Troubleshooting LDAP logins

This article is to assist in determining common causes of not being able to authenticate and authorize using LDAP (MS Active Directory or OpenLDAP).

Before you start

Make sure you've read How to Enable LDAP Authentication and Authorization for Open-AudIT and for good measure, also check LDAP_Servers. You might even watch the video,

So, you've read both of those, you've watched the video and you still cannot login using LDAP. Open-AudIT has quite extensive logging where LDAP auth is concerned, for exactly this reason. The logs, especially at debug level, will assist you in point out where exactly the process is failing.

Using LDAPS

By default, we skip certificate validation because customer tend to use self-signed certificates. To enable certificate validation, edit the file -

Linux

```
/usr/local/open-audit/code_igniter/application/models/m_logon.php
```

Windows

```
c:\xampp\open-audit\code_igniter\application\models\m_logon.php
```

Comment out the below line (about line 170 or so). Just place a hash # at the start of the line.

```
putenv('LDAPTLS_REQCERT=never');
```

Once commented out, your certificate will be validated, but may also fail this validation if you're using self-signed certificates and haven't configured your server correctly.

More information about debugging this can be found on a helpful Stack Overflow thread - https://stackoverflow.com/questions/25424622/authenticating-a-self-signed-certificate-for-ldaps-connection

One other item to be careful of - make sure you use the hostname (or fqdn) of your LDAP Server that matches what is in the certificate (not just the LDAP Servers IP address) when creating the LDAP entry in Open-AudIT.

Troubleshooting

NOTE - log_level 7 in the configuration should only be used when troubleshooting. Debug level logging will create a LOT of logs. Your normal level should be 5, not 7.

This process will remove any existing logs, so if you need them for some reason, you can export them using menu -> Admin -> Database -> List Tables -> logs -> Export to SQL | CSV | XML.

First

Let's set the log level to 7. Go to menu -> Admin -> Configuration -> List Configuration (or All Configuration if using Pro/Ent). Select the log_level item. Click the edit button and change it to 7. Now log out.

Second

Let's remove the logs data. On the command line, on the Open-AudIT server runt he below command.

Linux

```
mysql -u openaudit -popenauditpassword openaudit -e "DELETE FROM logs;"
```

Windows

```
c:\xampplite\mysql\bin\mysql.exe -u openaudit -popenauditpassword openaudit -e "DELETE FROM logs;"
```

Third

Let's try logging in using an LDAP user. I am assuming this will fail (otherwise, why are you still reading this?). Next, run the below in order to set the log level back to 5.

Linux

```
mysql -u openaudit -popenauditpassword openaudit -e "UPDATE configuration SET value = 5 WHERE name =
'log_level';"
```

Windows

```
c:\xampplite\mysql\bin\mysql.exe -u openaudit -popenauditpassword openaudit -e "UPDATE configuration SET value
= 5 WHERE name = 'log_level';"
```

Forth

Log back into Open-AudIT using the Admin account. and export the logs from menu -> Admin -> Database -> List Tables -> Logs -> Export to CSV. If there is a minimal amount of log lines, it may display on the bottom of the screen. Scroll down to view it. If you would rather view this in Excel, copy and paste the logs and save them as a text file with a .csv extension. Read through the logs and the final line will likely be the one of most interest. This line should give you the exact point at which the login failed.

Fifth

Send the artifacts to Opmantek. If you are a supported Opmantek customer,a couple of items will make helping your easier. Please do save the log output to a CSV. Please generate the support JSON at menu -> Help -> Support and click the Download icon on the right hand side of the header. Save this file. Export your LDAP server from menu -> Admin -> LDAP Servers -> Details. In the URL, add the following .json (so from http:/oa_server/en/omk/open-audit /ldap_servers/1 to http://oa_server/en/omk/open-audit/ldap_servers/1.json). Save that file.

Please send all three files to your support contact at Opmantek and describe your issue.

Sixth

Examine the log lines.

