redmineorg-copy202205 - Vote #63101

Link LDAP groups with user accounts

2022/05/09 13:19 - Admin Redmine

ステータス:	New	**開始日:**	2008/04/25
優先度:	通常	**期日:**	
担当者:		**進捗率:**	30%
カテゴリ:	Accounts / authentication_7	**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/1113	**status_id:**	1
category_id:	7	**tracker_id:**	2
version_id:	0	**plus1:**	3
issue_org_id:	1113	**affected_version:**	
author_id:	848	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	25		

説明

It would be a great feature for corporate wide use of Redmine, to be able to link users according to LDAP groups.

For example, when a user logs into the tool, and he is part of group A, then he should get "Member" permissions. When another user, not part of group A, logs into the tool, he should automatically get "Non-Member" permissions for example.

My reasoning behind this request is that, currently when using LDAP authentication, you set up Redmine to be accessible by anyone in the company that has an LDAP account. However, you would like to break that superset down into a subset of people that can for example see files & repositories for all projects, using LDAP groups.
Yes, the above is possible if you add the user to every single project, however with 100+ projects, it would be painful to add a new user.

Hopefully this is possible!

journals

Together Feature #1131, apache, mod_auth_krb5 this should provide complete authentication and authorization environment for enterprise environment.

The authentication port is handled by the web server, the result user is put into environment variable, the application should accept this as-is.

Then the application should fetch user groups from LDAP and allow simple transformation, for example, user@REALM should be converted to userPrincipalName=user@realm, then constructed into LDAP query which returns group DN. Each group DN should be linked to roles.

End result: No users are defined inside application. User permission is based on their LDAP group membership.

Also, more information may be fetched from LDAP, for example: full name, email.

For the email field, there also can be an option to construct it from user name, for example if user name is user[@RELAM], then email is user@domain.org, this will enable simple way to construct address without LDAP support.

Thanks!

This would be a very interesting feature to be implemented with the new 'User Groups' (in version 0.9, Issue #1018).

Would this work ? :

- When a user logs in with ldap, the list of groups he is in is fetched from ldap.
- For every of these groups, we check if a group with the same name already exists on the redmine site.
- If it does, add the user to the group.
- +Same for removals if he is no longer in the group

I guess this could be quite slow and would maybe need some optimization...

Any idea on this ?

What about http://www.redmine.org/boards/1/topics/10008 ?

If this could still be included in v0.9, with the Groups feature it would really be great...

alten benelux wrote:

> This would be a very interesting feature to be implemented with the new 'User Groups' (in version 0.9, Issue #1018).
>
> Would this work ? :
>
> - When a user logs in with ldap, the list of groups he is in is fetched from ldap.
> - For every of these groups, we check if a group with the same name already exists on the redmine site.
> - If it does, add the user to the group.
> - +Same for removals if he is no longer in the group
>
> I guess this could be quite slow and would maybe need some optimization...
>
> Any idea on this ?

This is almost exactly what I have done, except that if the

- When a user logs in with ldap, the list of groups he is in is fetched from ldap.
- For every of these groups, we check if a group with the same name already exists on the redmine site.
- If it doesn't, add the group
- Check if the user belongs to this group in redmine
- They they don't, then add the user to the group.

The code doesn't do removals at the moment. I also don't know what would happen if there was 100 groups and 10000 users - I don't know how well it would scale. The code doesn't deal with groups on the users, if the list of groups is stored in multiple memberOf attributes of the user in LDAP (I think AD does it this way).

Here is a patch implementing the import of LDAP groups. The patch is based on http://www.redmine.org/boards/1/topics/10008 but membership is detected using 'uniqueMember' LDAP attribute (not memberOf)

I would very much like to see this functionality in the trunk. We're currently using a hack that we would be more than happy to get rid of but would prefer if the solution came in the form of a patch applied to the trunk instead of applying it to the codebase ourselves.

I'm starting to work on some LDAP features for a customer, including linking them to groups in Redmine. A few of the new features have been added to a plugin in the form of Rake tasks. Feel free to try it out but it's still under active development.

http://github.com/edavis10/redmine_extra_ldap

You may also be interested in #4755.

