Metacat - Bug #6219

Is $ldap->start_tls(verify => 'none') good enough in the ldpweb.cgi?

11/14/2013 07:17 PM - Jing Tao

Status:	Closed	**Start date:**	11/14/2013
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2.3.1	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

Currently when the ldapweb.cgi binds the ldap server, it issue this command to start tls:

$ldap->start_tls(verify => 'none')

Is this command secure enough?

It seems verify can be 'none' | 'optional' | 'require'.

In the line 814, it is #$ldap->start_tls(verify => 'require',
#cafile => '/usr/share/ssl/ldapcerts/cacert.pem');

But they were commented out.

History

#1 - 11/15/2013 09:06 AM - Matt Jones

No, it is not. That is a security bug, as it means that the SSL cert from the server may be invalid. For maximum security, it should be set to 'require'.

#2 - 12/19/2013 01:34 PM - ben leinfelder

- Target version set to 2.3.1

#3 - 12/19/2013 01:42 PM - ben leinfelder

- Status changed from New to Closed

Jing added 'require' to the TLS calls in the ldapweb script so I believe we are good now. Also involved configuring the CA path correctly so it knows how to verify the ldap server's identity.