pfSense - Todo #9417

Convert LDAP TLS setup from environment to LDAP_OPT_X_TLS_* set options

03/21/2019 01:42 PM - Jim Pingle

Status:	New	**Start date:**	03/21/2019
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Authentication	**Estimated time:**	0.00 hour
Target version:	Future		

Description

PHP 7.1 added support for configuring the LDAP CA/Cert environment directly, rather than relying on the environment variables. These use new constants named LDAP_OPT_X_TLS_<blah>

For example:

```
ldap_set_option($ldap, LDAP_OPT_X_TLS_CERTFILE, "{$cert_prefix}.crt");
```

The use of environment variables may also be contributing to occasional failures of **Diagnostics > Authentication** testing LDAP logins with/without SSL.

Associated revisions

Revision 996a1ad9 - 03/21/2019 02:17 PM - Jim Pingle

LDAP TLS option update. Implements #9417

Revision efdba6ca - 05/10/2019 02:55 PM - Jim Pingle

LDAP TLS option update. Implements #9417

(cherry picked from commit 996a1ad90e5682bf881bafd8b75d1b1a7e3f7831)

Revision 2bf6d432 - 05/15/2019 03:18 PM - Jim Pingle

Revert "LDAP TLS option update. Implements #9417"

This reverts commit efdba6ca75e001e8426b2ecab49f71b53d5c9e30.

Revision 7729c5a1 - 08/27/2019 01:46 PM - Jim Pingle

Revert LDAP_OPT_X_TLS changes since they do not work. Issue #9417

History

#1 - 03/21/2019 02:25 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 996a1ad90e5682bf881bafd8b75d1b1a7e3f7831.

#2 - 04/01/2019 02:21 PM - Jim Pingle

See #9433 for an additional example of a problem case solved by this patch

#3 - 05/11/2019 04:47 PM - Jim Pingle

- Target version changed from 2.5.0 to 2.4.4-p3

#4 - 05/14/2019 11:08 PM - Chris Linstruth

2.4.4-p3

This all seems to work. It also seems much more consistent as posited in the description. I did a lot of bouncing around between SSL/636, STARTTLS, Clear, making changes to the server capabilities and requirements and everything seemed to happen as expected.

Much improved. Thank you.

#5 - 05/15/2019 11:18 AM - Jim Pingle

- Status changed from Feedback to Resolved

#6 - 05/15/2019 03:17 PM - Jim Pingle

- Status changed from Resolved to New

- Target version changed from 2.4.4-p3 to 2.5.0

Upon further testing this does not appear to be working for self-signed certificates. It works for global, however. Will need to be backed out of 2.4.4 and revisited for 2.5.0, where it also doesn't appear to be working for this scenario.

#7 - 05/15/2019 03:25 PM - Jim Pingle

- Status changed from New to Feedback

Applied in changeset 2bf6d4322622765bd1ce6ca8915ff75890885566.

#8 - 05/15/2019 03:28 PM - Jim Pingle

- Status changed from Feedback to New

#9 - 05/15/2019 03:35 PM - Jim Pingle

It looks like LDAP_OPT_X_TLS_CACERTDIR and LDAP_OPT_X_TLS_CACERTFILE are being set but for some reason not honored as they should be. I can retrieve the set values with ldap_get_option(), but the connection still fails to validate the CA even though the correct file is in place. Checking with the exact same CA file at the CLI using s_client shows the CA as valid.

There was a PHP bug filed a long time ago, but was closed for lack of feedback: https://bugs.php.net/bug.php?id=73558
A couple other similar posts around but nothing concrete either way.

Will keep testing on 2.5.0 but this may need backed out entirely, or at least reworked so the old style is only used for self-signed.

#10 - 08/21/2019 10:29 AM - Jim Pingle

- Category changed from User Manager / Privileges to Authentication

#11 - 08/27/2019 02:06 PM - Jim Pingle

- Target version changed from 2.5.0 to Future

Taking this off 2.5.0. I backed the changes out. It appears to be an upstream problem in PHP still, and no movement on the bug report above. I left a comment with some more details. We can revisit this in the future if the bug ever gets fixed.