Security Recommendations WMS

Francesco Giacomini

EGEE'08 - Istanbul

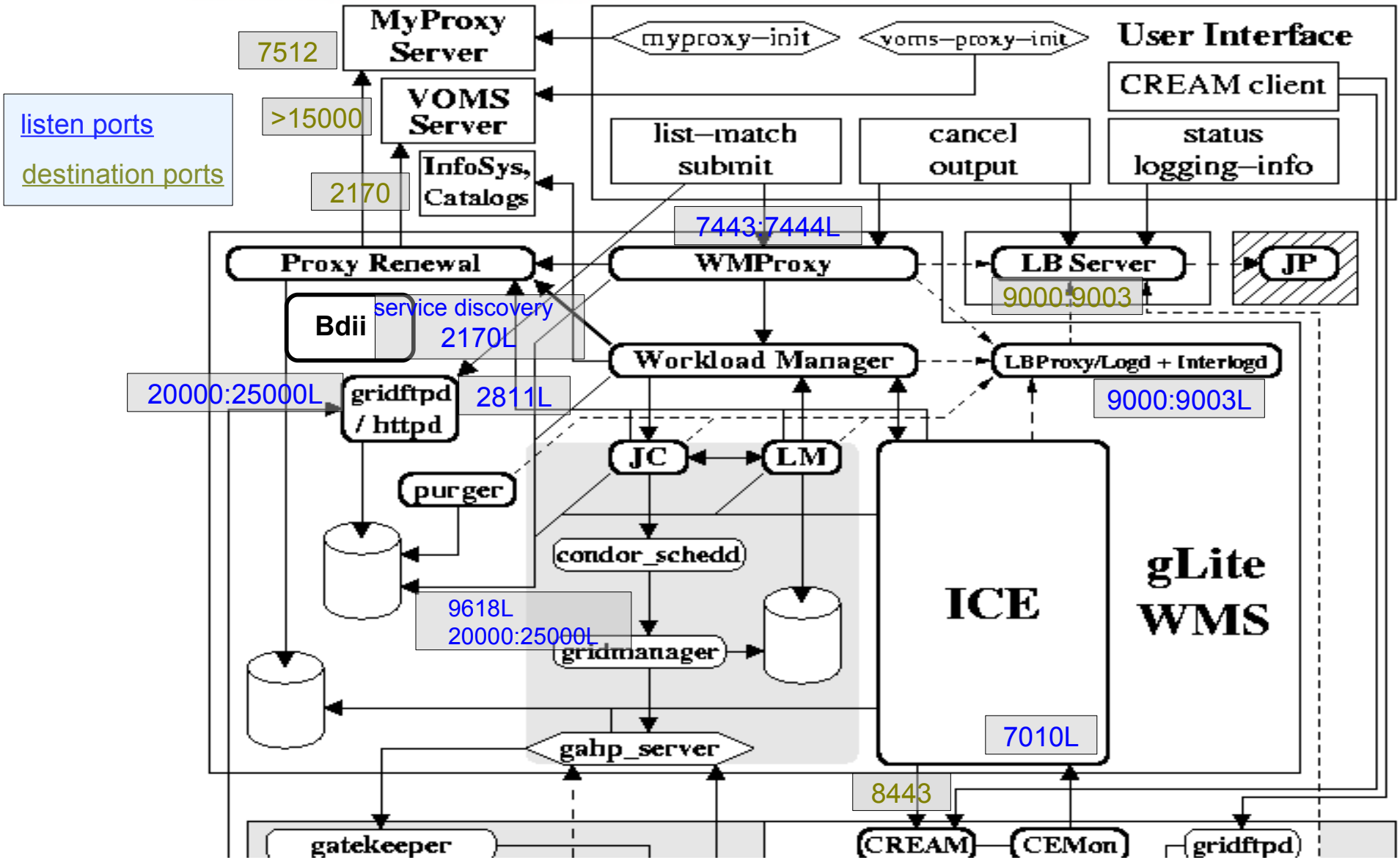
WMS Network Usage /1

- **The WMS internal components listen to a variety of incoming messages from different external sources**
  - SOAP over HTTPS, based on Apache/GridSit, for job management requests
  - GridFTP for sandbox management
  - services that submit jobs to CEs (Condor, ICE) listen for notifications from CEs (LCG-CE, CREAM)
- **Ports:**
  - 7443, 7444 (httpd ports: listen to incoming requests for computation)
  - 9618 (condor_collector process)
  - 20000-25000 (other condor related processes, i.e. negotiator, schedd, gahp server, ...)
  - 9000-9003 (glite-lb-* LB processes)
  - 2811 (gridftp control port)
  - 20000-25000 (gridftp data ports)
  - 2170 (bdii-fwd process: service discovery)
  - 7010 (ICE: notifications from CEMon)

WMS Network Usage /2

- **The WMS connects to a variety of external services to peform its job management operations**
- **Destination ports:**
  - 7512 (MyProxy server)
  - >15000 (VOMS server)
  - 2170 (BDII)
  - 9000-9003 (LB server)
  - 8443 (CREAM CE)

WMS Network Usage /3



WMS Log Files

- **Most log files are located in ${GLITE_LOCATION_LOG}**
  - httpd-wmproxy-errors.log
  - httpd-wmproxy-access.log
  - wmproxy.log
  - workload_manager_events.log
  - jobcontoller_events.log
  - logmonitor_events.log
  - ice.log
  - glite-wms-wmproxy-purge-proxycache.log
  - lcmaps.log
  - glite-wms-purgeStorage.log
- **But also:**
  - /var/log/messages - used, for example, by the LB proxy and the proxy renewal daemon
  - /var/local/condor/log/ - the Condor log directory
  - /var/log/gridftp-session.log
  - /var/log/globus-gridftp.log

WMS AuthZ

- **WMS authorization is managed by GridFTP and GridSite with two different mechanisms**
