Metacat - Bug #6954

ldapweb.cgi should use standard CA file

01/28/2016 10:06 AM - ben leinfelder

Status:	Resolved	**Start date:**	01/28/2016
Priority:	Normal	**Due date:**	
Assignee:	Jing Tao	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2.6.0	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

When Nick updated the ldap.ecoinformatics.org SSL certificate to use Let's Encrypt instead of GoDaddy, the Perl script for managing accounts could not establish a TLS connection with the LDAP server. I switched to script to use the standard ca-certificates.crt file (includes all standard CAs shipped with Ubuntu) and the connection was successful. I think we should try to use the standard CA certificate file whenever possible. The current default for Metacat is this old GoDaddy CA so on any Metacat upgrades will we need to remember to switch to the standard CA file unless we change the default configuration.

Current Metacat property default value:
ldap.server.ca.certificate=WEB-INF/gd_intermediate_bundle_nceas_ldap.crt

History

#1 - 01/29/2016 02:11 PM - Jing Tao

The reason we used an external ca certificate is that the old go-daddy certificate is not in the the system's default ca.

#2 - 02/03/2016 03:08 PM - Jing Tao

- Status changed from New to Resolved

We made changes on the ldap code. If users don't specify the ldap.server.ca.certificate on the metacat.properties, the code will use the default ca file /etc/ssl/certificate; if users specify that value, ldap will use that value. The default value of ldap.server.ca.certificate in metacat.properties is blank (not specify it).