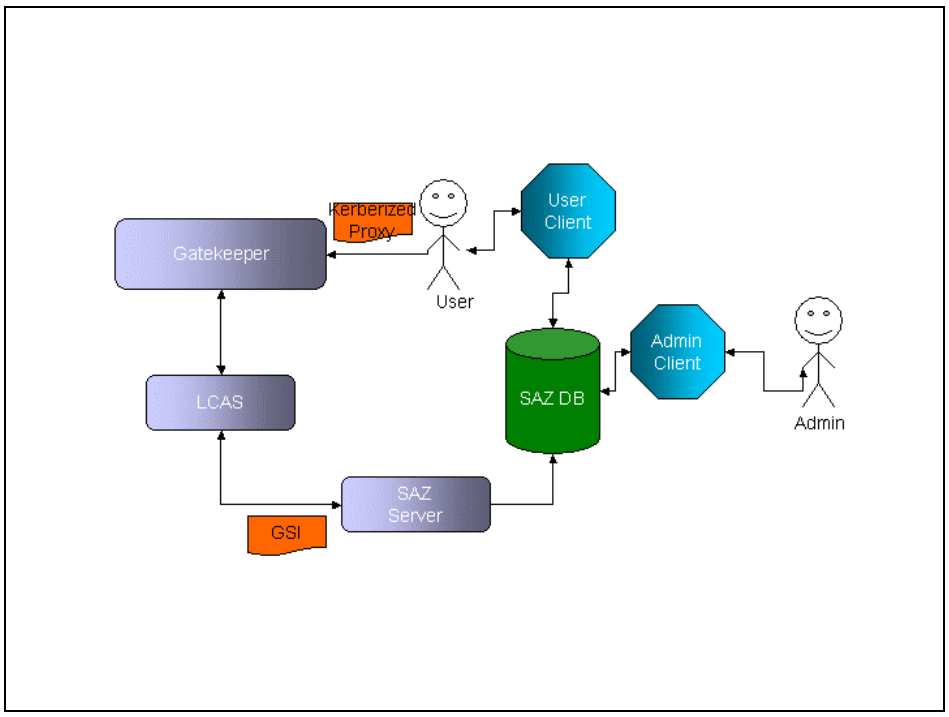
Figure 2: Local Resource Admin Service Architecture



