FermiGrid - Site AuthoriZation (SAZ) Service

Keith Chadwick, Neha Sharma, Steven C. Timm, D. R. Yocum

The Grid Resource Authorization Problem:

Grid resource administrators need the ability to control access to the resources by internal and external users:

- Black-list (or ban) during the investigation of a potential compromise, or in the actual compromise of credentials, virtual organizations or certificate authorities.
- White-list to assure that certain users are guaranteed access to the resource.

The above access decisions need to be based on:

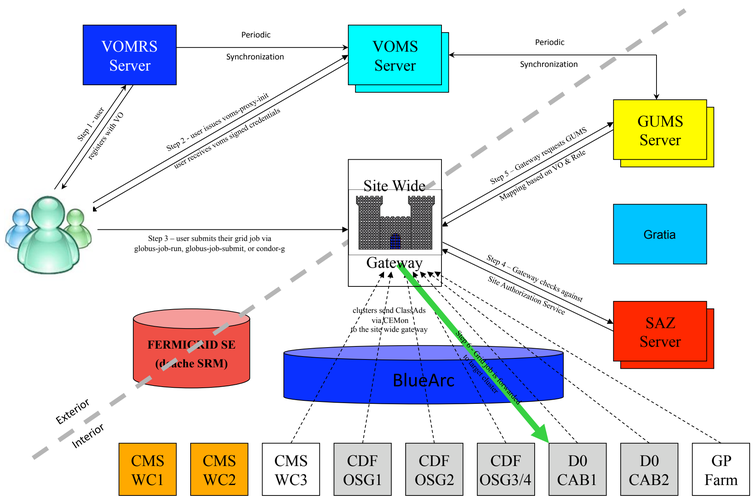
- Distinguished Name (DN),
- Virtual Organization (VO),
- Fully Qualified Attribute Name (FQAN = VO + Group and/or Role),
- Certificate Authority (CA).

Additional Requirements:

- Implement via standard Globus interfaces.
- Support fast response in the event of an incident.
- Ability to respond high number of authorization queries.
- Easy administration of the blacklist and easily restore access.
- Support the propagation of banning information.
- Verification/auditing of desired authorization policy.
- Staged deployment of banning tools and services.

FermiGrid - Current Architecture:

Fermilab supports a scientific program that includes experiments and scientists located across the globe. To better serve this community, Fermilab has placed its production computer resources in a Campus Grid infrastructure called 'FermiGrid'. The architecture of FermiGrid facilitates seamless interoperation of the multiple heterogeneous Fermilab resources with the resources of the other regional, national and international Grids.



Description of the Site AuthoriZation Service:

The Site AuthoriZation Service consists of the following components:

- The SAZ server with backend MySQL database.
- The SAZ client for Globus Gatekeepers.
- The interactive sazclient (used by gLExec within pilot jobs).
- The SAZ gPlazma plugin.
- The SAZ command line administration script.
- The SAZ web administration interface (under development)

The SAZ client for Globus Gatekeepers is configured through the globus_authorization entry in the configuration file /etc/grid-security/gsi-authz.conf

```
globus_authorization /usr/local/vdt-1.8.1/sazclient-1.2/lib/libSAZ-gt3.2_gcc32dbg globus_saz_access_control_callout
globus_mapping /usr/local/vdt-1.8.1/prima/lib/libprima_authz_module_gcc32dbg globus_gridmap_callout
```

The host name, port number and DN of the SAZ server that the SAZ client contacts are configured in:

```
/etc/grid-security/sazc.conf
```

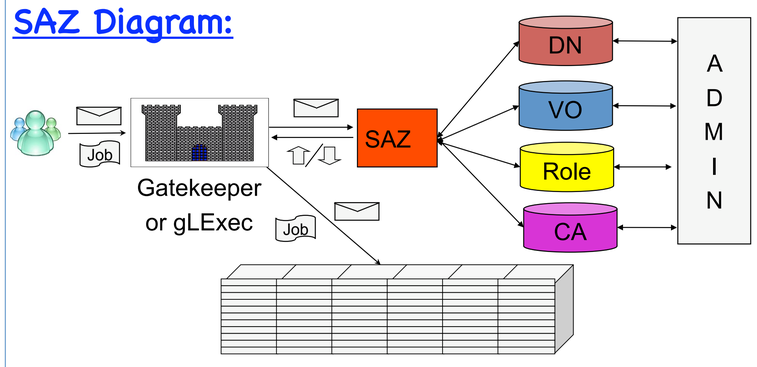
The typical contents of /etc/grid-security/sazc.conf are:

```
SAZ_SERVER_HOST saz.fnal.gov
SAZ_SERVER_PORT 8888
SAZ_SERVER_DN   /DC=org/DC=doegrids/OU=Services/CN=saz.fnal.gov
```

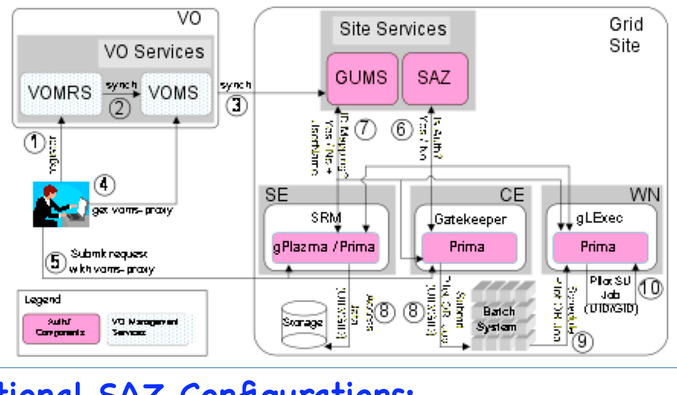
Multiple SAZ servers may be configured in sazc.conf. If more than one SAZ server is configured in sazc.conf, the SAZ servers are contacted in series for each and every authorization request.

