Setup LDAP for Bookstack

1. Take Snapshop
2. vi /etc/systemd/resolved.conf (Add both DNS servers and domain)
3. Run sudo systemctl restart systemd-resolved and make sure you can ping fqdn.
   (like ping fo.local or platinumcopiers.hou)

Put the following in /var/www/bookstack/.env file (but change the OU/DN to the correct one)
NOTE!! the LDAP_DUMP_USER_DETAILS will dump the details but the KB won't load!! so make sure to comment out
or you get a blank screen.

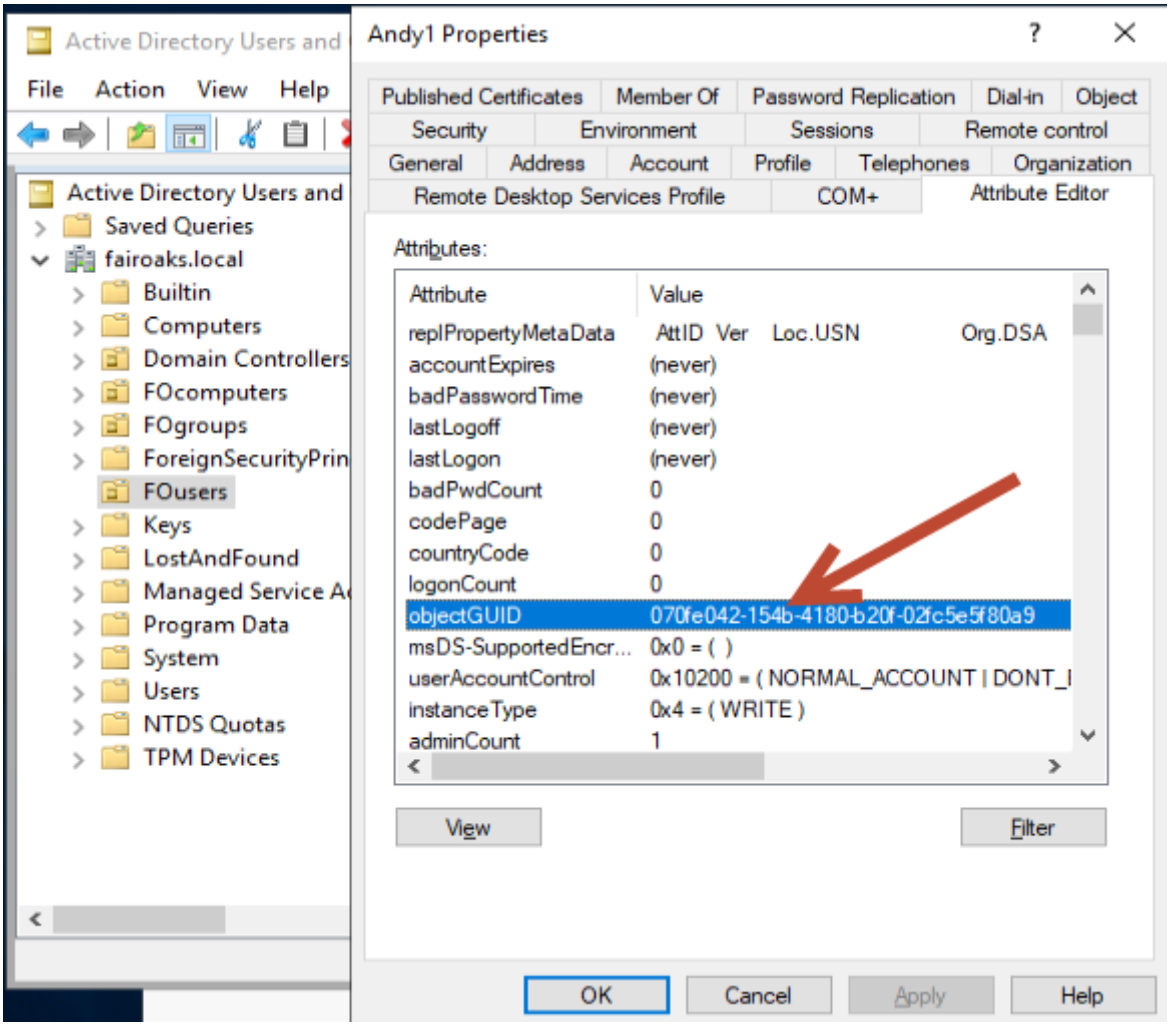
#LDAP
AUTH_METHOD=ldap
LDAP_SERVER=fo.fairoaks.local:389
LDAP_DN="cn=FOUsers,dc=fairoaks,dc=local"
LDAP_DN="cn=svcBookstack,ou=FOusers,dc=fairoaks,dc=local"
LDAP_PASS="BookmyStack"
LDAP_USER_FILTER=(&(sAMAccountName={user}))
LDAP_VERSION=3
LDAP_DISPLAY_NAME_ATTRIBUTE=cn
LDAP_ID_ATTRIBUTE=BIN;objectGUID
LDAP_THUMBNAIL_ATTRIBUTE=thumbnailPhoto
LDAP_EMAIL_ATTRIBUTE=mail
LDAP_START_TLS=false
#LDAP_DUMP_USER_DETAILS=true

