Open Science Grid Consortium
Privilege Project
PPDG-Common Project

FQANs Distilled.

A Manager's Guide to FQANs for RBAC on OSG v0.2

Last Updated: 06/03/2005

Open Science Grid infrastructure puts emphasis on Role Based Access Control (RBAC) as a preferred means of providing access to the resource fabric. Within the scope of this document, *resource fabric* refers to compute and storage resources.

The RBAC model on OSG v0.2 uses VOMS X.509 Attribute Certificates (ACs) to bind extra attributes to a certificate bearer. These ACs make use of a well-formed string called FQAN.

An FQAN or **Fully Qualified Attribute Name** is defined by the syntax:

Organizational membership[/Role=***role name***][/Capability=***capability name***]

Organizational membership is listed as a string in a directory like structure delimited by forward slashes. The first token in this string is *required*. Thus, **Organizational membership** is defined by the syntax:

vo[/***group***[/***subgroup***[/…]]]

Please note: (i) Square brackets [ ] imply *optional* tokens in the FQAN syntax. (ii) The token Capability may become deprecated in near future, more information will be listed here when available. Refrain from using this token meanwhile.

Responsibilities:

1. Management Personnel of a VO declare the FQANs relevant to this VO's virtual structure.
2. Members of a VO request registration with a clearance to use FQANs that apply to them.
3. VO Administrators maintain this information in registration databases.
4. Site Administrators perform necessary tasks required to make use of RBAC. These tasks entail creation of POSIX accounts (UIDs, GIDs) and related triage for both compute and storage resources, deployment of GUMS for each such *account-domain*, populating GUMS from registration databases, maintenance of VOMS servers contact information for all VOs, etc.
5. An OSG User (member of one or more VOs) specifies an FQAN and a VOMS server (or list thereof, if duplicate servers are available) to contact, while requesting an X.509 proxy.

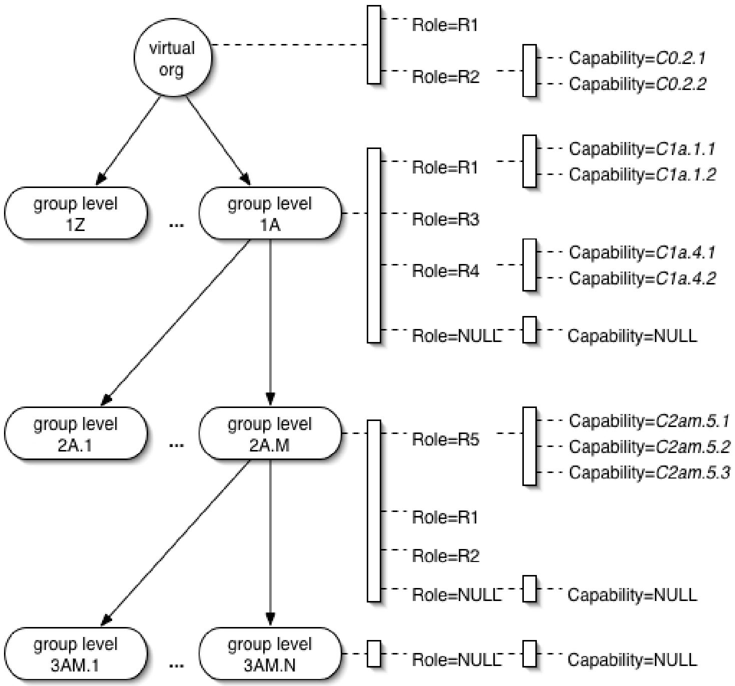
Recommendations to VO management personnel while declaring FQANs:

Please avoid uppercase alphabet, it is inconvenient and prone to ambiguity.

Deliberation within a VO may be needed to decide on the top-level membership string ***vo***. This string identifies the VO, and may be expected to persist for a long time on the OSG infrastructure. Any future changes will be inconvenient for, and will need to be communicated to, the user community.

Identify meaningful roles and capabilities in accordance with VO's computing needs and policies. The roles and capabilities can be declared for every level of membership.

Identify members within the organization to assign high-order privileges to, and communicate these to the VO registration administrators who maintain the databases.



FQANs descriptive of Group Membership with Roles and Capabilities in a Virtual Organization

```
/([a-zA-Z][a-zA-Z0-9-]*[a-zA-Z0-9]\\.)*[a-zA-Z][a-zA-Z0-9-]*[a-zA-Z0-9](/[\\w-]+)*(/Role=[\\w-]+)?(/Capability=[\\w-]+)?
```

More details, most current Regex, and Class API by **Gabriele Carcassi** are available at: `http://grid.racf.bnl.gov/GUMS/components/business/apidocs/gov/bnl/gums/FQAN.html`

Editors: Abhishek Singh Rana, Frank Wuerthwein. Comments: rana@fnal.gov