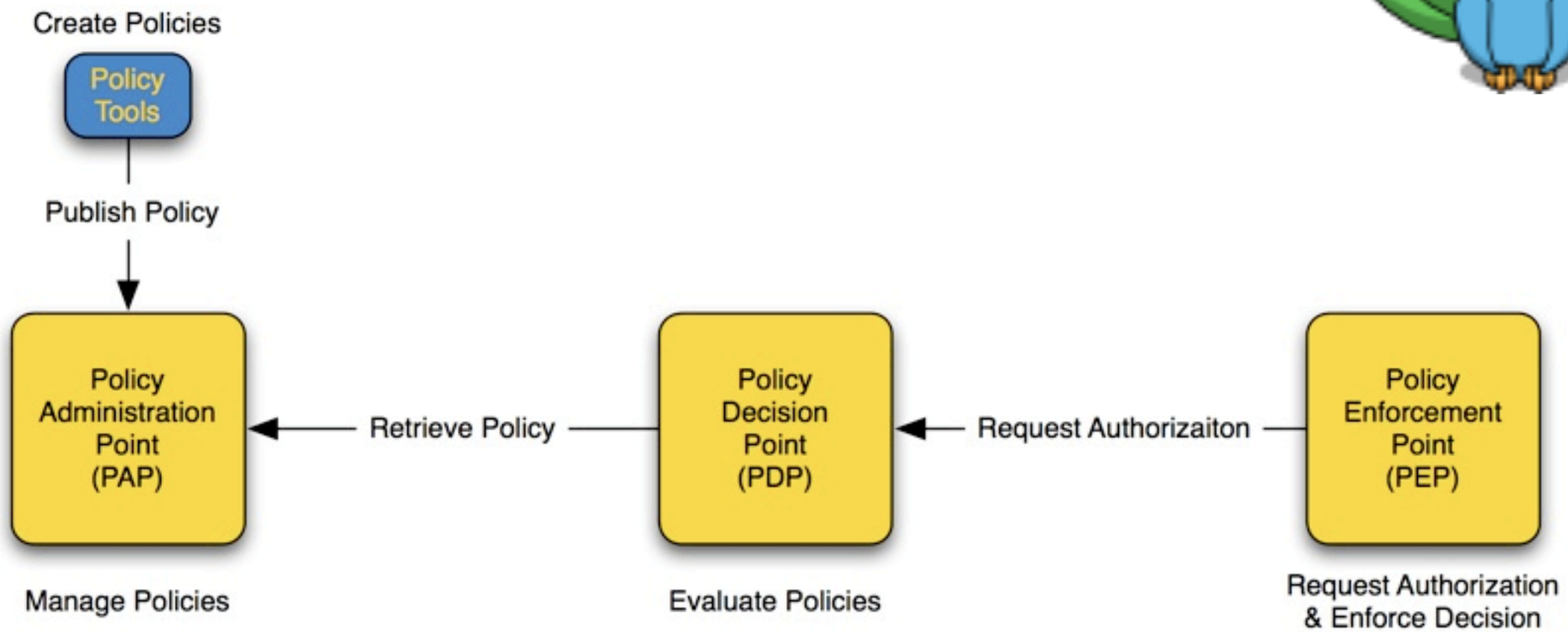
Argus central banning list for WLCG

Stefan Lueders & Romain Wartel, CERN IT.

OSCT meeting, Nikhef, 22th March 2010

Introduction to Argus

- **Argus is a system meant to render consistent authorization decisions for distributed services**
  - Author and maintain authorization policies (PAP)
  - Authored policies must be evaluated (PDP)
  - Authored policies are enforced (PEP)



https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework

Central banning

- **Highly desirable feature to contain security incidents**
- **Draft security policy available:**
  - http://www.jspg.org/wiki/Statement_on_Global_Banning_of_Users
- **Technical requirements**
  - A central service (PAP)
  - Argus client on glexec-WN
- **Operations**
  - The central PAP publishes the list of banned entities
  - The Argus clients trusting this PAP implement the policy
- **Limitations**
  - Currently no support outside of the WNs (storage, etc. not covered)

Running a central Argus service

- WLCG has to support a central PAP
- CERN runs a pilot service at argus.cern.ch

root@lxbrb1808:~ — ssh — ttys000 — 118×21

root@lxbrb1808:~ — ssh

```
[root@lxbrb1808 ~]# /opt/argus/pap/bin/pap-admin --host argus.cern.ch lp

default (local):

resource ".*" {

    action ".*" {
        rule deny { subject-issuer="CN=QuoVadis Grid ICA,OU=Issuing Certification Authority,O=QuoVadis Limited,C=BM" }
        rule deny { subject-issuer="CN=QuoVadis Grid ICA,OU=Issuing Certification Authority,O=QuoVadis
Limited,C=BM" }
        rule deny { subject-issuer="C=BM,O=QuoVadis Limited,OU=Issuing Certification Authority,CN=QuoVadis Grid ICA" }
        rule deny { subject="CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate,O=INFN,C=IT" }
    }
}
[root@lxbrb1808 ~]#
```

- All sites testing Argus can use this central PAP
  - Banned DNs from real incidents will be added by the CERN CERT

Future of the service

- **CERN is happy to provide a central PAP for WLCG**
  - Will remain at argus.cern.ch
  - Maintained by the CERN CERT

- **Who should have admin access to Argus?**
  - All NGIs security officers?
  - EGI/OSG/WLCG security officers?
  - CERN CERT staff only, acting on request from the relevant CSIRTs?

- **Possible issues:**
  - SLA, downtime?
  - Required response time?
  - On-site backup available, do we need an off-site copy at another site?