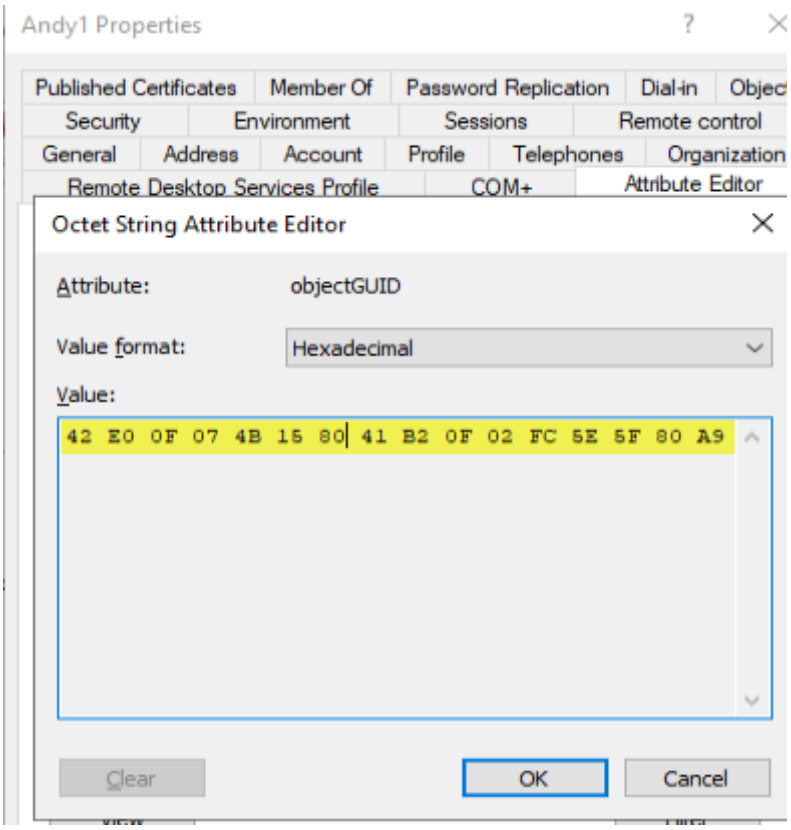
4. Vi /etc/ldap/ldap.conf

/etc/ldap/ldap.conf:
#TLS_CACERT /etc/ssl/certs/ca.crt
TLS_REQCERT never

5. Apt install ldap-utils (This is needed to do ldapsearch to test connectivity)

6. In AD Look at a users Attribute (you must double click it to get the real number). This will go into the user External Authentication ID if you plan on using an already created account before LDAP. (**Upper CaSe is fine but get rid of the spaces**)


Active Directory Users and
File Action View Help
Active Directory Users and
Saved Queries
fairoaks.local
Builtin
Computers
Domain Controllers
FOcomputers
FOgroups
ForeignSecurityPrin
FOusers
Keys
LostAndFound
Managed Service A
Program Data
System
Users
NTDS Quotas
TPM Devices
Andy1 Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Attributes:
Attribute
Value
replPropertyMetaData
AttID Ver Loc.USN Org.DSA
accountExpires
(never)
badPasswordTime
(never)
lastLogoff
(never)
lastLogon
(never)
badPwdCount
0
codePage
0
countryCode
0
logonCount
0
objectGUID
070fe042-154b-4180-b20f-02fc5e5f80a9
msDS-SupportedEncr...
0x0 = ( )
userAccountControl
0x10200 = (NORMAL_ACCOUNT | DONT_
instanceType
0x4 = (WRITE)
adminCount
1
View
Filter
OK
Cancel
Apply
Help


Andy1 Properties
Published Certificates
Member Of
Password Replication
Dial-in
Objec
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Octet String Attribute Editor
Attribute:
objectGUID
Value format:
Hexadecimal
Value:
42 E0 0F 07 4B 15 80 41 B2 0F 02 FC 5E 5F 80 A9
Clear
OK
Cancel

Test LDAP in Linux (must work or Bookstack wont)
ldapsearch -x -H ldap://fo.fairoaks.local:389 -D "CN=andy,OU=FOusers,DC=fairoaks,DC=local" -b "OU=FOusers,DC=fairoaks,DC=local" -W -d 1

Cause
The error shown below is similar each time there is an LDAP authentication issue.
• "The exception is [LDAP: error code 49 - 80090308: LdapErr: DSID-0Cxxxxxx, comment: AcceptSecurityContext error, data xxx, vece]."

However, there are several values that can indicate what LDAP function is causing the issue. Here are some general references for Microsoft Active Directory:

The AD-specific error code is the one after "data" and before "vece" or "v893" in the actual error string returned to the binding process
525 user not found
52e invalid credentials
530 not permitted to logon at this time
531 not permitted to logon at this workstation
532 password expired
533 account disabled
534 The user has not been granted the requested logon type at this machine
701 account expired
773 user must reset password
775 user account locked

Revision #2
Created 19 April 2025 21:28:56 by Andy
Updated 19 April 2025 21:38:31 by Andy