AAI usage, issues and wishes for HEP

Maarten Litmaath
CERN

Introduction

- WLCG deemed representative for HEP in general
  - Input received from ATLAS, CMS, LHCb
- Input also taken from 2009 autumn HEPiX presentation
  - "Security aspects of the WLCG infrastructure"
    - http://indico.cern.ch/contributionDisplay.py?sessionId=20&contribId=27&confId=61917
  - Provides further details, illustrations and background

Questionnaire answers (1)

1. How are users currently authenticated?
   1.1 Which credential(s) is/are used?
   1.2 How is the user vetting done?

- X509 credentials with VOMS extensions
  - LHCb also include their own extensions in the proxy for their DIRAC data analysis services
- Each user gets an X509 certificate from a national or organizational (HEP-specific) CA
  - Some institutes use SLCS certificates linked to local or national identities
- WLCG has a catch-all CA for LHC experiment members who cannot obtain a certificate from their country's CA
  - E.g. because an approved CA does not yet exist
  - GRID-FR also have such a service for CNRS partners

Questionnaire answers (2)

- A user is affiliated with an institution that participates in a research collaboration (e.g. experiment) → VO
- The user registers in the VOMS server of the VO and gets the right to attributes corresponding to the user's responsibilities
- The user can be suspended or removed from the VO by a VOMS admin for that VO
  - Effective within 6 h for services relying on a classic grid-mapfile
    - And for the LHCb DIRAC services
  - Else may be counteracted by long-lived VOMS proxies
    - WLCG VOs still allow for multi-day VOMS proxies

Questionnaire answers (3)

2. Is there a link to national identities? If so, how are different national identities leveraged?

- The VOMS hierarchies for ATLAS and CMS contain groups for national identities organized per country
  - A user can apply for membership of the relevant group(s)

- A resource provider in a particular country may configure certain resources to give preferential treatment to users affiliated with that country
  - When the primary FQAN of the proxy is the country's group
  - When the DN is recognized as being a member of that group
    - A local grid-mapfile could give a special mapping to such DNs

Questionnaire answers (4)

3. Which types of resources are used and how are users authorized?
   - 3.1 Resources accessed through grid technology
   - 3.2 Resources accessed without grid technology
   - 3.3 Web-based resources

- Through the grid, normally via native VOMS support or grid-mapfile equivalents
  - Computing and storage elements
  - Catalogs, possibly other databases
  - Workload and data management services
  - Information, monitoring and messaging services
    - BDII is world-readable
  - Proxy renewal services, VO agent nodes, …
    - MyProxy only requires trusted CA

Questionnaire answers (5)

- Outside the grid, via local user identities
  - Computing and storage elements
    - Local batch submission
    - Local (possibly insecure "backdoor") data access
  - Catalogs, databases
    - E.g. DB account + password in configuration file
  - …
- Web-based resources, via user certificates and grid-mapfile equivalents, or SSO, or user + password, or world-readable
  - Catalogs, databases
  - Workload and data management portals
  - Information and monitoring systems
  - Operations, ticketing and accounting portals
  - Documentation, conferencing, …

Questionnaire answers (6)

4. Where does the project want to be in ~5 years with regards to authentication and authorization?
5. Are your users and resource owners happy with the current AAI scheme that you use?

- Though the AAI schemes in use allow the HEP VOs to use the grid infrastructures quite successfully, users and resource owners are not really happy with how grid security works and would like to see various aspects improved in the coming years.
  - Details on the next pages.

Issues and wishes (1)

- VOMS lifetime may differ from proxy lifetime
  - VOMS renewal differs from proxy renewal
- Concurrent activities by the same user (e.g. with different roles) can be tricky to manage
  - Beware not to use/overwrite the wrong proxy file
  - Beware each node in an interactive cluster has its own "/tmp"
- Conflicting uses of primary FQANs
  - To get the right treatment on the CE (priority/share/queue) the primary FQAN is decisive
  - That FQAN may be very undesirable for data operations
    - VOs may need to grant artificial privileges to such FQANs in their storage elements, catalogs, …
    - Regenerating proxy on the WN (only for writing) → fragile
  - Pilot and cloud systems can avoid such conflicts
  - Roles/groups could be explicitly associated with services
    - Each service picks the role(s)/group(s) it recognizes

Issues and wishes (2)

- Web browsers cannot import VOMS proxies
  - Web services need grid-mapfile equivalents to regulate access
- Short lived tokens should be used to access a particular service repeatedly
  - Avoid expensive AA overhead
- Standard OpenSSL/GSSAPI/… should be used instead of Globus
  - Reduce dependencies, avoid conflicting versions
- It would be nice to have proxies supported at OS level

- Users would like not to worry about proxy expiration etc.
- Migration to a new certificate can be a hassle
  - Certificate validity could be increased to 3-5 years
    - People who leave should be faster removed from their VOs
  - DN should change only exceptionally

Issues and wishes (3)

- Management of a VO is centralized
  - VO manager is needed also for changes local to a group/site
- Consistent implementation of shares and permissions across sites is difficult due to lack of standardization
  - Storage quotas per user are essentially absent
  - VO super users would be needed for data management
- Synchronization of access rights on catalogs and all storage elements for the VO is cumbersome and ad-hoc
  - A consistency service demonstrator is expected in a few months

- Service authorization ought to be improved
  - A valid host certificate does not prove the service is valid
  - Service certificates should be better supported

Issues (4)

- Incoherence of security models implemented by services
  - Multiple libraries
    - Configurations, algorithms, logs
  - Mapping, ACLs
    - DN
    - VOMS attributes
  - Logging
    - Formats, contents
  - Banning
    - Not possible or awkward on certain services
  - Testing/debugging/forensics tools
    - Available for some scenarios on some services

- There probably are other issues not explicitly listed here…