ModAuthAndActiveDirectory2003

⚠️ THIS IS A SCRATCHPAD DOCUMENT, PLEASE CONSIDER THIS WHEN READING ON 💡

mod_auth_ldap has a problem with LDAP referrals as returned by Windows 2003 Active Directory. The AD behavior changed from 2000 to 2003 and thus a previously working mod_auth_ldap configuration could stop working when the queried AD server is upgraded to 2003.

This issue is listed in Bug 26538. A patch has been posted there to allow control of how mod_auth_ldap handles referrals by adding a `AuthLDAPFollowReferrals` config option. This wiki page is a start at collecting the information threaded from the above bug. It is unclear when or if the referenced patch will be merged into a release.

Disclaimer: non-expert's explanation The core problem is that if one queries LDAP on AD starting at top ("root") of the directory tree, the normal process is for the LDAP server to return referrals for the possible sub-tree OU nodes to be searched. The client should then re-query each OU nodes as necessary. Mod_auth_ldap does not follow these referals.

Workaround

Aside from building httpd using this patch, there are a few configuration workarounds.

1. Query the Global Catalog on port 3268. The Global Catalog AD server (a specific role of one Active Directory server in a typical Windows 2003 managed network) will not issue referrals when queried on port 3268.
2. Don't do queries that will require referals.

To quote from the bug report commentary:

```
Most of the time this can be worked around by changing the AuthLDAPURL to start
searching deeper down in the tree, thereby avoiding the referrals.

eg:
cn=Users,dc=<DOMAIN>,dc=com
OR
ou=something,dc=<DOMAIN>,dc=com

Unfortunately however, when you need to search two OUs, eg:
ou=A,dc=<DOMAIN>,dc=com  AND ou=B,dc=<DOMAIN>,dc=com

you have no choice but to start search at the top of the tree.
```

I have a more verbose (but not necessarily more informative) post on my blog: ApacheLDAPAndActiveDirectory – ChrisMorris