Infrastructure - Task #2706

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

Set up TLS for CN LDAP servers

2012-05-07 17:44 - Matthew Jones

Status:	Closed	**Start date:**	
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

History

#1 - 2012-05-07 19:29 - Ben Leinfelder

Useful info regarding configuration.
http://www.zytrax.com/books/ldap/ch15/#tls

#2 - 2012-05-07 20:23 - Ben Leinfelder

- Assignee changed from Matthew Jones to Ben Leinfelder

Added a TLS section to the slapd.conf with reasonable defaults for our deployments:

```
# Security - TLS section
TLSCertificateFile /etc/ssl/certs/_.dataone.org.crt
TLSCertificateKeyFile /etc/ssl/private/dataone_org.key
TLSCipherSuite TLSv1+RSA:!NULL
# the following directive is the default but
# is explicitly included for visibility reasons
TLSVerifyClient never
```

The postinst/config process prompts for the private key location and we use this new value if it is provided.

#3 - 2012-05-07 20:27 - Ben Leinfelder

- Status changed from New to In Progress

would like to test this before "closing it"

#4 - 2012-05-08 00:39 - Ben Leinfelder

Configured on cn-dev and worked through a few stumbles. The buildout should now prompt for everything it needs. We do need to make sure our private key files are readable by the ssl-cert group. Since private key deployment is manual, this can be a gotchya.

Will deploy on cn-dev-2 and cn-dev-3 to test actual synchronization.

#5 - 2012-05-08 00:58 - Ben Leinfelder

Looks good across the cn-dev-* environment. But how do we tell that TLS is actually being used?!

#6 - 2012-05-08 01:24 - Dave Vieglais

try:

sudo tcpdump -A -l -i eth0 port 389

then do something to initiate traffic

#7 - 2012-05-08 16:14 - Ben Leinfelder

I updated my givenName in LDAP and saw this (replication?) call between cn-dev and cn-dev-3.

09:12:25.958862 IP (tos 0x0, ttl 64, id 50474, offset 0, flags [DF], proto TCP (6), length 969)
cn-dev.dataone.org.ldap > cn-dev-3.dataone.utk.edu.38957: Flags [P.], seq 2797535443:2797536360, ack 1768833982, win 71, options [nop,nop,TS val 49034346 ecr 734503393], length 917
....-....inC....GV/.....
..4j+.....4Hto.F.....%.'T...

Still not conclusive to me. What do you think?

#8 - 2012-05-08 18:59 - Ben Leinfelder

- Status changed from In Progress to Closed