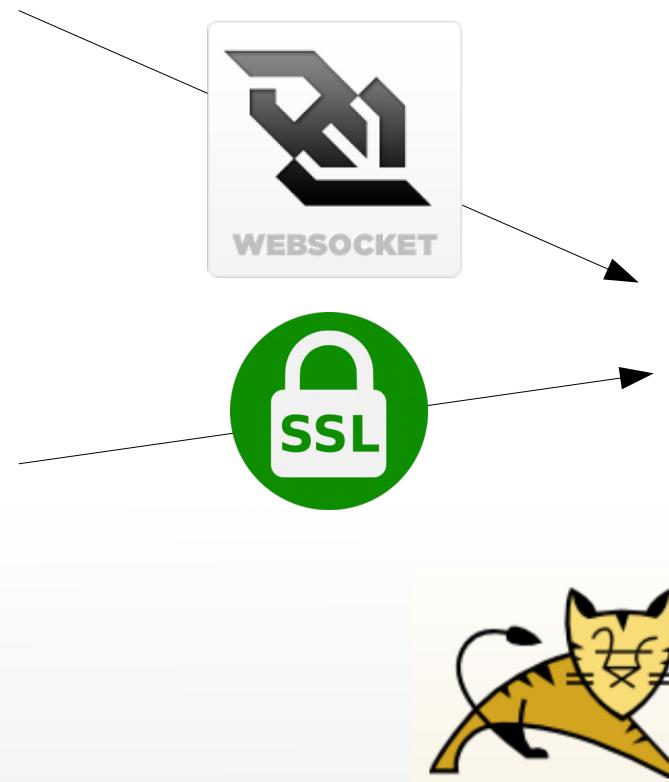


jAliEn client development

What is jAliEn client?

