About this document

This document is a comprehensive guide for synchronizing the OpenLM Database with an organizational Directory Server. For a more concise documentation, please refer to:

Directory service (e.g. Active Directory – LDAP) Synchronization: Basic Guide

You may also find the video in this link helpful.

The OpenLM Server is capable of synchronizing users and groups with an organization's Directory Service (e.g. Active Directory, Novell eDirectory, ApacheDS) to combine license management with other company information. For the sake of simplification, we will relate to this process as "LDAP Synchronization" throughout this document.

Benefits of LDAP Synchronization

There are many benefits in synchronizing the OpenLM Database with data resident in the organizational Directory Service for all decision makers in the organization:

From a managerial standpoint, it can be applied for

- Enforcing license usage permissions,
- Implementing usage chargeback (usage billing),
- Analysis of usage trends, etc.

Administrators may gain in:

- Automating the management of license restriction (e.g. through FLEXlm Options file management)
- Streamlining license usage reporting, according to updated Users' and Groups' data

From the end-user point of view:

- User information may be presented to easily locate other users that are holding a required license.
- Users may choose to authenticate their usernames on the OpenLM EasyAdmin web application via Windows authentication. Please read more about this here: EasyAdmin Windows Authentication

The Groups synchronization functionality is part of the Users and Groups extension, and requires additional licensing.

LDAP Synchronization steps

The elaborated procedure for committing LDAP synchronization is described throughout this document. Here is a summary of the steps required for LDAP synchronization.

1. Set Domain Definition:

a. Windows Start → All Programs → OpenLM → Configure OpenLM Server-Start Here.

b. Select the **LDAP** tab.

c. Click **Add Domain Definition>>**

d. Input the LDAP server details: Domain name, User Name, Password, LDAP server type and LDAP secure connection (SSL) activation.

e. Check connectivity to the LDAP by clicking **Check Domain**.

f. Save configuration to a temporary buffer by clicking **Apply changes**.

2. Define the synchronization parameters, by clicking **Add a Synchronization Definition to this Domain**:

- **Synchronization Name**
- **Synchronization start node**
- **Sync time interval**

3. Set Rules for Users using the drop-down menu to complete the **Rules for users synchronization**:

- **LDAP objects to sync**
- **Sync username attribute**
- **Sync only active users of licenses**
- **Users membership filter**
- **Search depth selection**

4. Configure Groups' synchronization parameters, as shown in **Group synchronization Settings>>**

- **Set Default Group**
- **Search depth**
- **No Groups**
- **Flat / Hierarchical / Attribute**

5. Click **Apply**

6. To apply the configured synchronization, open the OpenLM EasyAdmin web portal

Windows Start → OpenLM → OpenLM EasyAdmin2.

7. Apply the configured synchronization, as described in the **EasyAdmin Synchronization**

interface section below. Click the EasyAdmin Start button → Administration →Sync Definitions. The LDAP synchronization window opens. Click **Sync Now** to apply the synchronization.

8. View the outcome of the synchronization as described in the **Users and Groups presentation** and the **EasyAdmin Synchronization** interface sections below.

Users and Groups presentation

The Users and User groups which exist in the OpenLM Database are apparent in the EasyAdmin web application, in the Users and Groups windows respectively. To open these windows, click the EasyAdmin 'Start' button → "Users and Permissions" → and choose either 'Users' or 'Groups'.

Initially, upon installation of the OpenLM server, the Users and Groups are only populated by the defaultly disabled 'Generaluser' user, and the "OpenLM_Everyone" default group. "Generaluser" is by default a member of OpenLM_Everyone. See the following image for clarification.

Default groups

Default groups are groups of users, present in the OpenLM database. They are special in the aspect that they accumulate the time period of their members' license usage. When users are presented in the OpenLM database, they are by default automatically related to the **OpenLM_Everyone** group, and their license usage is accumulated in that group.

LDAP synchronization may be implemented so that users would become related to specific user default groups, other than the **OpenLM_Everyone** group. Default groups are highlighted in green in specific user's windows, under the **Groups** tab.

For example, in the image below U_A1 is a member of OpenLM_Everyone, G_A1 & GA_2. Group G_A1 was synchronized before G_A2, hence it assumed the default group role for user U_A1, and is highlighted in green.

For information on setting the default group, please see the "Set Default Group" section

below.

