redmineorg-copy202205 - Vote #65237

Advanced LDAP authentication

2022/05/09 14:03 - Admin Redmine

ステータス:	New	**開始日:**	2009/05/13
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:	Candidate for next major release_32	**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/3358	**status_id:**	1
category_id:	28	**tracker_id:**	3
version_id:	32	**plus1:**	0
issue_org_id:	3358	**affected_version:**	
author_id:	5352	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	47		

説明

This patch adds the following new features to LDAP authentication:

- using dereferencing aliases on search
- ability to select protocol LDAPv2 or LDAPv3
- connect using STARTTLS
- selecting server certificate validation level
- user-definable custom search filter
- bind as current user instead of admin account, see Feature #1913
- searching is sub-tree by default, in future GUI option may be added to configure this

If custom search filter is used, @$login@ is replaced with the username. For example, to search for users with objectClass posixAccount, use this filter string: @(&(uid=$login)(objectClass=posixAccount))

Note that this patch uses Ruby/LDAP instead of Net::LDAP, so this should be installed, for example on Debian, use @apt-get install libldap-ruby1.8@

After applying this patch, run @rake db:migrate RAILS_ENV="production"@, as auth_sources table is modified in the database. (filter, dereference, starttls, require_cert and protocol_version columns are added)

journals

Hello,

Are there any plans to integrate this or something similar to the next redmine release?

Thanks!

Hi,
i tried your patch against current trunk, and it doesn't work very well :
using a working set of params for creating an ldap authentication mode,
with redmine trunk the "Test" button works ok,
and with your patch i get that log :
Connecting to localhost:389, tls=false
Dereference set option
Trying to bind
Bind as user admin
LDAP Connect Error: Invalid DN syntax

The actual parameters are very simple :
host: localhost
account: admin
password: admin

Base DN: dc=localhost

and i set :
login: cn
firstname: givenName
lastname: sn
email: mail

of course the ldap objects have those four non-empty attributes

---

oops, sorry, actually it's the redmine trunk that wrongly reports the connection succeeds

i guess i'm not used to ldap ;)

ok, it works, my mistake.
Thanks !
The db migration maybe is screwing existing ldap authentication modes,
for example i had to re-enter "Account" field to get it working.

I hope that patch makes its way to trunk,
since dropping old ruby-net-ldap plugin seems a very good idea,
and your patch looks clean and simple.

Here's a patch to be applied over yours, that adds ldap synchronisation for "firstname, lastname, mail" attributes.
When one user changes these attributes using "My account" page, it updates them in ldap.
I thought it is logical to keep those three attributes synchronised ?

Maybe the auth_source should offer an option for this ?

This improved patch synchronises "firstname, lastname, mail" from LDAP to DB at login,

and from DB to LDAP when user changes his attributes.

Jérémy Lal wrote:

> This improved patch synchronises "firstname, lastname, mail" from LDAP to DB at login,
> and from DB to LDAP when user changes his attributes.

Looks good, but at least in the admin view, I don't see changes I made to another user on the LDAP backend... Can you confirm it works for you?

Felix Schäfer wrote:

> Hello,
>
> Are there any plans to integrate this or something similar to the next redmine release?
>
> Thanks!

I've tried to contact Jean-Philippe Lang two months ago, however I received no response yet. I'll update this patch to 0.8.4 soon. (Maybe to the current trunk as well.)

Jérémy Lal wrote:

> I thought it is logical to keep those three attributes synchronised ?
> Maybe the auth_source should offer an option for this ?

Yes, it is logical, however there are many cases where there is no option to modify the LDAP. So I think there should be a checkbox on the LDAP auth source configuration page which tells if update is allowed or not. I've not tried your patch yet, just looked at the source, but for me it seems there is no way to disable this feature.

Daniel Marczisovszky wrote:

> Felix Schäfer wrote:
>
> > Are there any plans to integrate this or something similar to the next redmine release?
>
> I've tried to contact Jean-Philippe Lang two months ago, however I received no response yet. I'll update this patch to 0.8.4 soon. (Maybe to the current trunk as well.)

works fine for me so far (against current trunk).

Does anyone know a quick tutorial to setup an LDAP server to test this on? If I can get one running locally, I can review this patch (and #3253) and see about fixing this issue.