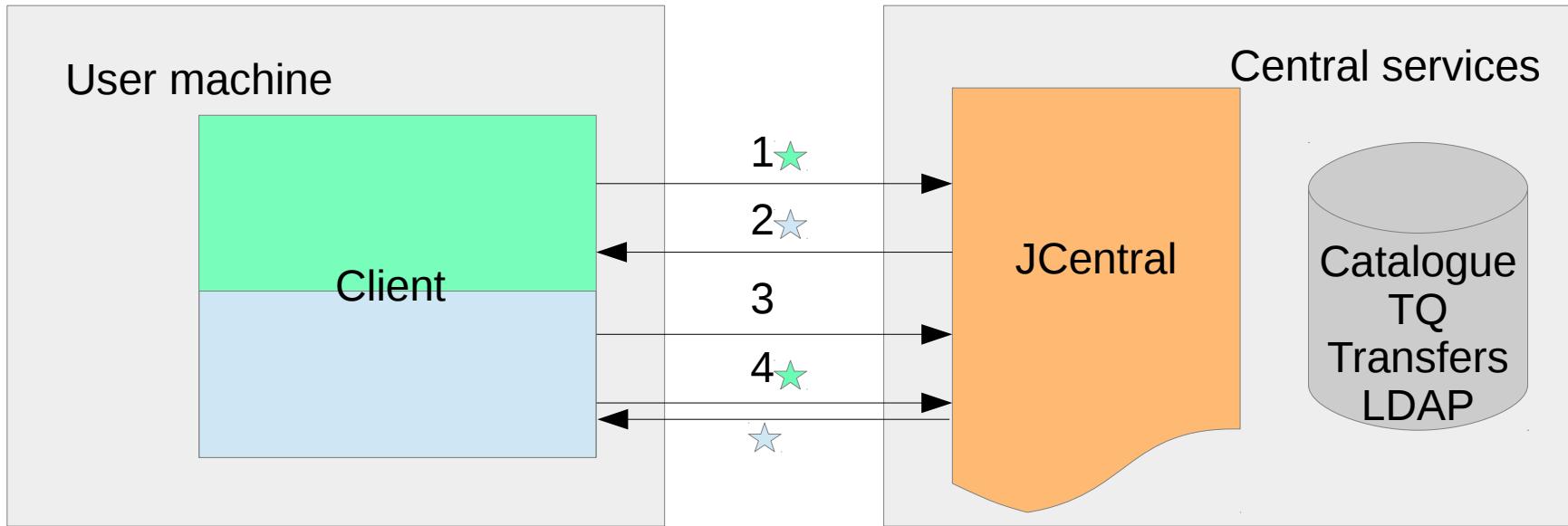


JCentral

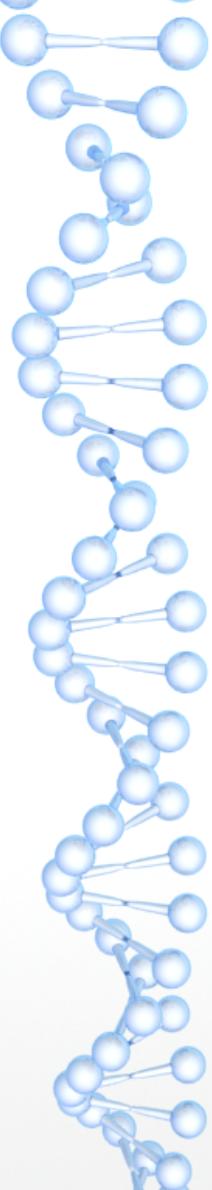


Apache Tomcat®

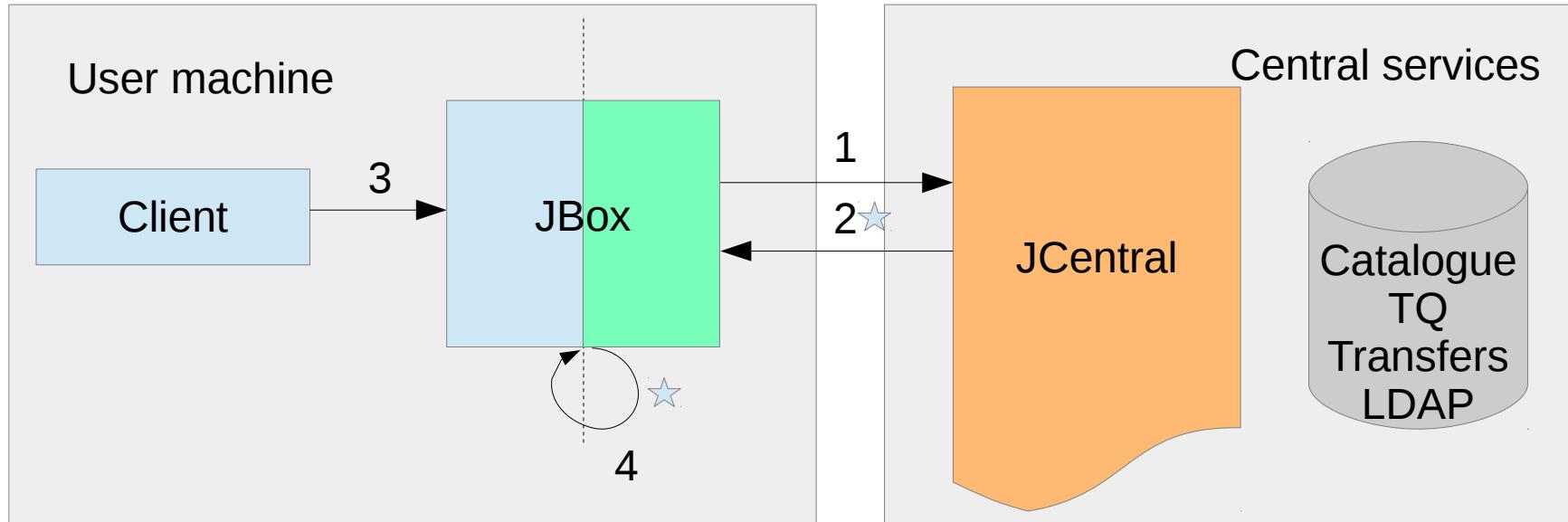
Introducing tokens



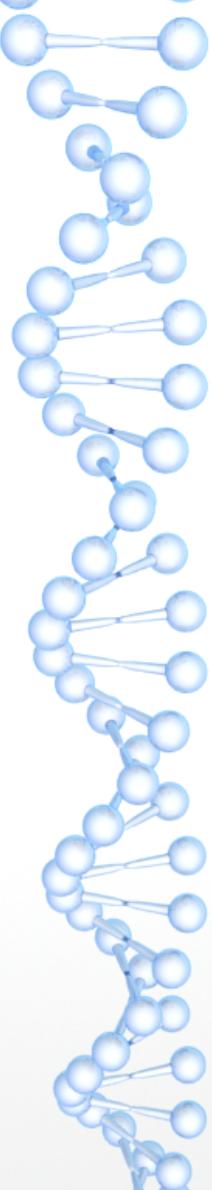
1. Initial connect with usercert
2. Get token
3. New connection with token (valid for 2 days)
4. Renew manually with **token** command



