



# EDG Package Spitfire

Installation, Configuration, Examples of use

legre@clermont.in2p3.fr

- ◆ Obtain host certificate and key from your CA (if you have already one for your DataGrid gatekeeper, you don't have to do it again)
- ◆ Download the latest version of Spitfire available on the code repository <http://datagrid.in2p3.fr/distribution/datagrid/wp2/>



- ◆ Spitfire provides a set of grid enabled middleware services for access to relational databases.
- ◆ Currently, it consists of the SQL Database Service.
- ◆ In addition, the jwget tool is provided for client side command line usage
- ◆ In the near future the ServiceIndex and a fine grained authorization mechanism will be added



- ◆ You can find complete explanation about installation and configuration in the README file included in the bundle and on the following url:  
<http://www.cern.ch/hep-proj-spitfire>
- ◆ Installation is really easy to do... you just need to execute one command !  
`rpm -ivh spitfire-bundle-<version><release>.<arch>.rpm`
- ◆ This will create a /opt/spitfire-bundle/ directory tree (you can specify another location using the --prefix option).
- ◆ It's not an obligation to install it as root...but it's an easiest way...
- ◆ create a special user named spitfire and give him the recursive ownership of the /opt/spitfire-bundle directory (it's not an obligation, just an advise).  
`chown -R spitfire.<mygroup> /opt/spitfire-bundle`

**Installation Complete !!!!**



## Configuration (1 / 2)

- ◆ As root, modify your path in your /etc/profile file like this

```
export PATH=$PATH:/opt/spitfire-bundle-1.0.1/share/spitfire/bin
```

- ◆ To configure the Tomcat Server as root you need to use a trick.

Create a /root/globus directory, then create links on your host cert and key location (in the example below we assume that they're in the /etc/grid-security directory).

```
mkdir globus
cd globus
ln -s /etc/grid-security/hostcert.pem usercert.pem
ln -s /etc/grid-security/hostkey.pem userkey.pem
```

- ◆ after that you need to reinitialize the keystore and truststore, so run... `tomcat-init-certs.sh`



## Configuration (2 / 2)

- ◆ Now you can start (or restart) your tom cat server by using the `tomcat-startup.sh` (or `tomcat-restart.sh`) command
- ◆ As user `spitfire` launches mysql using `mysqld` & command
- ◆ After this step the configuration is finished for system administrators, now it's final users turn...
- ◆ Once tomcat and mysql are up and running you can use `jwget`, or other http tools and APIs to query, insert, update, delete, from / to a database.
- ◆ Each user needs to configure `jwget` once, in order to trust the `spitfire` tom cat server. For that, runs the `jwget-initcacerts.sh`



## Let's go ! (3 quick examples)

- ◆ To run the following tests you need to have a valid grid-proxy running

```
jwget --grid-proxy https://localhost:8443/examples/servlet/  
HelloWorldExample'
```

```
jwget --grid-proxy https://localhost:8443/sqlDb/demo/showTableXsql  
?table=repCat'
```

```
jwget --grid-proxy https://localhost:8443/sqlDb/demo/getPFNsWithXsql?  
Lfn=lfn://cms.org/file1&table=repCat'
```

- ◆ Now we need to perform bigger and more efficient tests...