Log Line	Symptom	Status
No Roles retrieved from database	Something has gone seriously wrong. Open-AudIT cannot read the 'roles' table.	error
No Orgs retrieved from database.	Something has gone seriously wrong. Open-AudIT cannot read the 'orgs' table.	error
$x LDAP servers retrieved from database.	Where $x is a number. This many LDAP entries are in the DB and have been retrieved.	debug
An invalid LDAP server type was supplied $ldap->type skipping.	The LDAP server type is invalid. It should be either 'active directory' or 'openldap'.	error
An invalid LDAP version was supplied $ldap->version, skipping.	Usually should be set to 3.	error
LDAP connect failed for LDAP server at $ip. Check your host, port and secure settings. Attempted to use $ldap_connect_string	The LDAP server could not be connected to. At all. Check it's pingable from the Open-AudIT server. Check the correct port is open to the Open-AudIT server. An nmap from the Open-AudIT server will show this. Substitute your LDAP servers IP for $ip. Try: `nmap -vv $ip`	notice
LDAP server could not be reached at $ldap->host, skipping.	See above. NOTE - This could also be caused by a self-signed certificate on the LDAP server. We are working to allow for this in a future release.	notice
Invalid user supplied credentials for LDAP server at $ldap->host, skipping.	The credentials supplied by the user have failed.	info
Could not bind to LDAP server at $ldap->host, skipping.	Some other error has occurred when attempting to bind to the LDAP server. It is contactable (ie, the 'connect' above has worked), but for some other reason, binding has not occurred. Check the logs on the LDAP server.	info
Successful bind using credentials for LDAP server at $ldap->host	The LDAP server was connected to and the user credentials accepted for bind.	debug
Invalid DN supplied credentials for LDAP server at $ldap->host, skipping	The administrator supplied credentials to bind to the LDAP server, but they have not been accepted by the LDAP sevrer. Double check the credentials work on the LDAP server, and then check (or reset them) in the Open-AudIT LDAP Server entry.	info
Bound to LDAP using supplied dn details: $ldap->dn_account	The administrator supplied credentials that were successfully used to bind to LDAP.	debug
User $username in LDAP $ldap->name but not in Open-AudIT and not using LDAP for roles. Trying next LDAP Server.	The user that was specified exists in LDAP, but Open-AudIT is not configured to consume the LDAP groups for roles and that user does not exist within Open-AudIT. Either select "Use LDAP for Roles" on the Open-AudIT LDAP Server screen or create this user within Open-AudIT and assign roles and orgs.	info
LDAP search successful for user $username at $ldap->host	LDAP was searched for this user and their account was found.	debug
LDAP entries retrieval successful for user $username at $ldap->host	The users details were retrieved from LDAP.	debug
LDAP entries retrieval failed for user $username at $ldap->host	The users details were not retrieved from LDAP. Check the LDAP server logs.	info
LDAP search failed for user $username at $ldap->host	LDAP was searched for this user and their account was not found. Check the LDAP server logs. The user credentials have worked, but the user wasn't found. Also check you have specified the correct Base DN attribute when you created the LDAP Server in Open-AudIT.	info
Checking AD group membership for $user->name	Information only.	debug
User $username is a member of LDAP group for Role $role->ad_group	The user is in the LDAP group that matches this Role.	debug
No AD group associated with role $role->name, skipping.	This Role has no AD group specified. Check the roles details within Open-AudIT. Roles	debug
User $username is a member of LDAP group for Org $org->ad_group	The user is in the LDAP group that matches this Org.	debug
No AD group associated with org $org->name, skipping.	This Org has no AD group specified. Check the roles details within Open-AudIT. Orgs	debug
LDAP search for role $role->ad_group succeeded, $username is in group.	The user is in the LDAP group that matches this Role.	debug

LDAP search for role $role->ad_group succeeded, $username is NOT in group.	The user is not in the LDAP group that matches this Role.	debug
LDAP search failed for groups (roles) $user->name at $ldap->host	The search for group on the LDAP server failed. Check the LDAP server logs. Have you created these groups (for roles and orgs) on the LDAP server and assigned LDAP users to them?	debug
LDAP search for org $org->ad_group succeeded, $username is in group.	The user is in the LDAP group that matches this Org.	debug
LDAP search for org $org->ad_group succeeded, $username is NOT in group.	The user is not in the LDAP group that matches this Org.	debug
LDAP search failed for groups (orgs) $user->name at $ldap->host	The search for group on the LDAP server failed. Check the LDAP server logs. Have you created these groups (for roles and orgs) on the LDAP server and assigned LDAP users to them?	debug
No AD group associated with org $org->name, skipping.	This Org has no AD group specified. Check the roles details within Open-AudIT. Have you created these groups (for orgs) on the LDAP server and assigned LDAP users to them?	debug
New user $username logged on (AD account)	A new user logged in to Open-AudIT and was authenticated and authorized by the LDAP sever. That user was then created in Open-AudIT and logged in. Success.	notice
Existing user $username logged on (AD account).	An existing Open-AudIT user was authenticated and authorized by the LDAP server. Success.	debug
User $username exists in LDAP $ldap->name and attempted to logon, but does not belong to any OA groups for Roles or Organisations.	The user is in LDAP and their credentials are valid, but is not in any of the required Open-AudIT LDAP groups.	info
User $username exists in LDAP $ldap->name and attempted to logon, but does not belong to any OA groups for Organisations.	The user is in LDAP and their credentials are valid, but is not in any of the Open-AudIT LDAP groups for Orgs.	info
User $username exists in LDAP $ldap->name and attempted to logon, but does not belong to any OA groups for Roles.	The user is in LDAP and their credentials are valid, but is not in any of the Open-AudIT LDAP groups for Roles.	info