Long living authentication agent on the user machine (JBox)



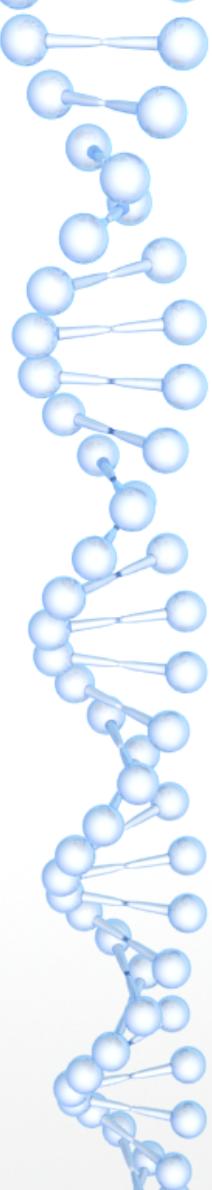
1. Initial connect with usercert
2. Get token
3. Client always uses token
4. Renew automatically every 2 hours



Defining priorities for certificates

- 1) If \$JALIEN_TOKEN is set, use token
- 2) Client cert from \$X509_USER_CERT or
\$homedir/.globus/usercert.pem
- 3) Host cert from *\$homedir/.globus/hostcert.pem*
- 4) Token from *\$homedir/.globus/tokencert.pem*

(locations can be configured in config.properties)



Switching users

```
gGrid->Command("token -u tutor");
```

AlienPrincipal

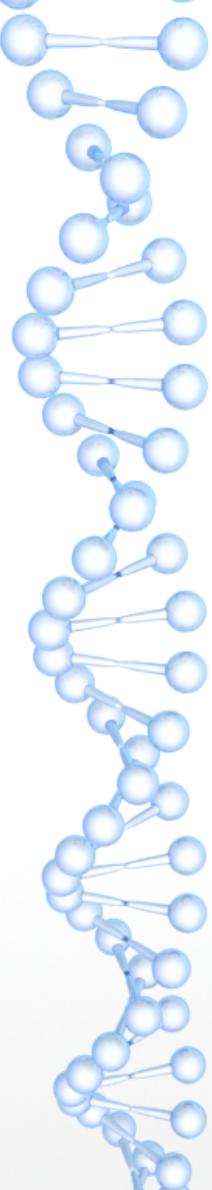
```
String username = "vyurchen";
String defaultUser = "vyurchen";
Set<String> roles = ["vyurchen",
"tutor", "..."];
```

canBecome(**final** String role)

AlienPrincipal

```
String username = "tutor";
String defaultUser = "vyurchen";
Set<String> roles = ["tutor"];
```

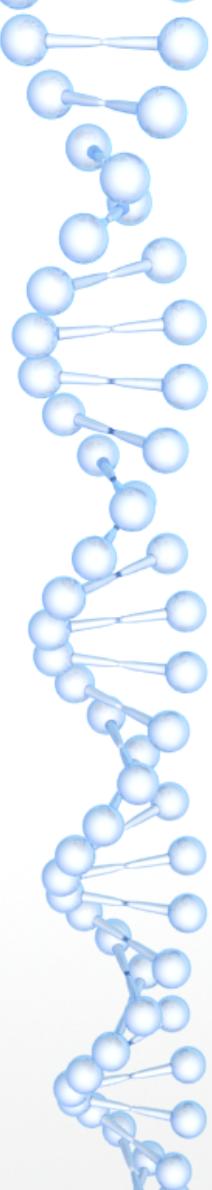
Account for 0 (/DC=ch/DC=cern/OU=Organic
Units/OU=Users/CN=vyurchen/CN=758460/CN=Volodymyr Yurchenko)
is: [vyurchen]
Successfully switched user from '[vyurchen]' to '[tutor]'.
6



