Logging & Bookkeeping: Security Recommendations

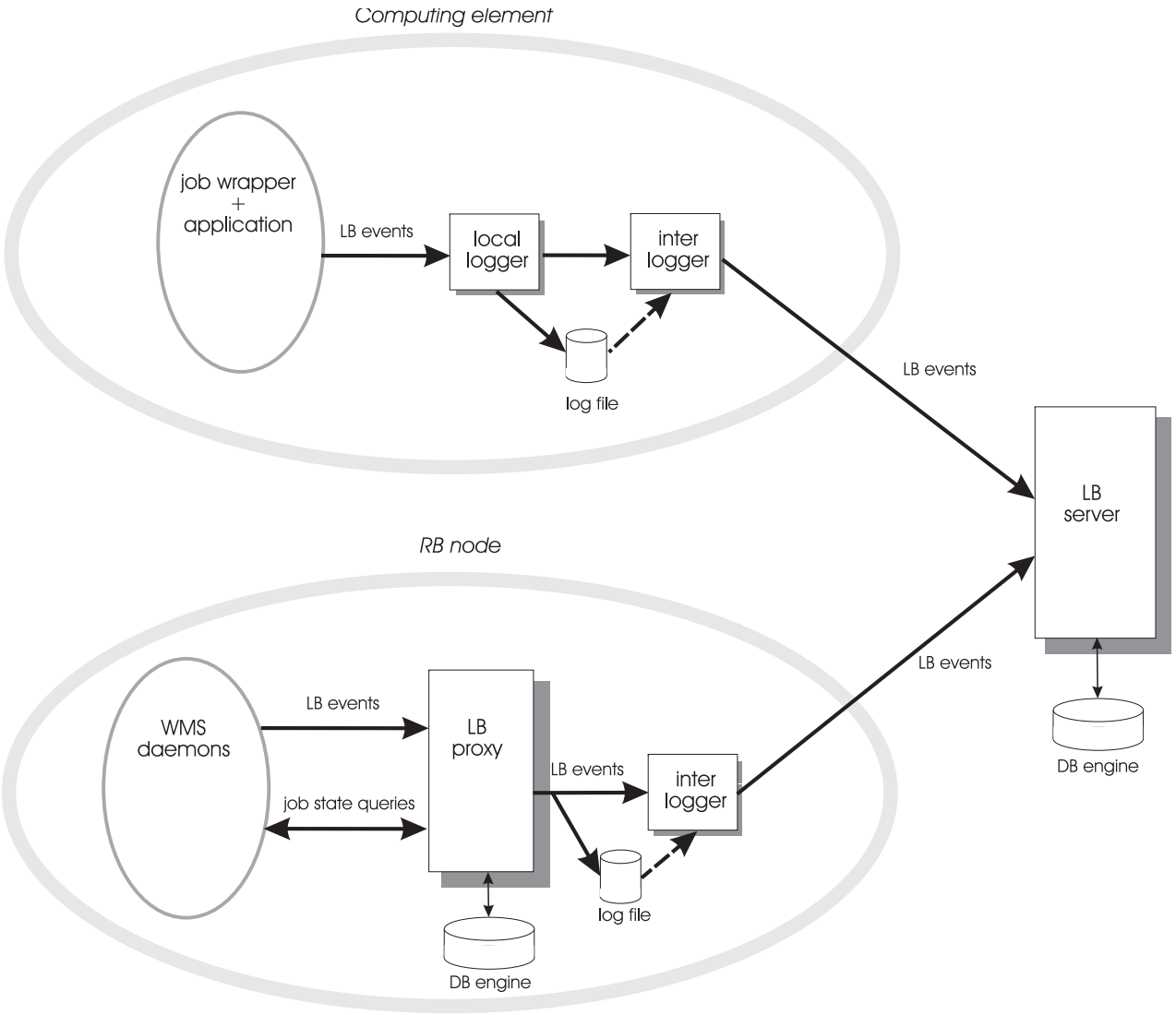
Daniel Kouril, CESNET

EGEE08

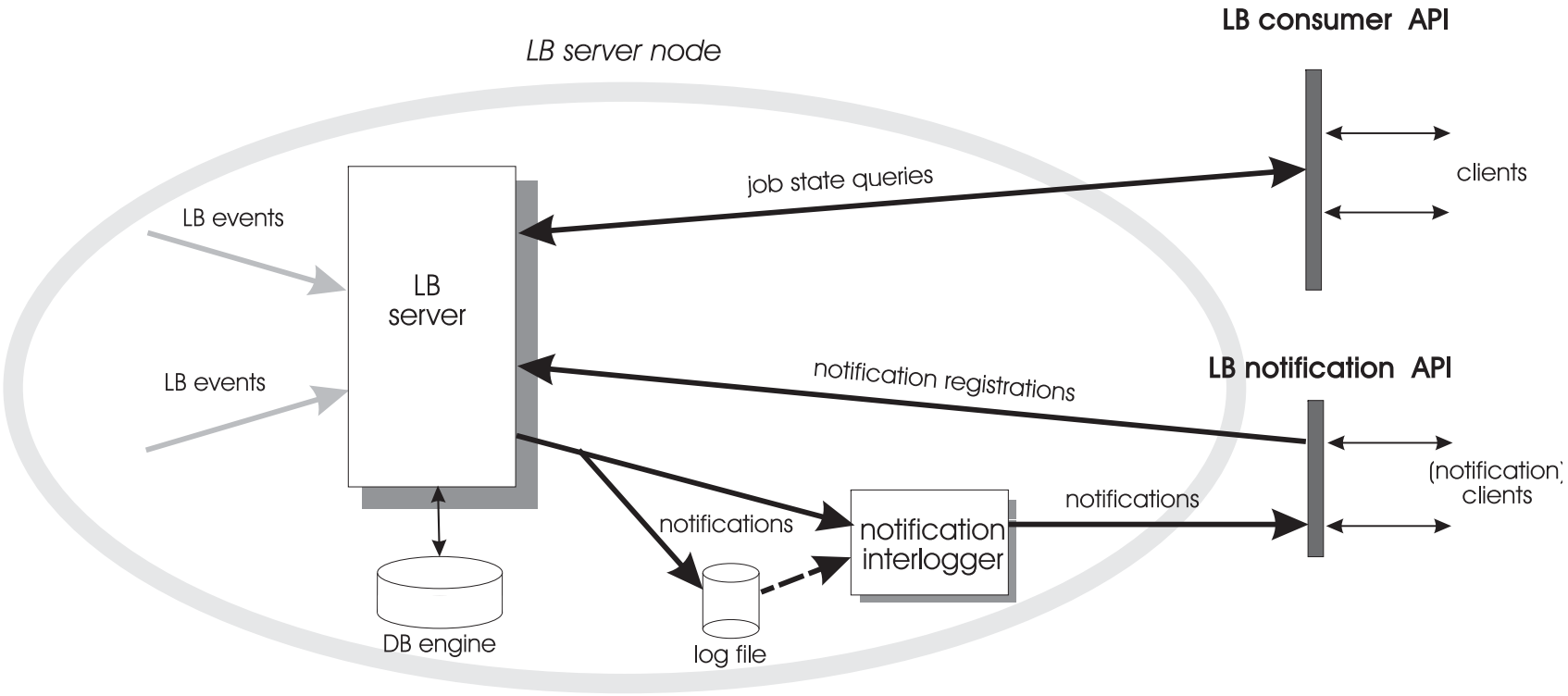
LB Overview

- **LB collects *events* from individual Grid components**
  - information about important point in the job‘s lifetime
    - transfer between WMS components, start runnning, done, ...
  - events sent as messages to the LB server
  - Based on events arrived LB server computes current job status
- **Own LB messaging infrastructure**
  - secure (protection, authN) and reliable (fault-tolerancy)
    - LB notifications use this messaging infrastructure too
  - events are tied with job (using the jobid)
    - job registration
- **Push model**
  - events are sent by the components (mostly WMS) upon changes

