



Enabling Grids for  
E-science in Europe

[www.eu-egee.org](http://www.eu-egee.org)

Operations Workshop -- Abingdon, 27-29 Sept. 2005

# VO box: Experiment requirements and LCG prototype

Antonio Delgado Peris  
CERN IT - LCG GD/EIS



EGEE is a project funded by the European Union under contract IST-2003-508833

- Introduction
- LCG's VO box prototype
- Experiments' requirements
  - Alice
  - CMS
  - Atlas
  - LHCb

# Introduction

- What is a VO box?
  - Dedicated node on which to deploy and manage VO specific long-lived agents and services
- Which VOs require a VO box?
  - Alice, Atlas, and LHCb
  - CMS requires some services at the sites (might sit in the VO box)
- Where
  - Alice: Tier-1s only
  - Atlas: Each site where they run
  - CMS: Each site where they run
  - LHCb: Each site participating in SC3
- Experiments requirements
  - Summary of what the VOs expect from the VO boxes
  - Not meant to be an exhaustive list

# Contents

- Introduction
- LCG's VO box prototype
- Experiments' requirements
  - Alice
  - CMS
  - Atlas
  - LHCb

# 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



# Contents

- Introduction
- LCG's VO box prototype
- Experiments' requirements
  - Alice
  - CMS
  - Atlas
  - LHCb

- General requirements:
  - PIII 2GHz, 1024 MB RAM. Any Linux flavour, kernel 2.4+.
  - User accounts for SGMs, via gsissh
  - UI functionality (including FTS and access to local catalog)
  - Access to the experiment software installation area
  
- Agents and services
  - Site service interfaces and monitoring agents:
    - Storage Element Service (SES), File Transfer Daemon (Interface to FTS)
    - Cluster Monitor (CM), MonALISA, Agents Monitoring
    - Alien Computing Element (Interface to LCG RB)
    - PackMan (PM), xrootd
  
  - Connectivity
    - Outbound connectivity + Access to local storage (direct or SRM)
    - Inbound connectivity on some fixed network ports
      - From CERN, for CM and PM (e.g.: 8084 and 9991)
      - From World, for SES and xrootd (e.g.: 8082 and 51234)
  
  - Local data buffer for intermediate input/output of jobs (SES service)
    - Size: at least the number of job slots on the site \* 3GB
    - Not necessary if xrootd is running on the site SE (may be included in DPM)

- Agents
  - PhEDEx, PubDB tools, job output harvesting
  - Machine
    - Pentium IV 2 GHz, with 1 GB memory
    - 20 GB local disk
    - Xen or comparable dedicated virtual machine would suffice
  - Shared experiment software area
  - Connectivity
    - Login access to site-local CMS administrators
    - Outbound connectivity + access to local storage
    - *Future*: possibly inbound connectivity, assuming security is guaranteed
- Web server
  - PubDB, DLS HTTP publication
  - Access to small database server
- Database servers
  - Small database server for PubDB, DLS, BOSS
    - Modest MySQL
    - Might be in the same machine as the local file catalog
    - Should not share the agents machine
  - CMS File catalog (possibly MySQL)

- General requirements
  - Host certificated required (non-Globus, without “host/” prefix)
  - Login via gsissh (no root access required)
  - Disk space requirements: less than 25 GB
    - 20 GB for logging information, 2 GB for POOL...
  - Software
    - Basic Globus support + gLite FTS client + POOL
    - Apache + MySQL + ATLAS DDM services (DQ2 site services)
  - No requirement to access experiment software installation area
- Agents and services
  - ATLAS Distributed Data Management (DDM) services
    - Datablock subscription agents
    - Claims service and Space Management service
  - Connectivity
    - Inbound connections through Apache: Insecure and secure ports (8000, 8443)
    - Outbound http(s) access to external catalogs
    - All messages are designed to be TCP traced: XML or plain text messages.
    - Use of standard clients (FTS, RFIO, SRM)
  - Installation and management done by the experiment

- General requirements:
  - 2.4 Ghz CPU Pentium 32-bit, 1 GB memory, SLC3 OS
  - Login to local user account via gsissh
  - Mount of the experiment software installation area
  - Request Data Base (MySQL server)
    - Disk space: 20 GB minimum, 100 GB normal.
  - LCG UI software including the LFC and FTS client
  - Service certificates required for secure operations
  
- Agents and services
  - Agents (non exhaustive)
    - Request DB service: Receives and stores requests (from WNs) for various operations
    - Transfer Agent: Performs data transfers via FTS, 3<sup>rd</sup> party GridFTP, SRM
    - Monitor Agent: Publishes information reported by jobs running at the site
  - Connectivity
    - Outbound connectivity required
    - Inbound connectivity only from the local Worker Nodes
  - Run using *runit* service control tools
    - Running in the user space
    - But small addition to the *inittab* will be necessary to start agents at boot