Redmine - Defect #10963

Encrypting LDAP/Repos passwords on the database prevent LDAP Authentification on Repos/Apache from working

2012-05-18 03:04 - Alexandre VIAL-BOUKOBZA

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	SCM extra	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix	**Affected version:**	1.4.2

Description

Short version of reproducing the case:

- Configure LDAP Connection WITH an account/password (Active Directory for exemple)
- Configure Authentification on Apache with Apache2::Redmine Authen::Simple::LDAP (and IO::Socket::SSL for LDAPS) for SVN/Mercurial serving.
- Define a value for "database_cipher_key" on configuration.yml
- execute rake to encrypt password => rake db:encrypt RAILS_ENV=production

You will get messages like [error] [Authen::Simple::LDAP] Failed to bind with dn '<account>'. Reason: '80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 52e, v1db1^@'

To Fix IT (but with the price of loosing repos/ldap passwords encryption on the DB):
- "rake db:decrypt RAILS_ENV=production"

Related issues:

Related to Redmine - Patch #17368: Enable encrypted LDAP passwords with Redmi...	**New**

History

#1 - 2012-05-21 20:27 - Jean-Philippe Lang

- Category changed from LDAP to SCM extra

- Status changed from New to Closed

- Resolution set to Wont fix

Yes, Redmine.pm can not work when using password encryption in the database.

#2 - 2012-05-25 15:16 - Alexandre VIAL-BOUKOBZA

Thanks !

Maybe a comment could be added in the documentation to prevent users from doing this mistake ?

#3 - 2014-07-01 15:29 - Marcus Schmid

- File ciphered_ldap_passwords4Redmine_pm.diff added

As we encountered the same problem last week, we modified Redmine.pm (see attached patch file) so that it can -- if necessary -- decrypt the password used for binding to LDAP, using the same logic/process as redmine's own lib/redmine/ciphering.rb (i.e. decrypting values only when there's a key set and the text is encrypted).

We introduced a new apache configuration directive, RedmineDatabaseCipherKey, which must be set to the same database_cipher_key that's used in your config/configuration.yml of your redmine installation. Otherwise, Redmine.pm won't be able to correctly decrypt ciphered LDAP passwords.

The modifications don't change the currently exposed behavior; without RedmineDatabaseCipherKey being set and/or with an unencrypted database no decryption will be performed, leaving the passwords as stored in the database.

Nonetheless two new dependencies are introduced by these modifications: Crypt::CBC and MIME::Base64 are needed to handle the ciphered database contents; maybe these could be handled like the already present dependency on Authen::Simple::LDAP (using e.g. $CanUseCiphering), but that was out of our scope (which was, simply put, "get encrypted LDAP passwords to work").

#4 - 2014-07-02 18:30 - Toshi MARUYAMA

- Related to Patch #17368: Enable encrypted LDAP passwords with Redmine.pm added

#5 - 2014-07-02 18:32 - Toshi MARUYAMA

FTR: note-3 patch is posted in #17368, too.

#6 - 2014-07-03 07:40 - Marcus Schmid

Actually, the note-3 patch is different from the patch I submitted in #17368; as I wrote in note-3, there are two new dependencies on perl modules. The note-3 patch will cause Redmine.pm to abort if the dependencies are not met at runtime, which may cause confusion to the administrator of an existing redmine installation if the note-3 patch was applied to the official Redmine.pm and shipped, because it changes the behavior of Redmine.pm on servers not having the abovementioned perl modules Crypt::CBC and MIME::Base64 installed (i.e. "it crashes").

The patch I submitted in #17368 is "safe for upgrade/inclusion to production machines"; it checks whether the two perl modules it's depending on are available, and if they are not, no decryption will be performed (regardless of whether the other conditions like "cipher key set in apache config" or "database is encrypted" are met). Redmine.pm will just work like before the patch.

Therefore, Patch #17368 may IMHO be safely integrated into the official redmine distribution, while the patch from note-3 may break existing installations.

Files

ciphered_ldap_passwords4Redmine_pm.diff	2.5 KB	2014-07-01	Marcus Schmid