VOMS-Admin developments

Andrea Ceccanti

JRA1 All-Hands Meeting

June 2007, Helsinki

Today

- **Voms-Admin 2.0.4 is now in certification**
  - oracle oci driver support
  - minor fixes for compatibility with glite configuration scripts
  - fixes for cli client on python 2.3

- **Should go in production quite soon**
  - Strong requests from the VOs

New developments

- **JSPG compliance**
- **Multiple certificates support**

- **Planned for**
  - VOMS-Admin 2.5
  - VOMS 1.8.0

- **ETA: October 2007**

- **Joint upgrade of core and admin is required to get the new features**

JSPG Compliance

- **JSPG rules compliant registration service means**
  - Multiple certificates support
  - Support for suspension/expiration of VO users
  - Support for management and versioning of VO Acceptable Usage Policy (AUP)
  - Support for users requests for
    - Group membership
    - Role assignment
    - Generic attributes assignment

Multiple certificate support

- **VOMS currently has a 1-to-1 coupling between VO members and certificates**
  - each (DN,CA) couple represents a member
  - attributes are mapped to each (DN, CA) couple
- **However**
  - We need to handle user's certificate expiration more gracefully
  - Allow for aliases (multiple identities) for the same VO membership

Multiple Certificate Support (...)

- **Users, once registered, can request the addition of other certificates to their membership**
  - This operation needs the VO-Admin authorization
- **The identities/aliases share the VOMS attributes info**
  - Groups
  - Roles
  - Generic Attributes
- **VOMS keeps track of certificate validity**
  - warn users when ceritificates are about to expire:
    - via email
    - at voms-proxy-init time

User suspension/expiration

- **Currently not supported in VOMS/VOMS-Admin**
  - but required for JSPG compliance
- **Needed to:**
  - Suspend users if they have not agreed to the more recent version of the VO Acceptable Usage Policy (AUP)
  - Suspend users after a security incident
  - Suspend users after a given period of time
- **Suspension will be implemented at the certificate level**
  - If you want to completely suspend a membership, suspend all the associated certificates
- **Users will be informed of suspension**
  - via email
  - at voms-proxy-init time

