How to Enable LDAP Authentication and Authorization for Open-AudIT

Overview

Open-AudIT can use Active Directory and/or OpenLDAP for user authentication and/or authorisation. Open-AudIT will query both types of LDAP servers to validate a user's username and password, then retrieve user details and the list of roles the user has and the orgs a user has access to. Open-AudIT will automatically create the user if they are authenticated and authorized so no manual user setup within Open-AudIT is required - at all!

How To

To enable this, create a new LDAP Server item by going to menu -> Admin -> LDAP Servers -> Create LDAP Servers.

Input the relevant details for either Active Directory or OpenLDAP.

Once you have done this, Open-AudIT will attempt to verify your user logon details against an LDAP server. If the user has valid LDAP credentials, Open-AudIT will ask LDAP for the list of groups (in LDAP) that the user is in. If the user is in the corresponding groups for Open-AudIT Roles and Orgs, those Roles and Orgs will be applied to that user.

If the user account does not actually exist within Open-AudIT, it will be created. If it does exist, the details such as email, full name, etc will be updated.

If the user either doesn't have valid LDAP credentials or is not in at least one Open-AudIT Role and Group, Open-AudIT will fallback to using local Open-AudIT user details and attempt authentication and authorization there. Failing that, the user will be denied access.

The user in LDAP must be a direct member of the required Open-AudIT groups for Roles and Orgs. A member of a group that is a member another group that is a member of the Open-AudIT group will not work (at this stage).

If a new Org is created, an LDAP group name is automatically derived from the name. For example, if a new Org is created and is named Test, the corresponding LDAP group will be named open-audit_orgs_test.

Roles can only be created and edited if you have an Open-AudIT Enterprise license. For most users, the default set of Roles should be all that is required. And if you think about it, it's more granularity than Open-AudIT has ever had at any time!

Authenticate via LDAP Only

You may wish to have Active Directory or OpenLDAP authenticate your users, but not provide authorization. To do this, make sure "Use LDAP for Authentication" is set to Y and "Use LDAP for Roles" is set to N. The credentials will be validated by LDAP, but you will need to have the user already created and assigned Roles in Open-AudIT.

Enabling for Professional and Enterprise

If you are using Open-AudIT Professional or Enterprise and you enable LDAP and you wish for user accounts to be automatically created at logon, you must edit the (text) file:

Linux – /usr/local/omk/conf/opCommon.nmis

Windows – c:\omk\conf\opCommon.nmis

And ensure that auth_method_1 is set to openaudit.

That's all there is to it. As long as Open-AudIT can talk to an LDAP Server - be it an Active Directory Domain Controller or an OpenLDAP server, your users can use their existing LDAP credentials to logon to Open-AudIT.

The default Open-AudIT groups for LDAP Server authorization are:

Roles Groups

```
+-----------+---------------------------+
| name      | ad_group                  |
+-----------+---------------------------+
| admin     | open-audit_roles_admin    |
| org_admin | open-audit_roles_org_admin |
| reporter  | open-audit_roles_reporter |
| user      | open-audit_roles_user     |
+-----------+---------------------------+
```

Orgs Groups

```
+----------------------+-------------------------------------+
| name                 | ad_group                            |
+----------------------+-------------------------------------+
| Default Organisation | open-audit_orgs_default_organisation |
+----------------------+-------------------------------------+
```