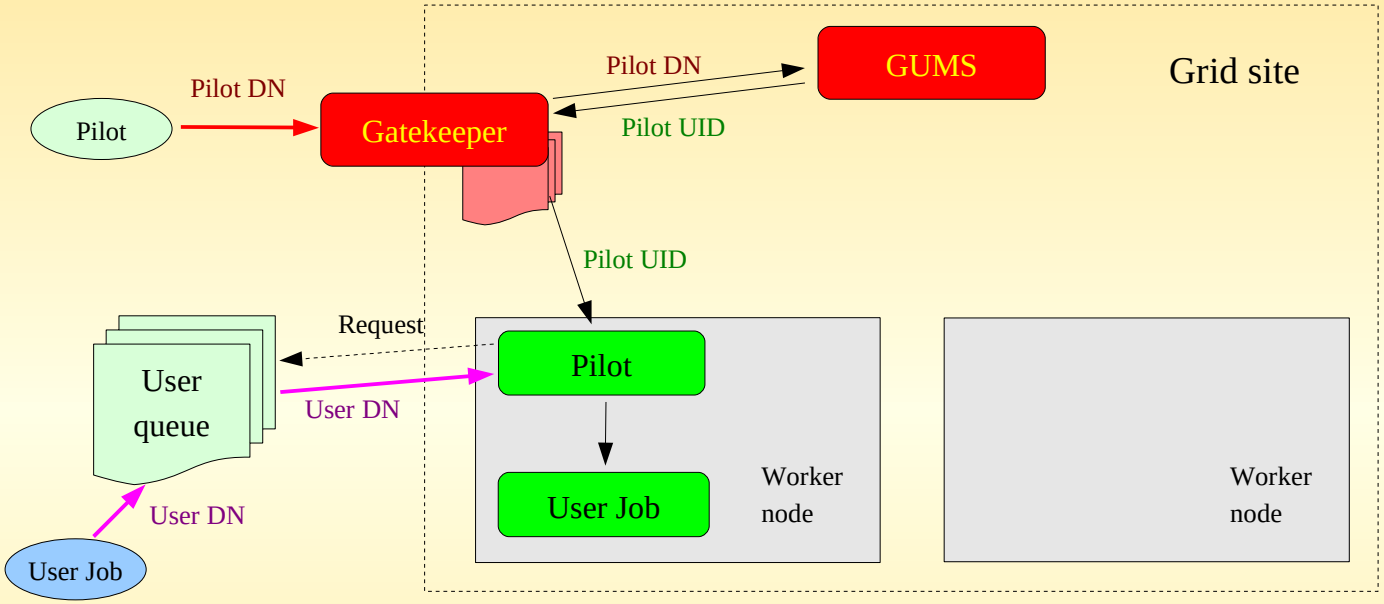
Middleware Security Group Meeting

gLExec

Experience with integration

by Igor Sfiligoi - FNAL

Pilot jobs in the Grid



Site problem

Grid site knows nothing about user jobs

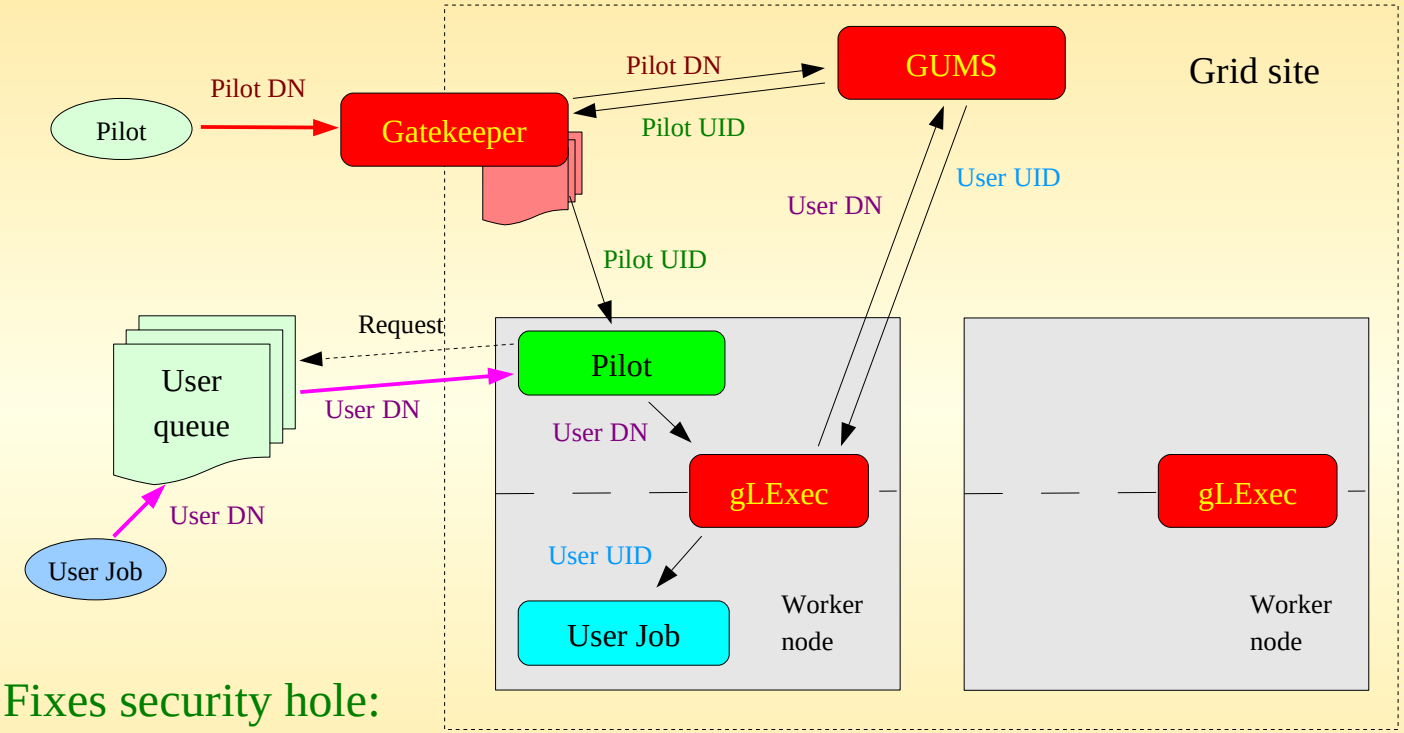
- All jobs run using the pilot credentials
- Must trust the pilot for all fine grained authorization and for monitoring