The Active Directory tab

Interfacing the LDAP Server

The LDAP tab is the OpenLM Server's interface to LDAP synchronization. The 1st thing to do is to connect to the LDAP Database. In order to do so:

1. Click the **LDAP** tab, and **Add** . The Domain Definitions' dialogue box opens.

2. Type in the LDAP server details:

- The **Domain Name** or **IP address** of the server which hosts the organization's domain controller
- **User Name** (e.g: administrator)
- **Password**
- **LDAP server type**: (e.g. "Active Directory").
- **LDAP secure connection (SSL)** active or inactive. In order to use an LDAP secured connection, check this check box and add a colon with a port number in the domain name textbox (e.g. Domain_Name:636)

3. Check the connection to the LDAP server by clicking **Check Domain**.

4. Save the configuration to a temporary buffer by clicking **Apply changes**.

5. To undo changes, and revert to the latest saved configuration, click **Cancel changes**.

6. Click **Apply** to save the changes to the OpenLM database.

7. Organizations may have multiple domain controllers (for example, different departments or subsidiary companies have their own servers for user authentication). In order to add a second domain, click **Add** and repeat steps 2 through 4 listed above.

COMMON GLOBAL CATALOGS

A global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest. When Common Global Catalogs are applied, a single search query using port 3268 would be sent to a global catalog server. This configuration is preferable to multiple domain control configuration for both simplicity and speed considerations. Please refer to this article for more information.

CONFIGURING LDAP SYNCHRONIZATION PARAMETERS

After having configured the OpenLM Server to interface the LDAP server, one must now configure the actual synchronization parameters. In order to do so, mark the newly created domain, and click **Add**. The synchronization window opens:

Synchronization Name

Name the synchronization scheme in the **Synchronization Name** text box.

Synchronization start node

Click the **Select...** button. A tree diagram of the LDAP structure opens. Select the synchronization start node. This node will be the upper-most object of the configured synchronization.

Sync time interval

The value in this example states that user details would be updated every 1 hour. Keep in mind that the synchronization process may demand considerable computer assets when applying on a large LDAP databases.

SYNCHRONIZING USERS AND COMPUTERS

Synchronization of Users and Computers is the basic operation of the LDAP synchronization process. It is important to note that synchronizing users to the LDAP is a tricky business; you may end up having taken in more users than you intended, and deleting users from the database is difficult. It is highly recommended to experiment on a separate database, NOT on the production database.

LDAP objects to Sync

It is possible to synchronize either Users or Computers. Use the **LDAP objects to sync** radio buttons to choose between those.

a) Sync username attribute

- **cn** should be used for any LDAP configuration other than “Active Directory”, i.e. “Novell Directory” or “Apache DS” .

- **sAMAccountName** is good for Pre Windows server 2000 Active directory versions.

- **userPrincipalName** is good for Post Windows server 2000 Active directory versions.

b) Users membership filter

Use this drop down menu to select whether to synchronize all users, only users within OUs, or only users within LDAP security groups.

c) Search depth selection

The Search depth selection number enables the administrator to truncate the synchronization process at a certain hierarchical level:

‘0’ (default): Full tree group hierarchy is synchronized.

‘1’: Only the start node group is synchronized.

‘2’: The start node group and its 1st level descendants are synchronized, etc.

Search depth configuration has no effect on the groups’ synchronization (see below).

d) Sync only active users of licenses

It is highly recommended to check the **Sync only active users of licenses** in order to avoid adding users that do not actively use the application. New active users would be added to the list of users as they check out a license, and their LDAP details would be synchronized when the **Sync time interval** elapses.

Group Synchronization settings

Users’ or Computers’ synchronization can be done either with or without synchronization of LDAP groups. In order to enable Groups synchronization, expand the “Groups synchronization settings”.

Group Syncronization

Group synchronization introduces groups in the OpenLM database according to information read from the LDAP.

Preview

At any stage you can click the magnifying glass icon, to get a preview of the groups as they would be synchronized into the OpenLM database (At the time of writing this revision – 0.1, preview is only implemented for Hierarchical types of synchronization). The image below shows the preview window:

a) Set Default group

Setting a user’s default group is done by checking the **Set Default group** in the OpenLM server configuration tool. This setting determines that the 1st group a user has been found a member of during synchronization, other than the OpenLM_Everyone group, would be declared as that user’s default group

b) Search depth

Configure the depth of search for the synchronized groups:

‘0’ (default): Full tree group hierarchy is synchronized.

‘1’: Only the start node group is synchronized.

‘2’: The start node group and its 1st level descendants are synchronized, etc.

Search depth configuration has no effect on the Users’ and Computers’ synchronization.

There are several different types of group synchronization schemes:

No Groups:

The default choice for groups synchronization is – No groups. This choice negates any configuration done in the group synchronization frame.

Flat:

This option enables the administrator to associate a particular group name to all synchronized users. The ‘Fixed’ name typed in the textbox is the group name of the users that would consequently be synchronized in this method.

