Authentication and Authorization (AAI) issues concerning Storage Systems and Data Access

Pre-GDB summary, 2013-02-13
Maarten Litmaath

Pre-GDB details

- Agenda
  - http://indico.cern.ch/conferenceDisplay.py?confId=222767
- Attendance
  - 36 people
  - ALICE, ATLAS, CMS
  - CASTOR, dCache, DPM, EOS
  - LFC, FTS, lcg_utils
  - ASGC, CERN, CNAF, DESY, GRIF, KISTI, LIP, NIKHEF, Prague, RAL, Roma1
  - WLCG + EGI + EMI security & operations
  - AA
- Duration
  - 3.5 h

Read access to data

- ATLAS, CMS: no data can be made world-readable
- Raise the bar sufficiently, but we have no industrial or military secrets
  - No worries about wiretaps etc.
  - Presentations in Indico are much more interesting targets!
- Local clients can still be given a lower authorization overhead for better performance
  - In particular for better caching
  - SE needs to determine at least the client’s VO and regulate access accordingly

Data ownership issues (1)

- Q: use VOMS nickname == CERN account == Kerberos principal for denoting ownership?
- A: rather try exploiting ACL functionalities instead!
  - – Also allows for sharing files
  - – And distinguish between write and delete access on EOS
    - Also seems possible on dCache/DPM
  - – And for superuser concept (to some extent)
    - ATLAS: the space owner is the space superuser
  - – Define and use VOMS groups as needed
    - Helps avoiding the need for modifying ACLs
  - – May need to use implementation-specific API

Data ownership issues (2)

- ALICE: LDAP service maps DN to AliEn/CERN account used for denoting ownership
  - SE only needs to verify if the access envelope looks OK and log the details
- External identity management → possible path to convenient federated identity support?
- Data owned by a VO, group or service → use robot instead of user certificates
- Kerberos access → site-local matter, not WLCG
  - CMS maintain map-file for EOS, ATLAS almost ready for deploying similar mechanism

ES

Data ownership issues (3)

- VO superuser for SE
  - Solved in EOS
  - Also works to some extent per ATLAS space
    - E.g. file deletion
    - Cannot fix ACLs, ownership DN, or mapping
    - Recursive changes often cumbersome for SE admin
  - Seems possible for dCache/DPM
    - With similar limitations
  - Need to use implementation-specific API

CERN
IT

Clouds and dreams

- Cloud storage concerns?
  - Too early, only used as back-ends for now
  - Try and move toward standard technologies and simplify things at the same time
- Avoid asking for non-trivial features that risk not getting used in the end!
  - ACLs were required and implemented, but not yet fully explored
- Use industry solutions like ACLs
  - Also better for getting EU resources