AAI on Storage Systems

Status quo

- SE + catalog configurations
  - ♦ Protect production data from users
  - ♦ Some experiments prevent tape access by users
  - ♦ User and group access regulated by experiment frameworks
    - ◊ Including quotas
    - ◊ SE may be more permissive than desired
      - · To be checked and fixed as needed
- X509 overhead
  - ♦ Use bulk methods, sessions, trusted hosts as needed
  - ♦ Cheap short-lived tokens may become desirable

Data protection

- Do different data classes need the same security model?
  - ♦ Custodial
  - ♦ Cached
  - ♦ User
- Access audit trail important for traceability
  - ♦ Security and performance investigations
- Protection needed against:
  - ♦ Information leakage ("Higgs-discovery.root")
  - ♦ Accidental commands
  - ♦ Malicious outsider, insider

Issues with data ownership

- Missing concept: data owned by the whole VO or by a service
  - ♦ Use robot certificates for that?
- Mapping person to/from credential
  - ♦ Changes have consequences for data ownership
    - ◊ Certificate might indicate "formerly known as"?
    - ◊ Make use of VOMS nicknames or generic attributes?
  - ♦ X509 vs. Kerberos access
- VO superuser concept desirable?
  - ♦ Avoid bothering SE admin for cleanups

More items

- CASTOR: RFIO/NS backdoors to be closed
- Not only data, but also SE itself needs protection
  - ♦ Against illegal data, DoS
- Storage quotas
  - ♦ On SE: conflict with replicas
  - ♦ Better handled by experiment framework
  - ♦ Can still be useful to SE admin
  - ♦ Low priority, available for some SE types
- Quotas on other resources e.g. bandwidth?
  - ♦ Prevent DoS

Pre-GDB meeting Feb 12, 2013

- Pre-GDB agenda
  - Introduction of the status quo and unresolved issues
  - Summary presented in the GDB meeting the next day

-- MaartenLitmaath - 29-Feb-2012

This topic: LCG > AAIOnStorageSystems
Topic revision: r6 - 2013-02-14 - MaartenLitmaath