Hierarchical:

OpenLM can create users’ and computers’ groups according to the hierarchical LDAP node tree. The synchronized group entities include OUs (Organizational Units), Security groups and Distribution groups. The user can set the synchronization scheme to include any combination of these entity types.

- Hierarchical – OUs (organizational units): This option is in use by organizations that have an organizational hierarchy represented in the LDAP; for example departments nested inside divisions. By selecting the OU synchronization method, users would be introduced into groups in the OpenLM database. These groups would be named after the LDAP OUs under which the users have been created.

- Hierarchical – Security Groups: This option goes through the list of users that populate

Security groups' nodes beneath the selected node. OpenLM groups are named according to these LDAP Security groups.

- Hierarchical – Distribution Groups: This option goes through the list of users that populate Distribution groups' nodes beneath the selected node. OpenLM groups are named according to these LDAP Distribution groups.

- Hierarchical – "Start node becomes a group": Select this check box in order to include the start node entity in the OpenLM groups.

Attribute:

OpenLM groups are created according to specific attributes their members have. In order to do that, select the **Attribute** radio button, and pick up a suitable attribute from the adjacent drop-down list of attributes. Examples for attributes are: "Division", "Employee ID", "Initials" or "Cost center". Type in a Regex expression that would articulate the required attribute.

The EasyAdmin Synchronization interface

OpenLM EasyAdmin shows users, computers and group entities as they have been introduced by the LDAP synchronization. In order to run the LDAP synchronization process (without having to wait for the synchronization period to elapse):

- Click the EasyAdmin Start button.

- Select **Administration** and **Sync Definitions**. The LDAP synchronization window opens.

- Click **Sync Now** link to start synchronization.

- Click **Administration** and then **Entities** to open the **LDAP Entities** window:

- From the **LDAP Entities** window, you can review the entities as they were read from the LDAP. Use the filter pane on the left side of the **LDAP Entities** window to select specific synchronization schemes, entities, entity types and Synchronization dates. You can also mark certain entities as ignored, and remove ignored entities from display.

- To find **Relations** select from the **Administration** window. The **LDAP Relations** window opens:

- The image above shows the **Relations** display for user U_A1. Note that the groups in which U_A1 is a member of are displayed, as well as the Synchronization name and the date of synchronization.

- Click on a specific entity name link, e.g. U_A1. The **User Details** window opens:

This window presents the LDAP synchronized information for that user. Additional information is available in the **Project** and **Groups** sub-menus.

User cleanup

Sometimes users get introduced into the OpenLM database by mistake. This may culminate to an annoying amount of users which makes browsing EasyAdmin cumbersome. OpenLM enables administrators to permanently delete the user pool, so that these users would not be synchronized again.

In order to activate this cleanup utility, click the EasyAdmin ‘Start’ button, select

Administration and **Cleanup initializer**.

For more information on the cleanup process, see the Cleanup case study below.

Case study

In order to demonstrate the different group synchronization methods, we have created the following OU structure, and enabled all users.

In this diagram:

- Organizational units are marked by blue triangles.
- Groups are marked by yellow ellipses.
- Users are marked by small rectangles.
- The bubbles mark nodes where users have been defined.
- 3 computers were defined in under operational units OU_AB, OU_A and OU_B. They are marked by green starts and are named Comp-AB, Comp-A and Comp-B respectively.
- OU_AA & OU_BB and their subsequent groups and users were only configured on the later case studies (see below).

CASE 1A: SYNCHRONIZE USERS AND COMPUTERS ONLY

Procedure:

OU_AB was selected as the start node.

Two parallel synchronization schemes were configured: for users and computers.

Group synchronization was not configured.

Outcome:

All Users and Computers were synchronized. No Groups or OUs were synchronized.

Observed:

The Entities' window contains LDAP users and computers:

Computers are presented in the "Workstations" window:

CASE 1B: NO GROUPS

Procedure:

Similar to the previous case 1a, OU_AB was selected as the start node. The same two synchronization schemes were configured: for users and computers. Group synchronization was opened, but the "No Groups" radio button was selected.

Outcome:

Similar to the previous case, all Users and Computers were synchronized. No Groups or OUs were synchronized.

CASE 2: FLAT SYNCHRONIZATION

Procedure:

OU_AB was selected as the start node.

Users synchronization was configured to include all users under that start node.

Groups' synchronization was configured 'Flat'.

Outcome

All users were synchronized, and gathered under the 'MyFlatGroup' group:

CASE 3: HIERARCHICAL SYNCHRONIZATION: USERS, COMPUTERS, OUS AND GROUPS

Procedure:

OU_AB was selected as the start node.

Two parallel synchronization schemes were configured: for users and computers.

