Infrastructure - Task #2710

Story # 1791 (Closed): Create secure configuration for LDAP replication across various deployment Environments

Edit ldap.conf to include CA cert location for TLS

2012-05-07 20:05 - Ben Leinfelder

Status:	Closed	**Start date:**	2012-05-07
Priority:	Normal	**Due date:**	
Assignee:	Ben Leinfelder	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Sprint-2012.19-Block.3.2		
Milestone:	CCI-1.0.0	**Story Points:**	
Product Version:	*		

Description

For syncrepl, the server not only needs to have a certificate and key when acting as a server, but also the CA for that certificate when acting as a client (?) to verify the TLS connection.

ldap.conf should have:

TLS_CACERT /path/to/CA/cert/file.pem
http://www.zytrax.com/books/ldap/ch6/ldap-conf.html#tls-cacert

which will be our DataONE CA if we use our DataONE-signed certificates for configuring the server's TLS.

History

#1 - 2012-05-07 20:25 - Ben Leinfelder

- Status changed from New to Closed

Using the *.dataone.org cert on all servers, therefore that same cert can be used as the CA. Until we find that this does not actually work.

new ldap.conf file includes this default block:

For syncrepl using TLS, we use the wildcard cert as the CA

because all the members are using this as their server certificate

TLS_CACERT /etc/ssl/certs/_.dataone.org.crt

#2 - 2012-05-08 16:33 - Ben Leinfelder

- Status changed from Closed to In Progress

Looking at this again, I think we need a configuration param for which DataONE CA we are using (test vs. production).
Setting the default to:
TLS_CACERT /etc/ssl/certs/DataONETestCA.pem
since we don't have the production CA yet. Other parts of the configuration (Apache, say) can accept a directory of CA certs rather than a single file which makes this easier to generically configure. We could bundle all the DataONE CA certs into a single .pem file, but I don't think we want to allow test certificates to be accepted in the production environment.

#3 - 2012-05-08 19:12 - Ben Leinfelder

- Status changed from In Progress to Closed

I'm not even sure this is needed since I currently have cn-dev* set up with certs that are not signed by the wild card data one cert (obviously) and syncrepl is working just fine.