redmineorg-copy202205 - Vote #67477

Association of an LDAP group to a Redmine group

2022/05/09 14:47 - Admin Redmine

ステータス:	New	**開始日:**	2010/06/23
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	LDAP_28	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/5742	**status_id:**	1
category_id:	28	**tracker_id:**	2
version_id:	0	**plus1:**	1
issue_org_id:	5742	**affected_version:**	
author_id:	17011	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	6		

説明

It should be possible to add *LDAP based auth_source mode* also for *Redmine groups*.

A +Redmine Group+, is an entry in the "users" table which has value of "type" column equal to "group", should have capability of having an "auth_source_id" value which represent the association to new type of auth_source that points to an +LDAP group+:

- +LDAP users+ authenticate in redmine as a "Redmine Users" using LDAP auth_source.
- +LDAP users+ belong to a +LDAP group+.
- +Redmine groups+ with LDAP auth_source are associated to +LDAP group+.

Within a project, it should be possible to add +Redmine roles+ to these LDAP based +Redmine groups+ as usual (and transparently), as the in model it only change the value of the auth_source_id.

But the belonging of a LDAP based "Redmine User" to LDAP based +Redmine groups+ (both entry have an auth_source_id) should be performed using a LDAP query instead of checking the "groups_users" table.

By a quick inspection of the code, the activity may imply:

- modify model, controller and views for auth_source so to allow management of this new type of auth sources
- manage the user group associations in case group has an LDAP based auth_source_id (I don't know which part of the code has to be changed for this) by executing a LDAP query instead of a SQL query on the groups_users table

Informations:
A valid LDAP group is identified by a DN (for example: CN=ACL-SVN-ADMIN,OU=SVN,DC=foo,DC=myco,DC=com)
it have a objectClass attribute of value "groupOfUniqueNames", and has many "uniqueMember" attributes with value containing the DN of LDAP users.

It is possible to query LDAP Server for belonging of a LDAP user to this kind of LDAP groups.

Motivations:
This would allow to sync Redmine users to LDAP based Subversion repository as described into this tutorial:
http://pteropus.blogspot.com/2008/04/securing-subversion-via-ldap.html

journals

Related to #1113, #4755

This would be a very useful feature. Right now our AD is setup in such a way that I cannot restrict users by OU, and anyone with an account can login (staff¦faculty¦students¦etc). Which we want them to be able to log in. However, this creates a problem for us when our only option for giving staff the rights to create projects is to allow all authenticated users to create projects.

+1

We are already using redmine, subversion, jenkins, sonar, nexus, openfire from the same user base and the only system which doesn't support ldap completly (mean groups) is redmine.

The most important feature of ldap beyond authenfication is grouping of users. This way we can make groups which holds users for roles on one place (ldap server) which is used by all systems.

My approach for a full ldap group support in redmine is minimal invasive:

First step:
Admin selects potential groups in ldap, that get known in redmine
Redmine should do an "on the fly" lookup if admin enters group search string. The admin can select groups from query result for setup in redmine. In Redmine group view, Groups which still exists in ldap get marked so you can distinguish them to "internal only" redmine groups or groups that has been deleted in ldap.

Second step:
The admin assigns projects and roles to that groups

Third step:

User authentification and "on tfe fly" project/role assigment via ldap group on login

If users logs into redmine, user gets authenticated agaist ldap and if valid redmine retrieves all ldap groups for that user - but only for configured group DN. Then redmine filters alls groups that exists in ldap and corresponding ones in redmine with same name. Groups don't get deleted in redmine if no longer exists in ldap on next check (on login or group configuration in admin gui), but get marked so that it is visualized it is no ldap any longer. Also if ldap group(s) no longer exists (can be made optional by checkbox, so internal groups can be used also) group(s) won't get used for project-role authorization.

This approach checks user group memberships in ldap and group existence in ldap on the fly and don't imports and synronizes all ldap groups all the time.

h2. Redmine Plugin : Add LDAP Users to Group

I just made some plugin that could help people with Redmine ~3.2

> Redmine plugin that automatically adds newly logged-in LDAP users to specific group that is configurated in plugin's settings.

https://github.com/savoirfairelinux/redmine-add-ldap-user-to-group

---

related_issues

relates,New,1113,Link LDAP groups with user accounts
relates,New,4755,Create and maintain groups from LDAP attributes
relates,Closed,5702,Please add ldap filters for authentication
relates,New,6202,On-the-fly group addition based on LDAP sources

履歴

#1 - 2022/05/10 17:22 - Admin Redmine

- カテゴリ を LDAP_28 にセット