VO Box Issues

Summary of concerns expressed following publication of Jeff's slides

(not necessarily the opinion of) Ian Bird

GDB, Bologna, 12 Oct 2005

General concerns

- Ops and security documents:
  - List of questions to help sites understand what is needed
  - Hard to translate into site policy – IPTables, firewalls, ports, etc.
  - Questionnaires are more overhead for site admins
- Use of host certificates for services is never acceptable
- Number of boxes – heavy tax on small sites
  - Do all sites need to run a VO Box?
- Many sites will say NO unless the requirements are minimal
  - E.g. UK only 1 site willing to provide this for ALICE
- Most security concerns addressed by document

Other concerns

- This should be a short term solution
- Experiments should ensure that VO specific services get translated into general grid services for the future
- This is not a grid solution !
- How does the software get certified?
- Concerns about allowing interactive logins at all

LCG VO Box *prototype*

OSG are developing "Edge Service Framework" based on virtual machines to solve the same problem.

VOBOX: Overview

- Basic (common) requirements
  - Scientific Linux 3 (usually)
  - Outbound connectivity as a UI
  - Inbound connectivity as a CE + gsissh port + VO requirements
  - Access to local user accounts (SGMs) via gsissh
  - Direct (mounted) access to the site's experiment SW installation area
- LCG's VO box prototype basic elements
  - gsissh server
  - Proxy renewal service (+ user level tool)
    - For automatic refresh of user credentials
  - For AFS-based sites with GSI-Kerberos mapping service:
    - GSSKLOG client to grant Kerberos tokens from X509 proxies
  - CLIs and APIs for job submission to local CE
    - Connection open for job lifetime ➔ Not scalable! ➔ Only for few special jobs

VOBOX: the gsissh server

- Allows the experiment SGM to access the VO box
  - User space (not root access)
  - Interactive login through gsissh client
  - Upload/Download files via gsiscp
- Usual authentication/authorization schema
  - GSI. Using the grid-mapfile
- Allows credential delegation
  - Only within the login session
  - Must be turned on at the client and server side
    - Done automatically for both by YAIM in LCG 2.6
- Running by default on port 1975
- Not VOMS-aware

VOBOX: Proxy renewal service

- Automatic SGM's proxy renewal procedure
  - The SGM…
    - Registers a long-living proxy in a MyProxy Server
    - Logs into the VO box
    - Registers his delegated user proxy for renewal (VO box specific CLI)
  - The proxy renewal service renews the user proxy every 2 hours
- The MyProxy server has to trust the VO box
  - The renewal service must present the (trusted) VO box host certificate
  - A root cronjob runs every hour
    - Creates the host proxy + "chown"s it to the VO SGM
- There can be only one VO per VO box
  - Or they all would share same copy of host proxy ➔ Traceability issue
  - Possible solutions to this problem
    - Run several VO boxes on the same HW, but on different virtual machines
    - Modify MyProxy to make it accept service certificates (several per machine)

VOBOX: miscellaneous

- User Interface clients should also be installed
  - Additional functionality at no cost (just clients)
  - Successfully tested many times and deployed at some sites
- A RB can also be installed on top of the VO box (next release)
  - For job submission to the local CE
  - (Solved) clash of two versions of the gridftp server (CE and RB)
    - The old one will be removed from the RPM list
    - Fully tested and supported in YAIM
  - BUT… This would need more maintenance effort from the site
- Experiment SW area
  - An env variable points to the experiment SW area of each VO
    - Not automatically accessible after YAIM installation (duty of the site admin)
    - Same as in a WN
  - A gssklog client allows to get kerberos credentials from a X509 proxy
    - Needed only if the Exp SW area is on AFS
    - A X509toKRB authentication server needs to be installed at the site