New capabilities

mkdir as *tutor* successful for
"/alice/cern.ch/user/t/tutor/testtoken"

mkdir as *tutor* fails for
"/alice/cern.ch/user/v/vyurchen/noprivileges"



Relying on certificate

Allows to check client's certificate again in critical points

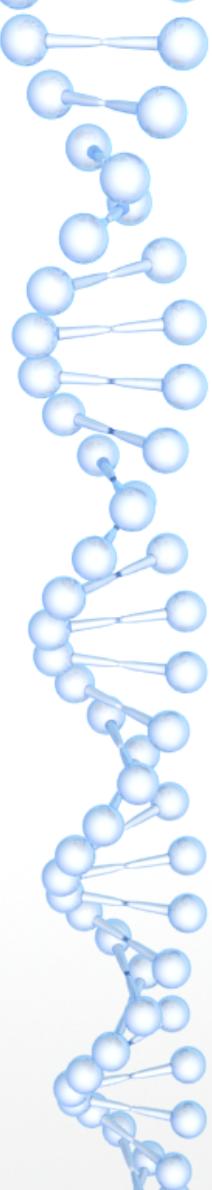
Old AlienPrincipal

```
String username = "vyurchen";  
String defaultUser = "vyurchen";  
Set<String> roles = ["vyurchen",  
"tutor", "..."];
```



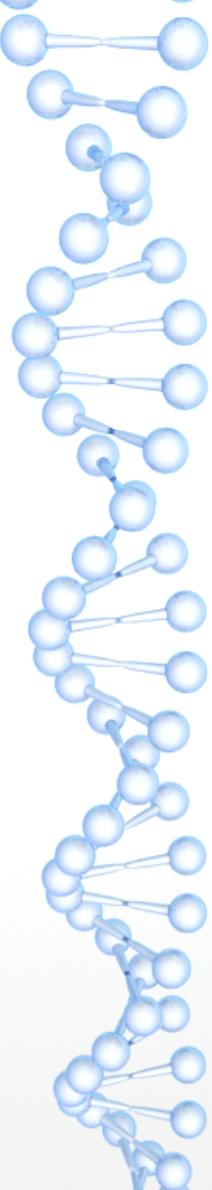
New AlienPrincipal

```
String username = "vyurchen";  
String defaultUser = "vyurchen";  
Set<String> roles = ["vyurchen",  
"tutor", "..."];  
X509Certificate[] usercert;
```



Extract information from DN

```
// Assuming we have user or job token, parse role to switch  
identity to that user  
// /C=ch/0=AliEn/CN=Job/CN=username/OU=role/OU=extension  
// ^ ^ ^ jobID  
  
...  
// if OU present in DN try to extract role  
p = getByRole(dn.substring(roleOU + 4, jobOU));  
// if second OU is present in DN  
p.setJob(Long.valueOf(dn.substring(jobOU + 4)));  
// if getByUsername or getByRole found credentials  
p.setDefaultUser(dn.substring(nameCN + 4, roleOU));
```



Updated AlienPrincipal Class

Provides a new ability to uniformly interact with central services and isolate jobs and services from executing other commands than what the respective context allows

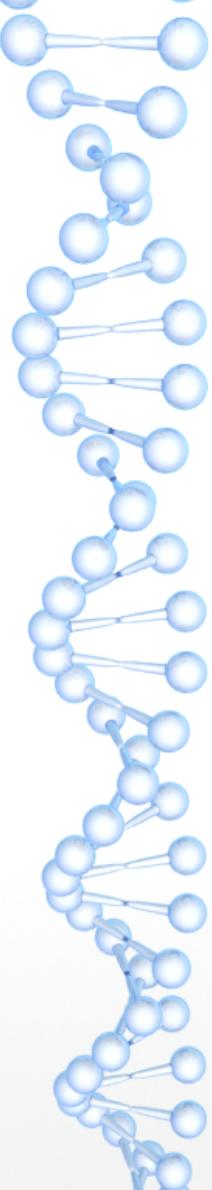
New AlienPrincipal

```
String username = "vyurchen";
String defaultUser = "vyurchen";
Set<String> roles = ["vyurchen",
"tutor", "..."];
X509Certificate[] usercert;
```