We want to use Redmine in Enterprise Environment but we need to use the ldap groups, cause need of central user/group managment. The groups are used also for other middleware developing inftrastructure like Hudson, Nexus, etc..

The Patch seems to go deep into the base and i am afraid of getting into troubles using redmine too far away of the main stream, then getting update problems and problems with other plugins.

Will this feature streamed into the trunk .. or why not? I couldn't find it on the roadmap.

Tx for information!

I'd like to see this either A) included with core redmine.. or B) have all LDAP features extracted to a plugin so LDAP can be developed in a single place.

Anyway .. I'm about to try your extra_ldap plugin now..

Thanks

It would be nice to have the "uniqueMember" parameter a variable so that we can customize it to our schemas (we use memberUid), but otherwise this patch seems like a good fit for our needs. I don't see how the extra_ldap plugin resolves the issue however, maybe I'm missing something?

Here's some modifications I've done from Natalia Lebedeva's patch.
Basically just made sure it pulled the user object only once pr. group, and made it pull all Redmine groups from the database and tries to remove you from every group in Redmine.

Since Natalia's patch already makes sure to create group and member group assosications, I found this the easiest way to deal of removal. Problem is that this probably doesn't scale very well as already mentioned, as this happens on every user login..

My modified patch is available here: https://gist.github.com/25e3df445eff2ab6a460 (rev c50cf3 at the time of writing). Note that I've changed the ldap filter lookup to "memberUid" as we use the nis.schema in our LDAP.

I assume the solution for making this scale rather well, is to make this task a cronjob task:

- Basically does the same as the patch
- Just make sure the actions in the patch runs as a transaction, so user doesn't notice he "was" removed from all the groups and added again. If the user is requesting project A which requires group Y while the transaction is running, this will only turn into a "tiny" longer waiting time (page load) then usual I think.

There's "two" problems with the cronjob deal:

- LDAP changes won't reflect right away, but just on every "sync" when the cronjob is doing it's tasks.
- Setuping up the cronjob is not out of the box as simply deploying Redmine, you actually need to setup the cronjob (but imo, if your dealing with deploying Redmine & LDAP - you probably should know how to setup a cronjob..)

We use Novell edirectory which has beyond "normal" groups a kind of "dynamic/virtual groups":
http://support.novell.com/techcenter/articles/ana20020405.html.

...
Dynamic groups let you specify the members of a group using a search filter. The members of a dynamic grou
dynamically by the eDirectory server(s) whenever the groups are accessed or evaluated. This makes it easier for a
p objects together because membership can be based on a certain criterion, without having to manually add each
he Group object..

As i understood this group type there is no memebership attribute at the member defined, but a group definitions referencing alls memebers via search filter query. So it would need to join the query result with the memeber(s) in redmine to evluate if its a members or not.

Will this patch also work with this kind of groups?

Hello,

I desperately need this feature. Redmine would be a no-go for the company here, otherwhise.
Tried to use the plugin, but I couldn't figure out what it does, if it does anything.

Attached is a modified version of Roy Sindre Norangshol's patch, with following changes:

- Well, I removed the deletion part, feel free to re-add it from Roy's patch, if needed/wanted.

- shorten the group CN if it's longer than 30 chars (braindead lastname.length limitation)
- check if the user exists already, as it would fail with on-the-fly registration (user get's created after authenticate(login, password) somehow).
- AD style: search for "member:" attribute containing user's DN, not memberUID. Should still be made configurable.

Now with this and on-the-fly registration turned on, it works, but users have to login twice.

+1

+1 !

+1

There is a new plugin for "ldap sync":
https://github.com/thorin/redmine_ldap_sync/blob/master/README.md

You can check :
https://github.com/Utopism/redmine_ldap_sync

a fork of the ldap_sync plugin with enhancements.

Why a cache?
Dynamic groups?

Jérôme BATAILLE wrote:

> You can check :
> https://github.com/Utopism/redmine_ldap_sync
>
> a fork of the ldap_sync plugin with enhancements.

---

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,5742,Association of an LDAP group to a Redmine group
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 17:29 - Admin Redmine

- カテゴリ を Accounts / authentication_7 にセット