Eric Davis wrote:

> Does anyone know a quick tutorial to setup an LDAP server to test this on? If I can get one running locally, I can review this patch (and #3253) and see about fixing this issue.

I can write a tutorial for you, but please tell which operating system are you using. Maybe I can set up a public test LDAP server, but I have to look for an available machine :)

Jérémy Lal wrote:

> This improved patch synchronises "firstname, lastname, mail" from LDAP to DB at login,
> and from DB to LDAP when user changes his attributes.

The patch redefines the "update" method for app/models/auth_source_ldap.rb , which ultimately breaks saving of an LDAP auth source, because ActiveRecord already has an update attribute, see http://api.rubyonrails.org/classes/ActiveRecord/Base.html#M002560 . I have renamed the method to update_user and changed (my patched) app/controllers/my_controller.rb accordingly. Another thing I'd like to see here: the logic to chose between updating the user attributes to the DB or to LDAP should be done in the user model, not the user controller, I haven't looked deep enough if the actual LDAP code should stay in the auth_source or go in the user model too, but I might do once I'm through with my exam next week.

Another thing that goes wrong in the patch: I haven't tested if it works well without a filter, but I think it would be the same: you provide ldap_con.modify with something akin to an LDAP search string, where it awaits a DN, so you need to do an LDAP search with the search filter you create and feed the result do ldap_con.modify.

What I'd really like now is some more LDAP integration, like custom user fields populated by LDAP attributes, and user groups in redmine mapped to the LDAP groups, that would be even better :-)

Daniel Marczisovszky wrote:

> I can write a tutorial for you, but please tell which operating system are you using. Maybe I can set up a public test LDAP server, but I have to look for an available machine :)

Debian Linux would be best, Ubuntu would be ok.

Eric Davis wrote:

> Debian Linux would be best, Ubuntu would be ok.

@apt-get install slapd@

It will ask for your administrator password
You have to confirm the password

Ok, OpenLDAP is installed.

Your default base DN will be your domain name, for example if
your FQDN is ldap.redmine.org then your base of the LDAP directory will be:
dc=redmine,dc=org

Your default user is:
cn=admin,dc=redmine,dc=org
(use the password specified during the install)

@apt-get install ldap-utils@

To search in your LDAP:
@ldapsearch -b dc=redmine,dc=org -x -D cn=admin,dc=redmine,dc=org -W objectClass=*

I usually use this small Java based GUI tool to manage LDAP:
http://www.brothersoft.com/ldap-browser-download-14779.html

I can create a sample LDAP tree that you can import into yours. Moreover (as I created this test machine in VMWare) I can send you the virtual machine.

I added a patch to redmine/extra/svn/Redmine.pm (apache auth source for svn server) to honor my (#1913) LDAP modifications. It might be a good idea to add your features to this tool as well... :-)
[[http://www.redmine.org/attachments/2454/Redmine-ldap-as-user.diff]]

Another thing: Did you consider implementing search scope selection? To me this is a showstopper as I need to have a scope of "one"... :-(

Adi Kriegisch wrote:

> I added a patch to redmine/extra/svn/Redmine.pm (apache auth source for svn server) to honor my (#1913) LDAP modifications. It might be a good idea to add your features to this tool as well... :-)
> [[http://www.redmine.org/attachments/2454/Redmine-ldap-as-user.diff]]

I'm afraid I can not add these, even I'm not using SVN integration for Redmine. However, I can help to create to common class/codebase to make these LDAP features available to these modules/patches.

> Another thing: Did you consider implementing search scope selection? To me this is a showstopper as I need to have a scope of "one"... :-(

Noone was interested till now ;) but I will add this (hopefully) within a week.

I'v implement the patch ldap_update to my redmine release but when submiting user informations, i got an internal error.
Do you know this problem ?

Florian Collot wrote:

> I'v implement the patch ldap_update to my redmine release but when submiting user informations, i got an internal error.
> Do you know this problem ?

I've renamed @user.auth_source.update to update_user in the model and the controller, so i have no more Internal Error, and when submiting, i got a redmine success. But, my ldap entry is not updated. What's wrong ?

Florian Collot wrote:

> I've renamed @user.auth_source.update to update_user in the model and the controller, so i have no more Internal Error, and when submiting, i got a redmine success. But, my ldap entry is not updated. What's wrong ?