Compatibility issues

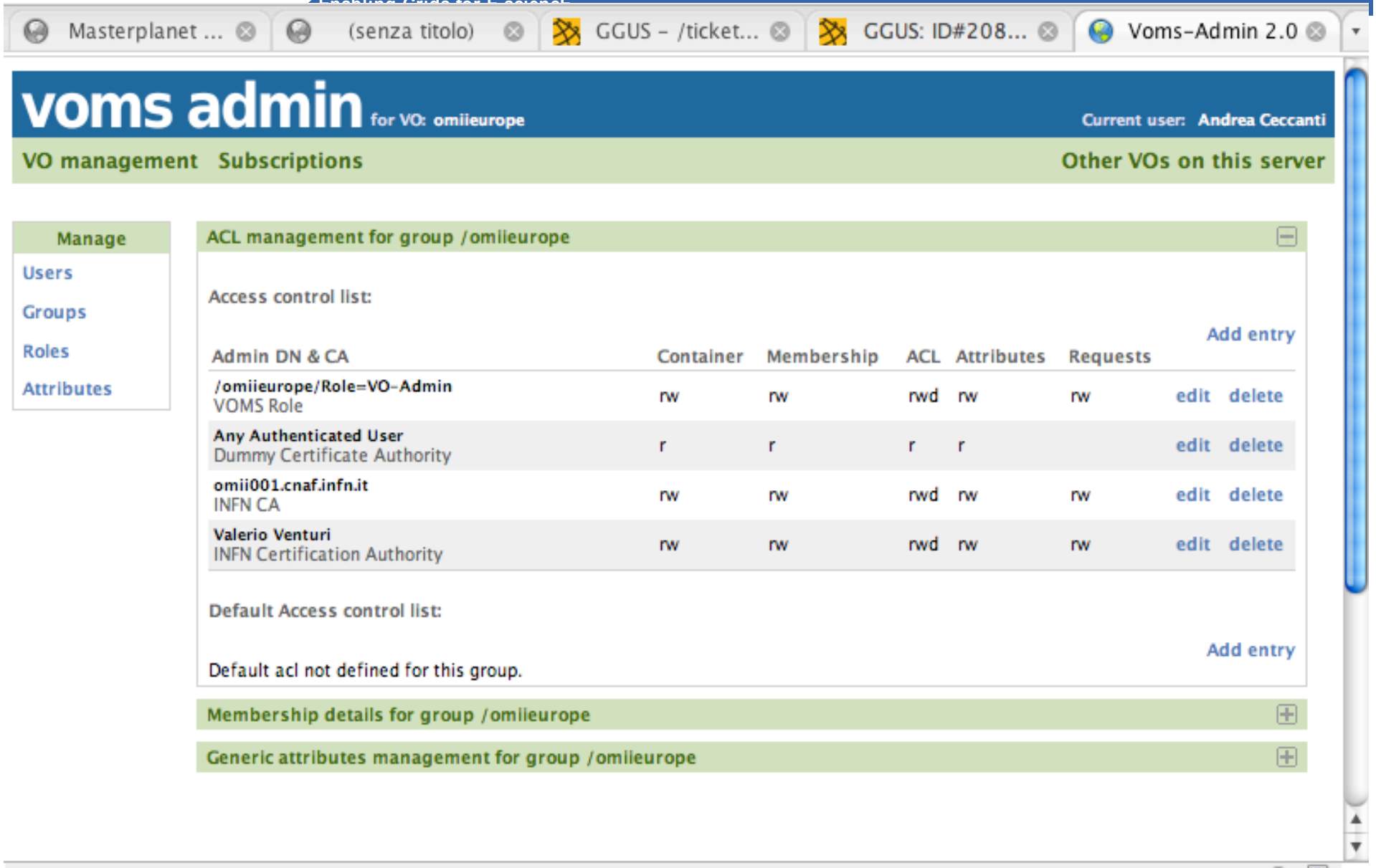
- **Existing APIs will continue to work as expected**
  - however distinct certificates will appear to VOMS as distinct VO members (exactly as today)
- **New APIs will be provided to manage**
  - user certificates
  - suspension

VOMS-Admin AuthZ framework

- **All Operations on the VOMS DB are authorized via ACL**

- **ACLs are (Context, Principal, Permission) triples**
  - The Context is a FQAN
  - The Principal is either
    - a (DN, CA) couple
    - a FQAN
    - ANY_AUTHENTICATED_USER
  - The Permission states what the principal can do in the Context
    - List/Add members to a Group/Role
    - Create subgroups
    - Manage attributes
    - Manage requests/subscriptions pertaining groups/roles

VOMS-Admin ACLs



Current framework limitations

- **It's impossible to group administrators without using FQANs**
  - However most administration tasks could have nothing to do with VO Membership and VOMS attributes
    - e.g., VO-Manager or Insitute Representatives JSPG "roles"
- **It is difficoult to create a hierarchy of administrators in order to delegate administration tasks**

The Admin Tags/Tasks framework

- **Very simple framework to organize administration activities on the VOMS DB**
- **Tags are basically labels that may be assigned to VO admins/users**
  - group together admins with the same permissions/responsibilities
  - used only for authorization purposes on VOMS-Admin
    - do not represent information that will end in users' voms proxies
- **Tasks are VOMS administrative operation that can be assigned to Tags (i.e., to group of admins/users)**
  - e.g., Approve group membership, Accept VO AUP,...

The Notification service

- **Simple notification service**
  - VO managers can send email messages to group members, members with a specific role,...
- **The core functionality is already implemented and used in the current simple registration service**
  - Will be augmented to incorporate Tags support
- **Need to work on a usable WEB UI**