  - GridFTP: performed by LCAS
  - GridSite: specified by means of GACL, an XML-based formalism
- **/opt/glite/etc/glite_wms_wmproxy.gacl contains the identities (VO, user, etc) with distinct permissions (exec, read, write, ...) to use the WMS**
  - To ban a user/group/VO it is sufficient to add his/her DN/FQAN and a deny tag, e.g.:

```
<entry>
  <person>
    <dn>/C=IT/O=INFN/OU=Personal Certificate/L=DATAMAT DSAGRD/CN=John
   Doe</dn>
  </person>
  <deny><exec/></deny>
</entry>
```

Delegation & Proxy Renewal

- **The WMS performs job related operations on behalf of the user**
  - To do so it needs delegated credentials by the user
  - Delegated credentials are kept in the root of the job sandbox area
- **A user can ask that the delegated credentials be renewed**
  - This is done registering the credentials with the Proxy Renewal daemon

How to Start and Stop the Service

- **For the WMS as a whole**
  - service gLite { start | stop | restart | status | version }
- **Each single service has its own start/stop script**
  - /etc/init.d/globus-gridftp { start | stop | restart | status }
  - /opt/glite/etc/init.d/glite-wms-wmproxy { start | stop | restart | status }
  - /opt/glite/etc/init.d/glite-wms-wm { start | stop | restart | status }
  - /opt/glite/etc/init.d/glite-wms-lm { start | stop | restart | status | check }
  - /opt/glite/etc/init.d/glite-wms-jc { start | stop | restart | reload | status | check } [JobController|CondorG]
  - /opt/glite/etc/init.d/glite-wms-ice { start | stop | restart | status }
  - /opt/glite/etc/init.d/glite-proxy-renewald { start | stop | restart | status }
  - /opt/glite/etc/init.d/glite-lb-proxy { start | stop | restart | status }
  - /opt/glite/etc/init.d/glite-lb-locallogger { start | stop | restart | status }