VOMS Attributes usage open issues.

EGEE Security Cluster.

www.eu-egee.org

Information Society

- The following answers reflect the short-term situation.
- General authorization study for medium term has been commissioned.
- Most of the items are a part of the overall authZ study in JRA1.

1. “Semantics of matchmaking. LCMAPS uses an ordered list with a first-match-wins algorithm. The workload management uses a symmetric technique that considers all matches in the list as equally valid. The DPM uses yet another technique that in principle assigns a distinct, unique ID to every new FQAN encountered; matchmaking in this sense means instructing the database by hand to map a list of FQANs to a single internal DPM id. This list only considers three products; there are more.”

   These applications have different goals, with obviously different usage.

   These issues will be considered in light of the overall authZ proposal.

2. “Syntax of matchmaking – how do FQAN patterns (perhaps with wildcards) match FQANs? We have already discovered a slight difference in the implementation of this matching between LCMAPS and the WMS. Other products have not been surveyed AFAIK.”

   The match-making rules have been clarified.

   See `https://edms.cern.ch/document/858263/1.`

   Software libraries in C and Java have been produced by JRA1.

   Under review by VOMS team.

3. “Syntax of ACBRs – the CEs have syntax like
   VO:atlas
   while for storage elements, it is simply
   atlas
   furthermore, it is not defined whether (by DESIGN, not by implementation), for example,
   VOMS:/atlas
   matches *everything* under /atlas (so, an implicit *), or means implicitly atlas with nothing else
   (/atlas/Role=Null/Capability=Null).”
   See `https://edms.cern.ch/document/858263/1.`
   Note: the first two examples are invalid FQANs.
   (The third example does not match everything under /atlas).
   Correct syntax is VOMS:/atlas etc. Please see:

   `http://edg-wp2.web.cern.ch/edg-wp2/security/voms/edg-voms-credential.pdf`

4. “Generic attributes – pressure to have these influence the action of the generic middleware, vs strong reaction from designers to keep generic attributes completely in domain of VO (ie that generic middleware is absolutely blind to GAs).”
   There is no difference between GAs and groups/roles as far as authoritativeness matters are considered.
   A consistent usage of GA requires a generic framework of handling these attributes across several VOs in the middleware.
   A use-case to consider is when the VOMS GAs package the Shibboleth SAML assertions (SWITCH).

5. “Multiple roles – pressure from experiments to have multiple roles in primary FQAN, vs known ambiguities and interoperability issues”

   One FQAN contains at most one role.

   The current implementation of multiple roles within one FQAN in not supported within the middleware. Consideration is given to this issue in the context of the authorization study (please provide feedback).

   No pressure to include this seen yet.

6. “DENY tags and/or negative ACLs – introduced as a short-term hack to deal with issue 1 above; in danger of elevating themselves above the hack level without understanding whether the status is warranted or even a good idea.”
   General opinion: bad idea, goes against the “minimum privilege” principle.

7. “the general issue of how to specify, within the lifetime of a single job, which of the various FQANs possessed by a user’s proxy, are to be used for various interactions with various grid services. For example use FQAN x for metadata catalogue access and FQAN y for uploading a file to the data management stack.”

   Attributes are used for many purposes.

   In general, attributes are not designed to be used in an ordered fashion.

   VOMS attribs CAN be ordered using `voms-proxy-init --order`

   MW SHOULD not have to depend on the order of attributes.

   The VO should decide how to divide these attributes, the division will be a result of the needs of specific software/VOs.

   No short term solution, subject in authZ study.