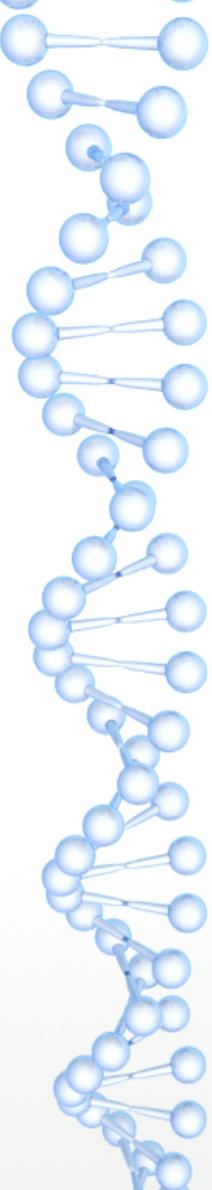
Newer AlienPrincipal

```
String username = "vyurchen";
String defaultUser = "vyurchen";
Set<String> roles = ["vyurchen",
"tutor", "..."];
X509Certificate[] usercert;
Long jobID = null;
boolean jobAgentFlag = false;
```



Killing zombies

- Server disconnects clients with uptime > 2 days, forcing them to reconnect if needed and revalidate the tokens
- TODO: discover idle clients
 - Clean up connections basing on lastUpdateTime + make it configurable
 - Use monitoring class to build charts and investigate the best interval for cleaning idle connections



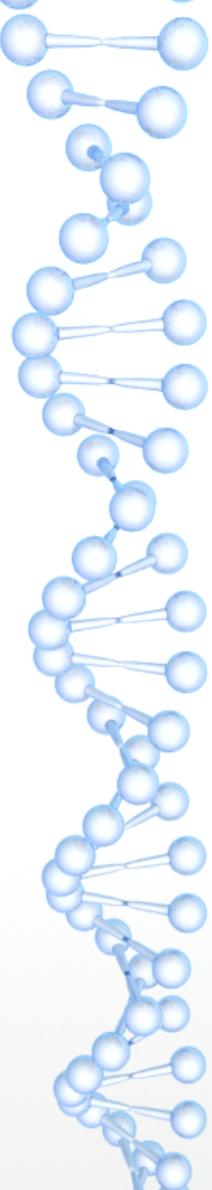
Reconnecting

```
root [5] gGrid->Ls("/alice/cern.ch/user/v/vyurchen");
```

```
Error in <TJAlien::Command>: Connection is broken,  
retrying...
```

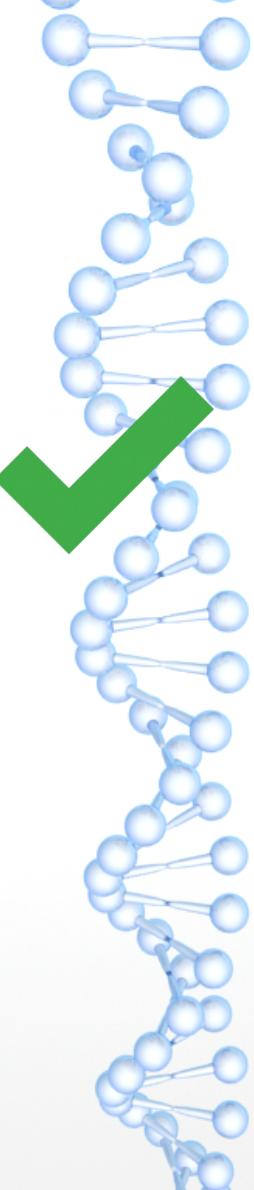
```
Info in <TJAlien::TJAlien>: Connecting to JBox:  
host=127.0.0.1, port=8097, user=vyurchen,  
cert=/home/yuw/.globus/tokencert.pem,  
key=/home/yuw/.globus/tokenkey.pem
```

```
Info in <TJAlien::Ls>: Ls command successful
```