The SAZ server interfaces to the backend MySQL database via the Java hibernate method.

SAZ Diagram:



OSG VO Services Architecture:



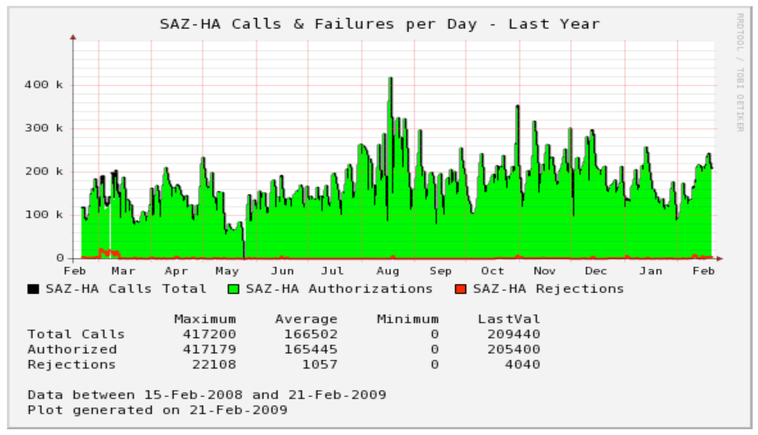
Current Status:

SAZ V1.0 was deployed within FermiGrid in October 2006.

The current version of SAZ is V2.0.1b (released in November 2008).

All code paths in the SAZ service are regression tested prior to the release and production deployment of the new version.

The current SAZ deployment has been stress tested to 1,000,000+ authorization decisions/day, routinely handles 18,000 authorization decisions/hour and has handled peaks of > 27,000/hour.



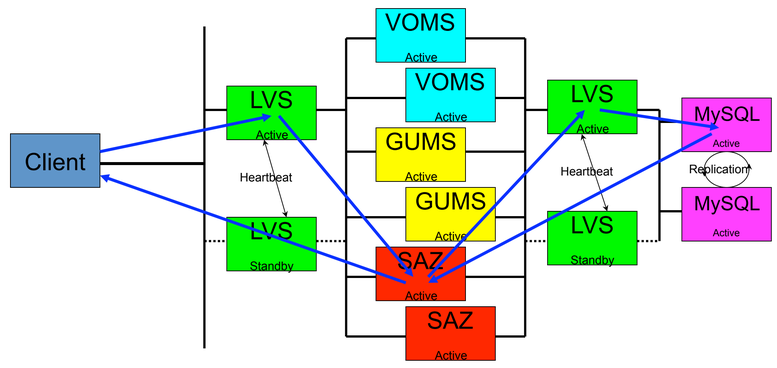
SAZ & FermiGrid-HA:

SAZ is one of the services in the FermiGrid service catalog that is deployed in high availability (HA) configuration that is collectively known as "FermiGrid-HA".

- The goal for FermiGrid-HA is > 99.999% service availability.
- For the period of 01-Dec-2007 through 30-Jun-2008, we achieved a service availability of 99.9969%.
- for the period from 01-Jul-2008 through 20-Feb-2009, we have currently achieved a service availability of 99.9810%.

FermiGrid-HA utilizes three key technologies:

- Linux Virtual Server (LVS).
- Xen Hypervisor.
- MySQL Circular Replication.



Optional SAZ Configurations:

As indicated in the SAZ service description above, the SAZ client can be configured to query multiple SAZ servers.

A site can deploy multiple SAZ servers. Possibilities include:

- One to control access to Globus gatekeepers,
- A second to control access by Grid pilot jobs (gLExec),
- A third to control access to Grid storage via GridFTP or SRM/dCache.

These SAZ servers can be configured with:

- Individual backend MySQL databases,
- Shared access to a common backend MySQL database,
- A combination of individual and common backend MySQL databases.

A Grid may deploy a central SAZ server.

- The contents of the central SAZ server backend MySQL database can be replicated to individual Grid sites to reduce the WAN latency and potential timeouts.

Individual Grid resources may:

- Query the local Grid site SAZ server,
- Query the central Grid SAZ server,
- Replicate the contents of the central Grid SAZ server MySQL database to a local SAZ server MySQL database,
- Use a combination of a local and an (optionally replicated) Grid wide SAZ service.

Future Work:

The SAZ service is under active development.

The current SAZ administrative interface is via a command line tool, a web interface will shortly be deployed.

A security review of the SAZ code was recently undertaken, and the results of the security review will be incorporated in the near term work.

The SAZ client-server interface will be extended to support the Globus XACML interface.

As a consequence of the XACML extensions, the majority of the Grid proxy information parsing will move into the client (currently this in the server), and this is expected to significantly improve the performance of the SAZ server.

Conclusions:

The SAZ service is working well in FermiGrid.

There are some known limitations that will be addressed shortly.

We are open to offers of collaboration in the future development and deployment of SAZ.

Work supported by the U.S. Department of Energy under contract No. DE-AC02-07CH11359