Pilot problem

Pilot faces a security security hole:

- User job and pilot job run under the same UIDs
  - User job can access the pilot job files (in particular the pilot proxy)
  - User job can manipulate pilot jobs (kill them or attach a debugger)

gLExec on the WN



Fine grained authorization

- User must be mapped, thus authorized, before executing

Site gains

Fixes security hole:

- User job and pilot job run as different UIDs
  - User job cannot access the pilot job files (in particular the pilot proxy)
  - User job cannot manipulate pilot jobs

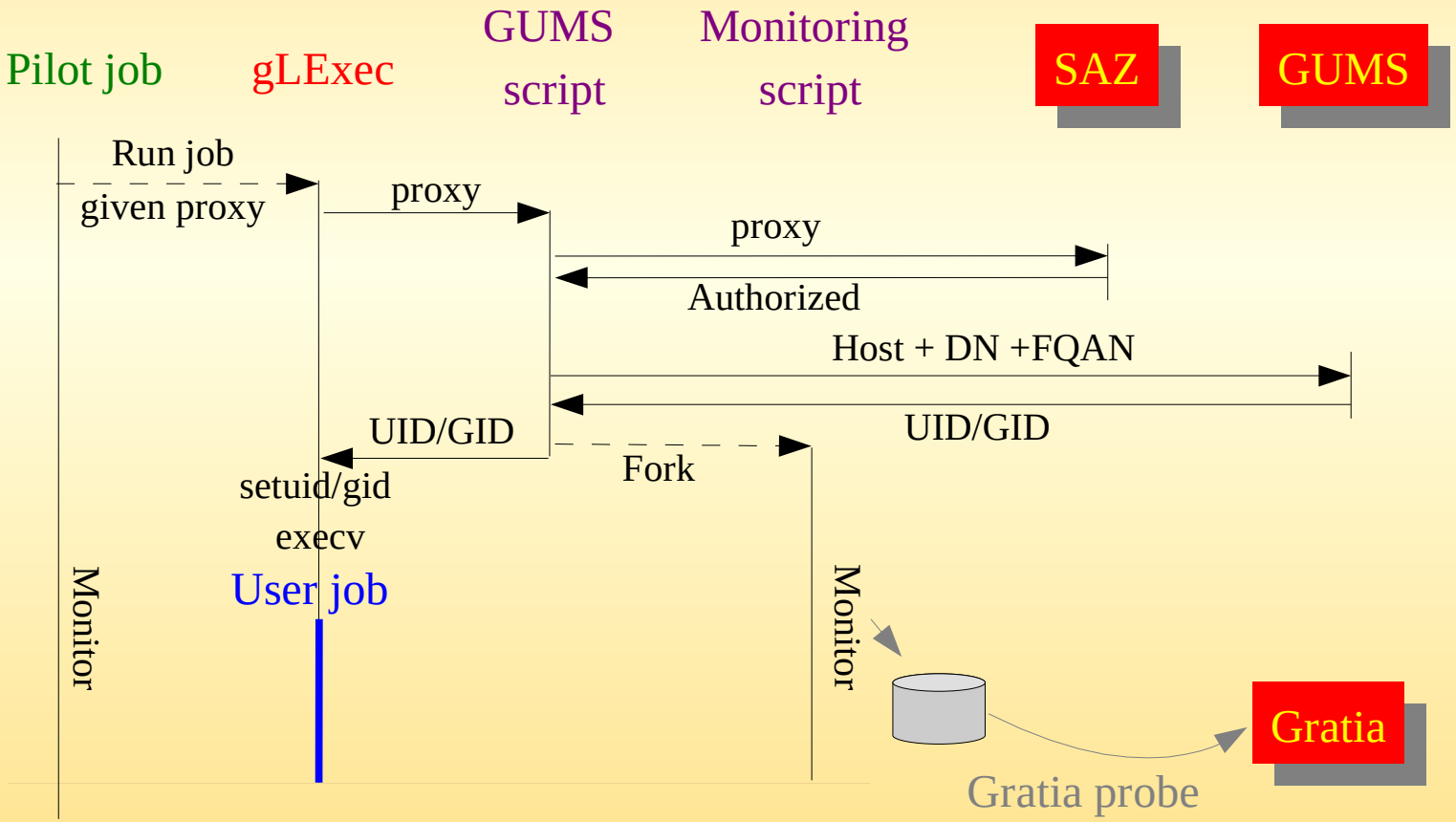
Pilot gains

gLExec on WN development

- NIKHEF developers provided a callout plugin for gLExec that forwards the full user proxy via a pipe
- FNAL team provided a script that processes the proxy, calls GUMS and returns the local mapping via the reverse pipe
  - Same script also calls SAZ and provides log information to Gratia

GUMS plugin script

- Actually does more than contacting GUMS



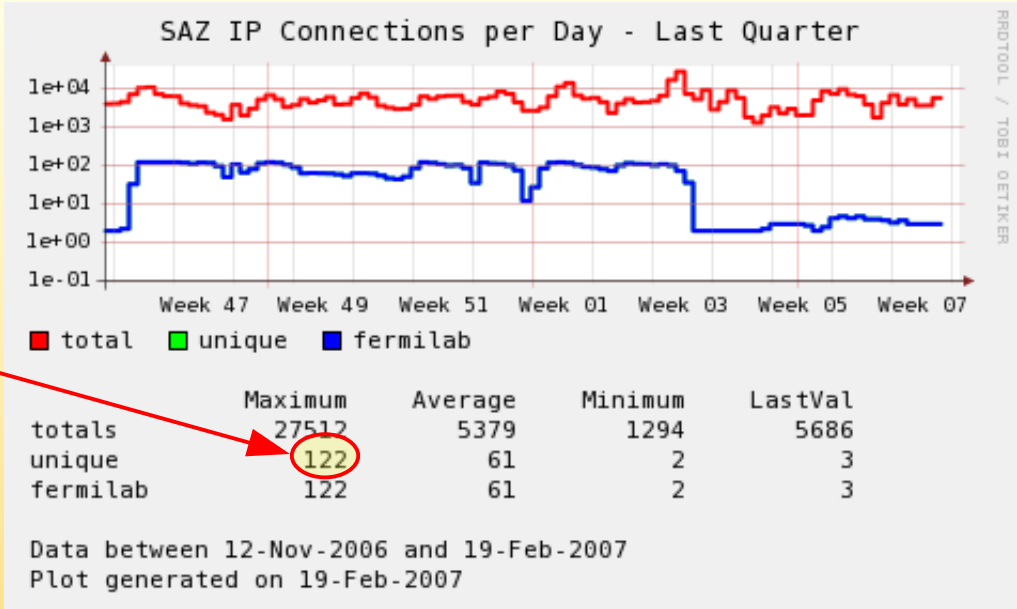
gLExec @ FNAL

- All software packaged as RPMs
  - Deployed on most of the FNAL worker nodes
- Client needs host certificate to talk to GUMS
  - at FNAL we make a short lived (few hours) host proxy of the gatekeeper and copy it to all the worker nodes several times a day
  - krb5 used for authentication

gLExec @ FNAL

- CDF using gLExec in production for few months
  - With Condor v6.9.1 glideins
  - Found a problem with Condor CoD (used in CDF for monitoring)
    - Crashing startd when used with gLExec
    - Waiting for fix from Condor group before re-start using gLExec

Used on
120 WNs



gLExec outside FNAL

- Two major problems:
  - Host proxy distribution is FNAL specific (KRB5)
    - OK for sites with host certificates on WN (very few)
    - Other secure copy mechanisms needed
  - Software not distributed via VDT
    - OSG usually distributes software via VDT
    - Maybe not a real problem?

Future development

- Better packaging
  - Add support for non-krb5 distribution of host proxies
    - Need feedback from Grid sites
  - Distribute gLExec + GUMS script via VDT
- Improve error messages
- Centralize management

Conclusions

- gLExec on WNs a reality at FNAL
  - was used for several months by real users
  - no major issue found with gLExec
- Ready to be pushed to other Grid sites
  - but packaging needs to be improved