

Mysteries of openldap

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2007-11/msg05262.html>

- *From:* Timothy Murphy <tim@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 30 Nov 2007 14:17:44 +0000
-

I'm running openldap on my desktop,
and can access it fine from my laptop.
But I'd like to use TLS encryption
(as the desktop ldap is open to the world).

Unfortunately I find the openldap documentation
very difficult to follow.
It is almost as though they speak a different language,
say Finnish or Hungarian.

I've followed the instructions in chapter 14, "Using TLS",
in the OpenLDAP Software 2.4 Administrator's Guide
at <<http://www.openldap.org/doc/admin24/>>.
I've un-commented out the lines

```
-----  
TLSCACertificateFile /etc/pki/tls/certs/ca-bundle.crt  
TLSCertificateFile /etc/pki/tls/certs/slaped.pem  
TLSCertificateKeyFile /etc/pki/tls/certs/slaped.pem  
-----
```

and restarted "service ldap".

But I see no evidence that this has had any effect.
I can access the ldap directory from my laptop
exactly as I did before,
even if I make the change

```
-----  
# TLS_REQCERT allow  
TLS_REQCERT try  
-----
```

in ldap.conf on my laptop,
which as far as I can see (from "man ldap.conf")
should require my certificate(s) to be checked.

But it seems to work, as I said, with or without certificates,
and I see no evidence from tcpdump that
any encryption has been requested or implemented.

If someone who speaks openldap could enlighten me

Mysteries of openldap

I should be very grateful.

Incidentally, I have avoided installing SASL authentication, basically because I assumed that as it comes from Cyrus it was somehow related to Cyrus-Imap, which caused me great grief before I moved to dovecot.

Is SASL in fact the standard way to authenticate openldap? I read somewhere that there are "many ways" of authenticating openldap, without unfortunately any particular way being suggested.

Apologies for addressing what is probably an inappropriate forum. I tried posting to the gmane newsgroup mirroring the mailing list at openldap-software@xxxxxxxxxxxxx but unfortunately my postings there never appear.

Any advice or suggestions gratefully received.

—
fedora-list mailing list
fedora-list@xxxxxxxxxxxx
To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>