I think you got it backwards.Vanilla Redmine fetches information from LDAP only to populate some or all of the fields of a user at creation time, the patch does refresh the Redmine user attributes from the LDAP attributes every time the user logs in. In either case, Redmine reads the LDAP fields, but never updates them.

Felix Schäfer wrote:

> I think you got it backwards.Vanilla Redmine fetches information from LDAP only to populate some or all of the fields of a user at creation time, the patch does refresh the Redmine user attributes from the LDAP attributes every time the user logs in. In either case, Redmine reads the LDAP fields, but never updates them.

Thanks to your quick answer !
your project is really beautiful even though at present it is not possible to update the Active Directory entries :-) It doesn't matter, and it may be better so that users cannot update their informations themselves

Thx !

Florian Collot wrote:

> Felix Schäfer wrote:
>
> > I think you got it backwards.Vanilla Redmine fetches information from LDAP only to populate some or all of the fields of a user at creation time, the patch does refresh the Redmine user attributes from the LDAP attributes every time the user logs in. In either case, Redmine reads the LDAP fields, but never updates them.
>
> Thanks to your quick answer !
> your project is really beautiful even though at present it is not possible to update the Active Directory entries :-) It doesn't matter, and it may be better so that users cannot update their informations themselves
>
> Thx !

Florian Collot wrote:

> Thanks to your quick answer !

Pas de problème :-)

> your project is really beautiful even though at present it is not possible to update the Active Directory entries :-) It doesn't matter, and it may be better so that users cannot update their informations themselves

Well, I have a POC to read the user attributes from LDAP each time the user object is instantiated, so that they are always fresh, not only when the user logs in, but that goes well over the intended use of the auth_source, so I'm not sure as what I should file it... I'll try to clean up the code and update it against current trunk, and send a patch.

Hi,
Just wanted to thank you Daniel for your great patch ! Thanks to this patch, my redmine install can now authenticate my users against my ldap server which requires a TLS encrypted connection :-)

May i suggest however that requiring to check the **START_TLS** option *and* the **LDAPS** when using a start_tls connection is a little bit

confusing.
As you know, LDAPS and start_tls are two different way to secure the connection to an ldap server. The LDAPS connection (which is a bit deprecated i think) is negociated on port 636 of the ldap server while the START_TLS connection occurs on the usual 389 port. See http://www.openldap.org/faq/data/cache/185.html

So i think that those two options should be mutually exclusive :-)

HTH,

I work for an edu and have a local department ldap, and campus wide ldap. I have the 2 setup currently and can login via each LDAP instance, thank you.

(1) How hard would it be to provide a drop down list to allow the user to select the LDAP source to authenticate against?

(2) ... Ideally as a user authenticates the 1st time and Redmine creates their account on-the-fly in Redmine ... I would the Admin to insert them into given projects then email them that their account is setup fully ...

If given a bit of pointers I hope I could create the patch for at least (1) above ... any feedback is appreciated.

regards,

David

Daniel Marczisovszky wrote:

> - ability to select protocol LDAPv2 or LDAPv3
> - connect using STARTTLS
> - selecting server certificate validation level
> - user-definable custom search filter
> - bind as current user instead of admin account, see Feature #1913
> - searching is sub-tree by default, in future GUI option may be added to configure this

Yes, it would be great to see this implemented in a next release, it would avoid to manually change the LDAP filter in app/models/auth_source_ldap.rb everytime a new release appears...

Anyone has a working patch for the latest trunk? We need TLS support but the patch is for a pretty old version of Redmine.

Updated patch of Daniel Marczisovszky to current version of redmine (1.2.1) and current trunk revision (r6417).

Also added german translations of new fields in settings form.

Günter Dressel wrote:

> Updated patch of Daniel Marczisovszky to current version of redmine (1.2.1) and current trunk revision (r6417).
> Also added german translations of new fields in settings form.

Do you think i can try to apply this patch on 1.2.2 stable redmine installation, anybody try ?
After that, can i have problem in the future to upgrade my installation ?

