pfSense - Todo #10704

Work around PHP issues with SSL LDAP and multiple authentication servers

06/25/2020 11:08 AM - Jim Pingle

Status:	Resolved	**Start date:**	06/25/2020
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	User Manager / Privileges	**Estimated time:**	0.00 hour
Target version:	2.5.0		

Description

Based on a report from a customer, the PHP environment we have to setup for SSL LDAP clients does not appear to gracefully handle multiple authentication servers. It ends up not trusting the CA for one or more of the attempted connections. Unless the issues in #9417 have fixed on PHP 7.4 (See #10659), we should try to find a way to handle this situation better, if possible.

2.4.5-p1 workaround: Set the LDAP auth server entries to use Global Root CA List, copy CA cert PEM data to /etc/ssl/<hash>.0 where <hash> is the output of openssl x509 -hash -noout -in ca.crt

2.5.0 workaround: Set the LDAP auth server entries to use Global Root CA List, edit the CAs in the cert manager, check "Add this certificate to the Operating System Trust Store".

That should allow all of the LDAP server CAs to be trusted concurrently.

One possible workaround would be to setup more isolated environments for each server, perhaps with a unique ID per LDAP server or CA hash, but there may still be PHP environment issues when doing it that way.

History

#1 - 06/26/2020 03:26 PM - Jim Pingle

- Description updated

#2 - 10/19/2020 09:20 AM - Steve Beaver

- Tracker changed from Todo to Documentation

#3 - 10/19/2020 10:29 AM - Jim Pingle

- Tracker changed from Documentation to Todo

There is still likely to be a technical / non-documentation way to address this.

Some of that depends on the outcome of wider testing for #9417

#4 - 11/12/2020 01:13 PM - Jim Pingle

- Status changed from New to Feedback

This is technically waiting for feedback on #9417 so I'm changing the status accordingly.

If #9417 has to be backed out again, this can be changed back to a documentation ticket and I can update the docs as needed, and it is not a release blocker at that point.

#5 - 02/09/2021 12:51 PM - Renato Botelho

Marking it as resolved since nobody answered in 3 months

#6 - 02/09/2021 12:53 PM - Renato Botelho

- Status changed from Feedback to Resolved