Conclusions from VO Box Working Group

J. Templon (NIKHEF)

Operations Workshop (CERN)
19 June 2006
• Introduction
• Classification of VO services
• Priorities:
  – Development
  – Operations
• Longer-term Issues

• The priorities and issues within each section are listed from highest to lowest priority.

• VO box agendas and minutes can be found here:
Classification of VO Services

- **Class 1:**
  - Can access site's services (and work correctly) from a private network. (I.e. does not need to live within the trusted subnet of a farm.) Uses only service APIs/interfaces which are exposed to the external world past their firewall.

- **Class 2:**
  - Uses 'private' interfaces to access information/services at the site (i.e. not exposed to those beyond the site's firewall). Essentially this is anything which is not a Class 1 service.
• **Reduce security issues with VO services “inside” site.**
  - Without class 2 services, security issues are at the same level as public interfaces which are already acceptable and managed by sites.
  - Current class 2 examples
    - Package management of ALICE (NFS access)
    - “SRM ls” for CMS (direct access to SE disks)
  - These cause problems with accounting, balancing service load, controlling access, etc.

• **Permit alternate, more flexible deployment scenarios.**
  - If only public interfaces are used, the firewall is already configured to allow external access.
  - Can then have VO Box deployed externally which would allow sharing of VO Boxes between sites, etc.
• Package management (ALICE)
  – Class 2 issue: access to shared file system for sw installation
  – Package management service which allows dynamic installation of experiment software.
  – Requirements document available and still valid.
  – Needs to be simple, bare-bones implementation initially.

• SRM v2 (CMS)
  – Class 2 issue: need access to disks for listing files
  – Need “list” functionality in SRM to ensure consistency between SE and central catalogs.
**Development Priorities**

- **Consistent Security Framework (All expts.)**
  - Documentation of overall framework.
  - Proxy renewal service
    - Handles VOMS renewal as well.
    - Run as root and use host certificate.
    - Work out scalable mechanism for who can renew.
  - Delegation service/API
    - Mechanism better publicized with examples.
  - Consistent use of security model throughout services.
    - E.g. FTS proxy renewal, not passwords for new proxies.
    - Integration of VOMS groups, roles

- **xrootd as SE transport protocol (ALICE, CMS)**
  - Would avoid inefficient data transfers through VO Box for ALICE (if deployed at VO service on VO Box).
  - Others would probably use protocol if it were available.
“Operations” Priorities

- Eliminate use of shared credentials:
  - Default configuration must work without using shared credentials.
  - E.g. must not assume that all “software managers” are mapped to the same unix account.

- SFT (Site Functional Tests)
  - Must be developed to test “core” software on VO Boxes.
  - Make documentation available for writing application-specific SFTs.

- Mechanism for publishing VO services:
  - Experiments have need to discover their own services.
  - Need sol’n for doing so integrated into the gLite distribution.
Longer-term Issues

- **Messaging and notification**
  - See need for these popping up in many contexts
    - Job monitoring
    - Interactions between services (e.g. FTS and VO services)
  - Need to work out general framework for providing this functionality and then include appropriate services in gLite.
Longer-term Issues

- **Monitoring via monalisa:**
  - ALICE, CMS, and LHCb are interesting in using this for monitoring.
  - Potential license issue for inclusion in gLite release.
  - Sites want single monitoring framework: if monalisa comes in, something else goes out (noises about GridIce on PPS list …).

- **General VO service framework**
  - Is and will be needed for VOs to run services.
  - Need to work towards a generic framework to allow this to be done flexibly by the VOs.
  - Related for example to VO-specific plugins to services.
  - Consistent security framework and tools are prerequisites.
Conclusions (JT)

- VO boxes are deployed but “on probation” as long as class 2 services are present
- WG was “not worried” (technical issues) about VO boxes if pure class 1
- Good case was made that “one size can’t quite fit all”
- Proper framework eases problems for everyone
  - Plan exists for both short and long term