Thanks

You can try - of course :)
I have to mention that I run into one little problem once I tried to apply my updated patch to another instance of redmie.
It was about that one LDAP property was forgotten to overwrite (One line of code, it's about STARTTLS vs. classic TLS)
If you are not trying to connect via STARTTLS you will not experience a problem at all.

And yes - it would lead to inconveniences for further upgrades, since you patch the core files.
You'll need to patch those files after each upcomming upgrade again.

If you are still looking forward to test it, I'm willing to support you with further testing on 1.2.2

Regards,
gue

Günter Dressel wrote:

> You can try - of course :)
> [...]
> If you are still looking forward to test it, I'm willing to support you with further testing on 1.2.2
>
> Regards,
> gue

I try to patch my 1.2.2 version, i have no error when patching, but after that, redmine crash with error :

```
[ pid=8941 thr=-609826598 file=utils.rb:176 time=2011-12-09 20:01:03.799 ]: *** Exception PhusionPassenger::UnknownError in PhusionPassenger::ClassicRails::ApplicationS
pawner (no such file to load -- ldap (MissingSourceFile)) (process 8941, thread #Thread:0xb74d91b4):
from /usr/local/lib/site_ruby/1.8/rubygems/custom_require.rb:36:in gem_original_require'
from /usr/local/lib/site_ruby/1.8/rubygems/custom_require.rb:36:inrequire'
from /usr/lib/ruby/gems/1.8/gems/activesupport-2.3.11/lib/active_support/dependencies.rb:184:in `require'
from /var/www/redmine/app/models/auth_source_ldap.rb:20
```

Thanks for your help

SR.

I install libldap with apt-get install libldap-ruby1.8, and after i rake,

i have successful connection when i test in ldap_authentification, but when i try to enter a user + pass, i cannot login ...

OK, after many test, i attach the png of my configuration, and a txt file with log of the "test" button on ldap auth page.

When i try to enter a login and password on login page, i have no debug in the log file of slapd, so ... ?

Is it still needed for redmine 2.0.0 ? somebody has already tested this patch with 1.4.x or 2.0.0 ?

Especially considering ruby-net-ldap is now 0.3.1

The latest net-ldap (0.3.1) supports STARTTLS.

My patch for STARTTLS was merged three years ago.

Hi,

any news on this? This could be very helpful for our windows users! :-)

Any solutions to this? It is still not working with the latest version of Redmine. There is still no option to ignore the certificate check which is rather important. Since the file structure changed a lot, the applied patches do not work anymore.

I think that "redmine_ldap_sync":http://www.redmine.org/plugins/redmine_ldap_sync should serve as a model how this should get implemented. Actually, why not merging code of the plugin (after review) to the Redmine, as it works like a charm at the moment.

This is a quick fix to get STARTTLS working for 2.2.3, just an update of the most recent patch above. There isn't much point in doing too much work on this patch, as moving back to Net::LDAP seems much more logical anyway, but until one of us gets a chance to rewrite it properly this should restore the functionality for those who need it (like me).

Note that this does effectively remove some of the more recent improvements to Redmine LDAP, such as validating the LDAP filter, but should still do what the original patch was intended to. This may be obvious to others, but you need LDAPS checked for STARTTLS to work with port 389 and, if you are using an LDAP filter with Redmine 2, don't forget to add (&(uid=$login)...) to it.

Correct me if i am wrong, so StartTLS(389) for LDAP is not supported in the latest Release of redmine?

If you need to use *StartTLS* instead of *SSL* (PORT 689), just edit the file

/app/models/auth_source_ldap.rb

in Linie 135, replace *simple_tls* with *start_tls*, save the file & restart Apache. Also under the LDAP web Interface settings check LDAPS with port 389,
StartTLS should work now!

tested on:

Redmine version 2.5.2.stable.13231
Ruby version 1.9.3-p194 (2012-04-20) [x86_64-linux]
Rails version 3.2.19
Environment production
Database adapter Mysql2

Please merge this patch into the repo or create a new patch to implement STARTTLS for LDAP.

Thanks.

---

related_issues

relates,New,3253,LDAP Auth : Alias Dereference
relates,Closed,29606,Support self-signed LDAPS connections

履歴

#1 - 2022/05/10 17:25 - Admin Redmine

- カテゴリ を LDAP_28 にセット

- 対象バージョン を Candidate for next major release_32 にセット