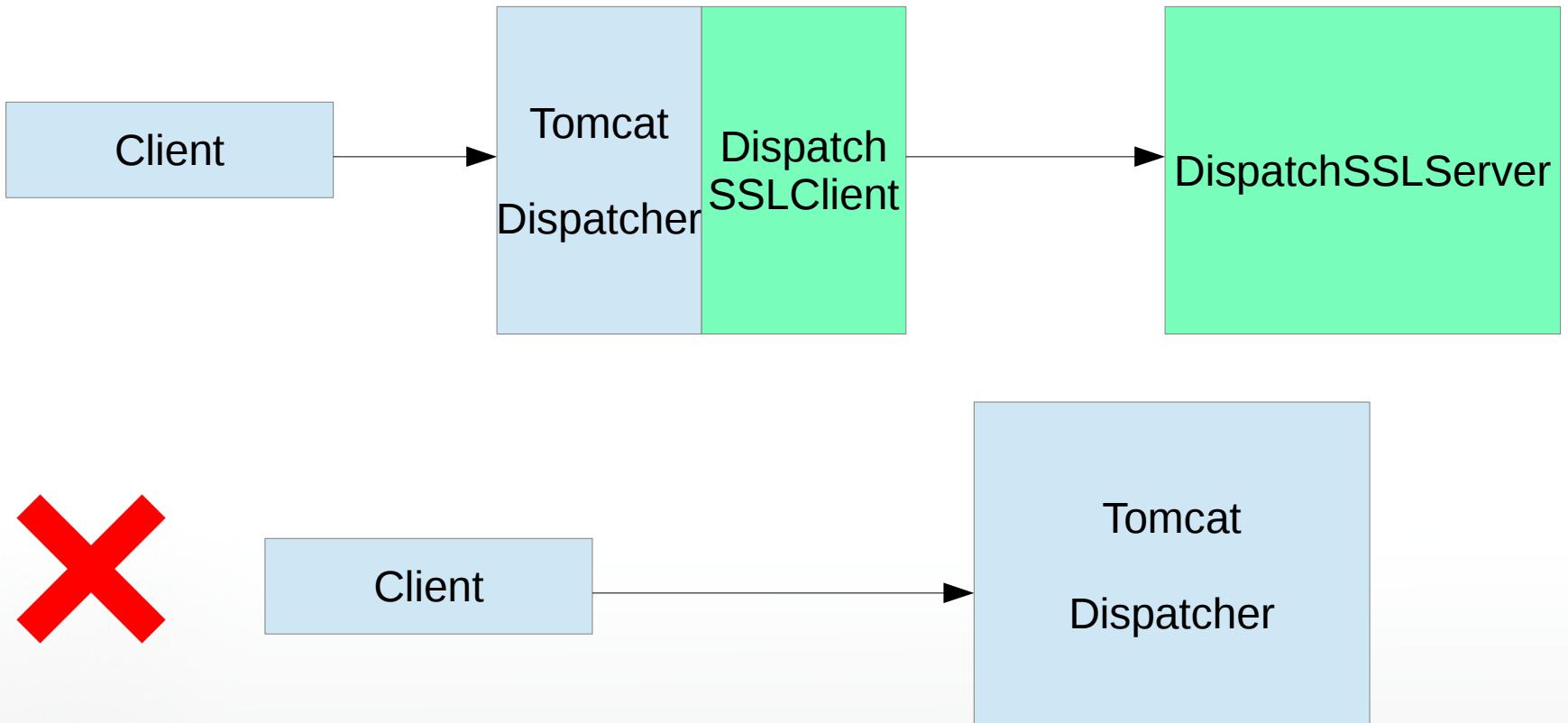


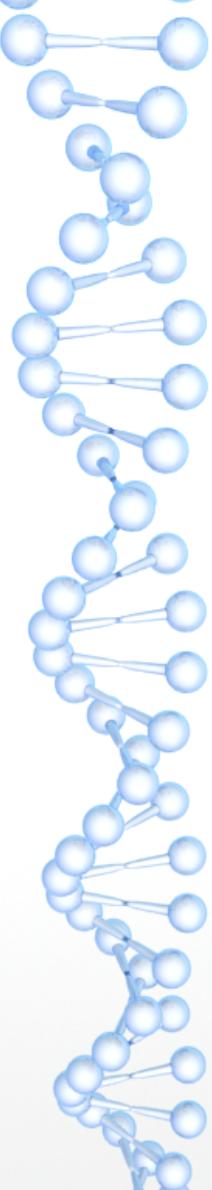
Bug fixes

- Authorization bug with Request Dispatcher (allowed clients to execute request on behalf of *alienmaster* user)
- Initializing db variables not in central service (slowed down the process of executing certain commands)



