Metacat - Bug #5997

Restrict KNB trusted CAs

06/05/2013 11:00 AM - ben leinfelder

Status:	Closed	**Start date:**	06/05/2013
Priority:	Normal	**Due date:**	
Assignee:	ben leinfelder	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2.1.0	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

Instead of trusting all commercial CAs, the KNB Member Node should only trust the DataONE and CILogon certificate authorities.

To see a list of all them that are (currently) trusted:

```
openssl s_client -connect knb.ecoinformatics.org:443
```

History

#1 - 06/05/2013 11:02 AM - ben leinfelder

We should be able to simply use the DataONE chain file that we have installed already:

```
SSLCACertificatePath /etc/ssl/certs/
SSLCACertificateFile /etc/ssl/certs/DataONECAChain.crt
```

(i.e., comment out the first line)

#2 - 06/06/2013 03:48 PM - ben leinfelder

- Status changed from New to Closed

Commented out the line that includes all CAs in /etc/ssl/certs and reloaded Apache. Now we are down to the short list of accepted CAs.