Hierarchical group synchronization was configured to include all: OUs, Security Groups and Distribution groups.

The hierarchical group search depth was set to '0': Full tree.

Outcome:

All groups, OUs, users and computers beneath OU_AB were synchronized. The Hierarchical tree was preserved.

Observed:

The EasyAdmin Entities and Relations' windows display all LDAP entity information:

EasyAdmin groups show all groups in a Hierarchical tree. Users are assigned as members of these groups. In the example below, user U_AA1 is shown to be a member of group G_AA1

CASE 4: HIERARCHICAL SYNCHRONIZATION – SEARCH DEPTH 2 (USERS) 2(GROUPS)

Procedure:

OU_AB was selected as the start node.

Hierarchical group synchronization was configured to include all: OUs, Security Groups and Distribution groups.

User search depth was set to 2.

Groups search depth was set to 2.

Outcome:

All OUs and groups in the uppermost entity and its immediate descendants were synchronized.

All users which were declared in the uppermost entity and its immediate descendants were synchronized.

Observed:

Users were properly grouped within these limitations.

CASE 5: HIERARCHICAL SYNCHRONIZATION – SEARCH DEPTH 2 (USERS) 1(GROUPS)

Procedure:

OU_AB was selected as the start node.

Hierarchical group synchronization was configured to include all: OUs, Security Groups and Distribution groups.

User search depth was set to 2.

Groups search depth was set to 1.

Outcome:

Only the uppermost entity OU_AB was synchronized.

All users which were declared in the uppermost entity and its immediate descendants were synchronized.

Observed:

Group OU_A contains all the synchronized users that were declared beneath it.

Case 6: Synchronize only Active users

Procedure:

OU_AB was selected as the start node.

Hierarchical group synchronization was configured to include all: OUs, Security Groups and Distribution groups.

The hierarchical group search depth was set to ‘0’: Full tree.

The “Sync only active users of licenses” box was checked, and the user U_A1 logged into EasyAdmin in order to establish its status as an active user.

Outcome:

All LDAP groups were introduced in the OpenLM database.

Only user U_A1 appears in the Users window. U_A1 was synchronized to the LDAP, hence its attributes (First name, Last name, Department) are also presented.

CASE 7: SYNCHRONIZE ONLY USERS WITHIN SECURITY GROUPS

Reminder:

User U_B1 was grouped under G_B1, but was created in Organizational unit OU_AB

Procedure:

OU_B was selected as the start node.

Users' synchronization was configured to include only users within Security groups.

Group synchronization was not configured.

Outcome:

All user beneath the OU_B node, that were grouped under security groups were synchronized.

CASE 8: SYNCHRONIZE ONLY USERS WITHIN OUs

Procedure:

OU_B was selected as the start node.

Users' synchronization was configured to include only users within OUs.

Group synchronization was not configured.

Reminder:

User U_B1, U_AB2 and U_BB1 are members of groups under the OU_B Organizational unit. However, only U_BB1 was declared in OU_BB1, which resides beneath the start node OU_B

Outcome:

Only user U_BB1 was synchronized.

CASE 9: ATTRIBUTES

Reminder:

- Users U_A1 & U_B1 have been defined owning “department” attributes with the value “olm_drink”.
- Users U_AA1 & U_BB1 have been defined owning “department” attributes with the value “olm_food” (See LDAP diagram).

Procedure:

OU_AB was selected as the start node. The “Attribute” group synchronization method was chosen. The ‘department’ attribute with the regular expression (‘Regex’) value olm_(.*) was configured in the LDAP configuration form. This regular expression would create a group for each department attribute that starts with olm_, i.e. food & drink.

Outcome:

- All Users in OU_AB were synchronized.
- Users U_A1 & U_B1 are members of the drink group.
- Users U_AA1 & U_BB1 are members of the food group.

CASE 10: USER CLEANUP

Procedure:

OU_B was selected as the start node.

All users under this node were synchronized.

Cleanup was applied.

OU_AB was selected as the start node, and a 2nd phase of synchronization was applied.

Outcome:

Only users which were not declared under the OU_B node remained.

Observed:

After Synchronizing OU_B, all users beneath that start node were present:

Then the cleanup was applied to users:

And the users disappeared:

After that – synchronization of OU_AB was applied. All entities from both synchronization processes appear in the entities window, but only OU_AB users that were not part of OU_B were synchronized and appear in the users' window.

In particular, U_AB2 which was a member of the first synchronization hierarchy will be omitted from the users' list in the cleanup process, and will not be reinstated there after the 2nd synchronization.

Case 11: Groups Cleanup.

In the current version (1.8.16) Groups cleanup is not yet implemented.

See more details on the cleanup manager in this document.