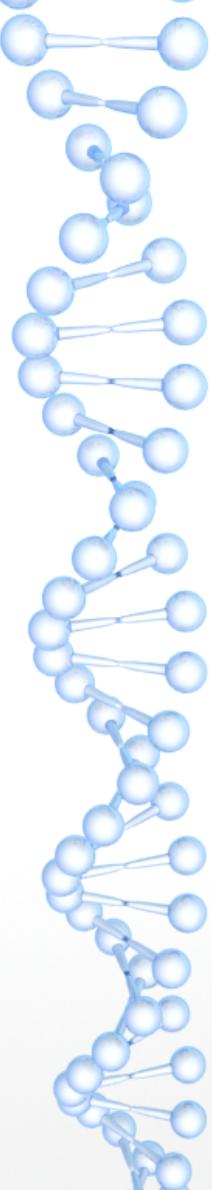
Authorization Bug





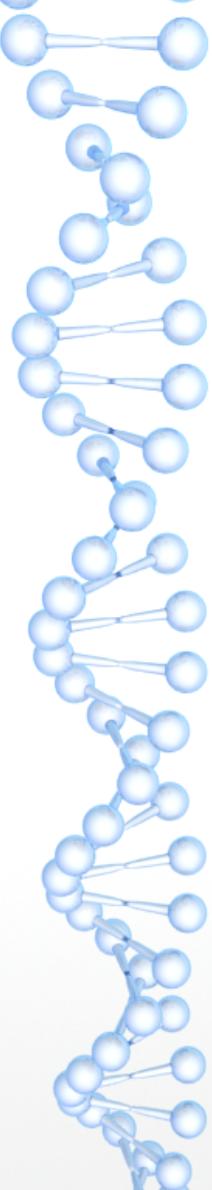
Polishing the code

- Put neutral notification in logs when client disconnects (instead of exception stacktraces)
- Remove unused variables
- Correctly close websocket session



Commands

- **ls**: send all information (“-la”) to ROOT clients
- Add extra check if Ifn exists to the **cp** command
- Pass correct fields to ROOT in the **submit** command
- Pass correct fields to ROOT in the **rmdir** command
- Implement **rm** command
- Implement file **open/write** commands



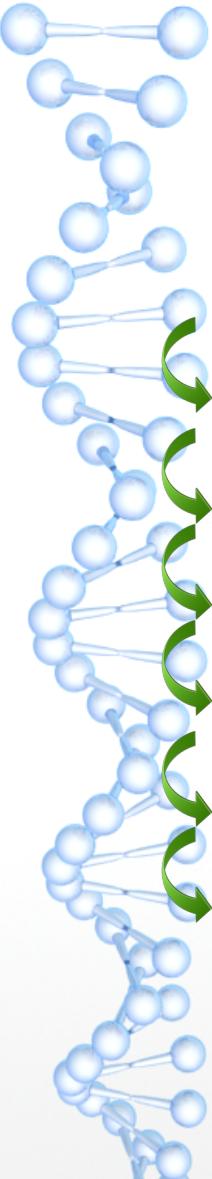
File operations

- Full read and write from ROOT working

```
root [1] TFile* myfile =  
Tfile::Open("alien:///alice/sim/2017/LHC17j8c/245353/001/aod_ar  
chive.zip#AliAOD.root");
```

```
root [2] TFile::Cp("alien:///alice/cern.ch/user/v/vyurchen/test.root",  
"alien:///alice/cern.ch/user/v/vyurchen/plain.root");
```

```
[TFile::Cp] Total 0.00 MB |=====| 100.00 %  
[0.5 MB/s]
```



Next steps

- Implement writing files to specific SE
- Register TJAlien ROOT plugin in AliBuild system
- Try ROOT6
- Custom SSL checks for proxy files(?)
- Smart detection of idle connections
- Refactor code to create uniform PrintWriter
- Rewrite JShell to use websockets