LB Architecture – Events gathering



LB Architecture – Retrieving data



Operating LB components

- **No need for administrative rights**
- **no user accounts needed**
  - just a “service” account used for daemons – usually *glite*
- **All network connections secured using SSL**
- **Logging messages using syslog**
  - /var/log/messages
  - lines always contain name of the process
- **Starting/stopping the daemons using init.d scripts**
  - /opt/glite/etc/init.d/glite-lb-*

Operating LB logger node

- **composed of entry point (logd or proxy) and LB interlogger (*glite-lb-interlogd*)**
- **outbound connectivity to LB server(s)**
- **files with events stored on disk before delivering to LB server**
  - /var/glite/log/dglogd.log*
- ***glite-lb-logd***
  - TCP port 9002, accepts connections from clients (job)
  - availability depends on clients' need, usually one-catch all logd on WMS
- ***glite-lb-proxy***
  - local daemon on WMS
  - no public network interface, only local unix socket

Operating LB server

- **LB server (*glite-lb-server*)**
  - TCP ports 9000 (queries) and 9003 (WS queries)
    - used by users
  - TCP port 9001 (event gathering)
    - connections from logger nodes
- **mysql DB R/W access**
  - tables created on installation
- **Purging DB**
  - regular purging necessary to avoid overloading db
  - CLI and cron script provided (*glite-lb-purge*)
    - different purging timeouts for different job states
  - purging triggered remotely or locally, purged data are stored on local filesystem on server
  - purged data about jobs should be archived sufficiently long

Operating LB server

- **LB super-users can access any data on LB server**
  - Normal users can only access their job information unless ACL is used
  - specified in the LB server configuration (-R/-F)
  - using X.509 DNs or VOMS attributes
- **Notification interlogger (*glite-lb-notif-interlogd*)**
  - runs on the LB server node
  - sends out messages to subscribers when necessary
  - no public network interface
  - started/stopped together with LB server

Addressing Incidents

- **stop daemons**
- **check logs**
- **consider possible tampering/faking of job events**
  - job status data may not be reliable
- **check temporary job event files on loggers**
  - verify they contain valid LB server name(s)

Tracing jobs using LB

- **LB keeps complete history of jobs submitted via WMS**
- **useful information for tracking jobs**
  - what CEs have been used during last X hours by particular user
- **OSCT/JRA1 is working on a CLI tool to ease the information retrieval**

```
trace_jobs.sh "/DC=cz/DC=cesnet-ca/O=Masaryk University/CN=Daniel Kouril" skurut1.cesnet.cz \
    2008-06-22

https://skurut1.cesnet.cz:9000/0CUi8_1eoBRavGkoAqSafQ (Submitted):
     submitted to skurut68-1 WMS on Thu Jul  3 14:32:36 2008

https://skurut1.cesnet.cz:9000/5QsEfMN7GIJoUPF5ew234f (Done):
     submitted to https://195.113.219.85:7443/glite_wms_wmproxy_server WMS on Mon Jun 23
    16:43:01 2008
     CE used: grid012.ct.infn.it:2119/jobmanager-lcglsf-auger

https://skurut1.cesnet.cz:9000/Gm4UnWFessxw2cKgrN0bCg (Aborted):
     submitted to https://195.113.219.85:7443/glite_wms_wmproxy_server WMS on Mon Jun 23
    16:42:41 2008

https://skurut1.cesnet.cz:9000/PaeU3rrS9j-XxDsAczA6-g (Cleared):
     submitted to https://195.113.219.85:7443/glite_wms_wmproxy_server WMS on Sun Jun 22
    18:13:39 2008
     CE used: grid012.ct.infn.it:2119/jobmanager-lcglsf-auger
              golias25.farm.particle.cz:2119/jobmanager-lcgpbs-gridauger
```