NORDUGRID

Grid Solution for Wide Area Computing and Data Handling

KnowARC

arcproxy

Weizhong Qiang

presented by Oxana Smirnova

EGEE'09 Conference

Barcelona, Spain, 22 September 2009

Existing proxy creation utilities

- grid-proxy-init
  - Issues a proxy certificate by itself (no external services involved)
- voms-proxy-init
  - Contacts a VOMS server to acquire an Attribute Certificate (AC)
  - Issues a proxy certificate with AC embedded
  - Policy support as PCI (Proxy Certificate Information) extension

Existing proxy creation utilities

- myproxy-init
  - Contacts a MyProxy server to delegate user's credential to this MyProxy server
  - Contacts MyProxy server to retrieve the delegated credential (2nd-level delegation)
- gridshib-saml-issuer
  - Issues a SAML assertion by itself and binds this assertion to the proxy certificate as a certificate extension

NORDUGRID
Grid Solution for Wide Area Computing and Data Handling

Why arcproxy?

- By popular request, all the above functionalities should be included in **<u>one</u>** proxy utility by ARC
- ***<u>No wrappers allowed</u>***, as one of the key principles of ARC is:
  - Minimize dependency on external packages
    - That is: we can not tolerate installation of all the (obscure) packages to get the functionality; those packages tend to depend on other packages that again add multiple unmanageable dependencies
- A “super-proxy” client utility is needed:
  - To include all known functionalities
  - To be extensible to include other certificate extensions

NORDUGRID
Grid Solution for Wide Area Computing and Data Handling

What is arcproxy?

- Client utility for proxy generation
  - Includes functionality of `grid-proxy-init`, plus supports embedding of delegation policy (PCI extension)
  - Includes functionality of contacting VOMS server and generating proxy certificates with VOMS AC
    - speaks boith GSI and standard TLS for protocols
    - also includes functionality of listing available VOMS attributes
  - Includes functionality of working with MyProxy servers (delegating credentials to and getting delegated credentials from MyProxy servers) via GSI

NORDUGRID
Grid Solution for Wide Area Computing and Data Handling

How is arcproxy implemented

- Based on the modular implementation of new ARC clients/services
  - GSI or TLS protocol usage is configurable
- VOMS
  - Reuses part of the VOMS code (parsing attribute certificates), but does not depend on the VOMS API
  - Re-implements the protocol required to contact VOMS server
- MyProxy
  - Re-implements the protocol required to contact MyProxy servers (http://grid.ncsa.illinois.edu/myproxy/protocol/)
  - Currently, “authorization challenges” are not supported

NORDUGRID
Grid Solution for Wide Area Computing and Data Handling

arcproxy TODO

- Future work: embed SAML assertion as a proxy extension
  - arcproxy authenticates against AA (Attribute Authority) service, and acquires SAML assertion
  - arcproxy embeds SAML assertion as a proxy extension
- An example of an AA can be e.g. SAML VOMS
  - ARC also implements own AA service
    - Act as an Attribute Authority to issue SAML attribute assertion
    - Has the same interface as the VOMS AA service
    - Can reuse VOMS database as a back-end database
    - Can reuse voms-admin service for managing the VOMS attributes
    - Configurable to adapt other database schemae

NORDUGRID
Grid Solution for Wide Area Computing and Data Handling

How to use arcproxy?

- `arcproxy` (simple RFC-compliant proxy)
- `arcproxy -S knowarc.eu` (RFC-compliant proxy with VOMS extension)
- `arcproxy -S atlas -O` (GSI legacy proxy)
- `arcproxy -G -S knowarc.eu` (use GSI instead of TLS)
- `arcproxy -V /some/path/myvomses -S knowarc.eu:all` (acquire all possible roles)
- `arcproxy -S knowarc.eu:/knowarc.eu/Role=Developer` (specify the VO name and role that you need to acquire from VOMS server)
- `arcproxy -S atlas:list` (only list the attributes in the VOMS server, does not create any proxy)
- `arcproxy -U oxana -L knowarc1.grid.niif.hu -M PUT` (store delegated proxy at a MyProxy server; use `-M GET` to retrieve)
  - Can be used together with acquiring VOMS extensions