Towards CREAM – Argus integration

Massimo Sgaravatto – INFN Padova
On behalf of the CREAM team

Authorization in CREAM

- **Authorization in CREAM now implemented via gJAF**
  - Allows to manage authorization based on VOMS attributes (voms-pdp) or on DNs (gridmap-pdp)
  - Also possible to ban specific DNs (banner-pdp)
- **Implemented by EGEE security cluster**
- **Official authorization solution for the Java world in EGEE**
- **Not maintained anymore by JRA1 security cluster for lack of resources**
- **→ "Imported" in CREAM code (just the part relevant for us) and now maintained by the CREAM team**

Credential mapping and gridftp

- **Credential mapping**
  - To map Grid credentials on local accounts and execute commands on behalf of these local accounts
  - Implemented via glexec
  - Glexec makes use of lcas and lcmaps
- **Gridftpd**
  - Gridftp server running on a CREAM CE
  - Used for proxy renewal (fresh proxy pulled from the job wrapper running on the WN, as for the LCG-CE), for staging of input sandbox (ISB) files, for publishing VO tags
  - Gridftpd makes use of lcas and lcmaps
  - Same grid and group mapfiles, but different configuration files wrt the ones used by glexec

Issues with existing solution

- **So different authorization mechanisms used within a CREAM CE**
- **Because of misconfigurations/bugs/…, inconsistent decisions could be taken**
  - E.g. gJAF grants you access, while lcas doesn't
  - E.g. gridftpd and glexec map you to different local users
- **→ single authorization service needed**
- **… and this is the new gLite Authorization Service (Argus)**

CREAM and Argus integration

- **CREAM and ARGUS integration discussed between CREAM and Argus developers + Maarten**
- **Agreed to perform such integration in 2 steps:**
  1. glexec → sudo
     - *Replace glexec calls with sudo calls*
     - *Use glexec just once per job submission (to get the localid to be used in the sudo calls)*
  2. Integration with Argus
     - *Argus used as authorization service (the only one)*
     - *Allows to address the previously mentioned issues*

Glexec → sudo (1st step)

- Discussions if we could replace glexec calls with sudo ones
- Pros
  - Reduced authorization calls
  - Improved performance
  - Facilitate CREAM – ARGUS integration
- Cons
  - glexec requires the possession of a valid proxy; this is not the case with sudo
  - sudo cannot force 'tomcat' to switch to the exact account to which glexec would have mapped the proxy
- Since no unanimous consensus found, issue raised at the MWSG and SCG (thanks to Christoph)
- This was discussed at the MWSG and then to SCG, who eventually approved this glexec → sudo switch

Glexec → Sudo (1st step)

- **What is needed**
  - Plugin in CREAM to get (via glexec) the localid (to be then used for sudo)
    - Done, to be tested
  - BLAH sudo aware
    - Done, being tested
  - CREAM integration with sudo-aware BLAH (TBD)
  - CREAM using sudo instead of glexec for the non-BLAH operations (TBD)
  - Needed changes in yaim, e.g. sudoers creation (TBD)
- **Will be released with CREAM CE release 1.6 (patch #3179): ~ October 2009**

Integration with Argus (2nd step)

- **Argus will be used as the only one authorization service**
  - Besides deciding if a certain operation is authorized, it will also tell the mapped local user
    - To be used in the sudo calls
- **Remove gJAF, glexec (and also LCAS and LCMAPS) from the CREAM CE**
  - → Reduced dependencies
- **Prerequisites**
  - Glexec → sudo (1st step)
  - Gridftpd also integrated with Argus
    - Implemented by Valery
    - Successfully performed some tests
  - Argus functionality and performance successfully demonstrated in the glexec on WN use case
    - Argus patch (#3076) now in certification
- **Timeline: CREAM CE release 1.7 (January 2010)**

3rd phase

- **Use of ARGUS to manage more complex authorization policies**
  - E.g. CREAM has the concept of super-user, who can manage jobs submitted by other users, and can perform some special operations
    - This could be managed via Argus
  - E.g. allows user X to manage jobs of VO Y
  - …

Other info

- **Glexec → sudo (1st step)**
  - https://savannah.cern.ch/task/?9557
- **Full CREAM-Argus integration (2nd step)**
  - https://savannah.cern.ch/task/?7746
- **CREAM web page**
  - http://grid.pd.infn.it/cream