Site authentication and authorization service

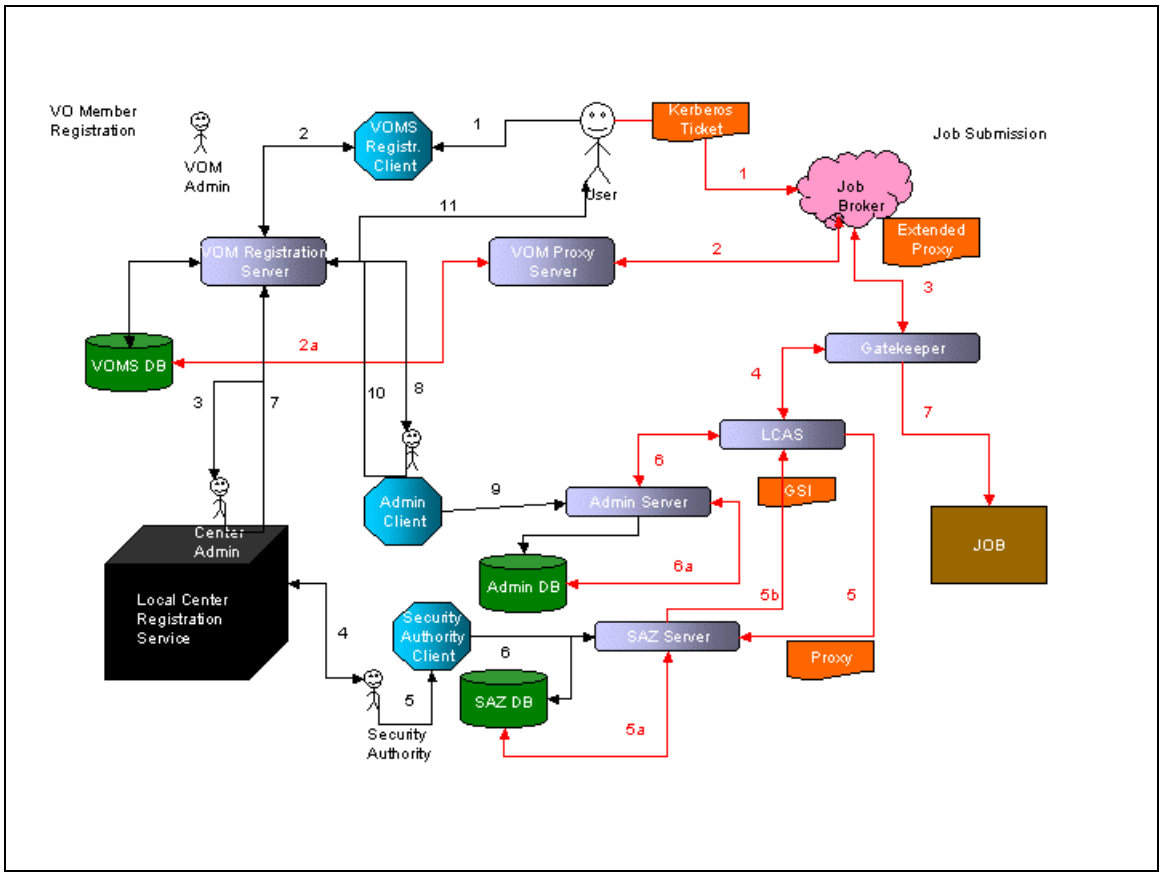
SAZ allows local security authority to ban or allow the access to the site to particular users. SAZ prototype is implemented at Fermilab as a Globus-authenticated grid service. Communication between LCAS and SAZ has not been implemented in prototype.

Figure 3: SAZ Architecture



Interaction between VOX Components:

Figure 4: VOX Project overall design



Used Cases:

New VO member successful/failed registration (black arrows on figure 4):

1. User submits personal & experiment related information via VO Registration Client
   User failed to provide minimum information
2. Information propagates to VO DB via VO Registration Server
3. VO Registration Server notifies Local Center Registration Service about potential user using provided protocol.
   All Local Center Registration Services deny user application
4. Local Center Administrator notifies Local Security Authorities about new user

All Local Security Authorities deny user access

5. – 6. Local Security Authority adds new user to SAZ D, allows user access to the site and notifies Local Center Administrator that user is accepted
7. Local Center Administrator notifies VO Registration Server that user is accepted
8. – 9. Local resource admin add new user/groups/roles in local Admin DB, maps this user to local account and creates the account on grid clusters.
10. Local sys admin notifies VO Registration Server that user can submit job to local grid clusters
11. VO Registration Server notifies user that he is VO member

Successful/failed job submission (red arrow on figure 4):

1. User obtains certificate and submit job to Job Broker
   User has invalid certificate
2. Job Broker talks to VO Proxy Server and receives the list of sites user can submit job and extended proxy for user job. Proxy contains user DN, role, group
   List of sites is empty – user is not a member of VO or doesn't have approval from Local Center
3. Job Broker finds appropriate Gatekeeper and forwards user job
4. , 5. Gatekeeper verifies (via LCAS and SAZ server) that user is not banned from the site
   User is banned to access any sites
5. , 6. Gatekeeper verifies (via LCAS and Admin server) that user has an account and is allowed by sys admin to run during this time slot
   User doesn't have appropriate local account or time slot on any of the grid clusters
7. Gatekeeper starts job

User is banned to access the site:

1. User access standing has changed in SAZ DB (form "allowed" to "banned")
2. The following information has changed in Local Resource Admin DB
   a. User access standing from "allowed" to "banned"
   b. Current time is out of time slots when user is allowed to run
   c. Allowed group/role list
3. The following information has been changed in VO DB:
   a. User is not VO member
   b. New personal information were requested from the local center