Redmine - Patch #29606

Support self-signed LDAPS connections

2018-09-13 15:35 - Gregor Schmidt

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	LDAP	**Estimated time:**	0.00 hour
Target version:	4.0.0		

Description

With the introduction of certficate checks to LDAPS connections in trunk #24970 (and maybe 3.4 in #29476), we should enable the user to fall back to the old behavior, where server certificates were not checked.

This is especially important, where *local* domain controllers and LDAP servers are used as an authentication backend. Because there servers will often use self-signed certificates.

The attached patch adds a configuration option to disable the certificate checks for LDAPS connections.

Implementation

The patch adds a new boolean column to auth_sources called verify_peer. The LDAP auth source edit screen is extended so that users may decide if they want to use "LDAP", "LDAPS without certificate check" (this one is new) or "LDAPS with certificate check".

Screen Shot 2018-09-13 at 14.24.18.png
Depending on the selected option, the tls and verify_peer attributes are set on the auth source.

Furthermore the patch extends the LDAP connection setup code, to use the newly introduced setting.

Backwards compatibility

To ensure backwards compatibility with the current Redmine trunk, the new column verify_peer defaults to true. This way, connections which use tls will continue checking the certificates.

If you want to stay compatible with the behavior in the latest Redmine release, then the default value should be false, since 3.4 currently doesn't verify certificates, as explained in #29476.

I chose to introduce a new column instead of changing the existing one, so that the db schema remains compatible with other auth sources, which may be used by plugins. Adding a new column, should not break any existing code.

Redmine.pm compatibility

Redmine.pm currently does not verify certificates.

A brief check suggests, that the library which is used in Redmine.pm simpy doesn't support checking server certificates. Therefore in order to properly secure LDAP authentication for SVN and/or to support this new configuration, Redmine.pm would need to switch to a different LDAP library. But this would be out of scope for this ticket. This patch neither improves nor worsens the security of Redmine.pm's LDAP authentication.

Related issues

- #24970 introduces server certificate checks for LDAPS for Redmine 4.0
- #29476 suggests to backport #24970 to Redmine 3.4
- #27071 seems to be facing the problem, that the certficate cannot be validated
- #3358 was suggesting (among others) a similar feature

The attached patch is targeted at r17480.

Related issues:

Related to Redmine - Defect #24970: Net::LDAP::LdapError is deprecated	**Closed**
Related to Redmine - Defect #29476: Update net-ldap to 0.16.0	**Closed**
Related to Redmine - Defect #27071: Error testing LDAPS Connection: "Unable t...	**Closed**

Related to Redmine - Patch #3358: Advanced LDAP authentication	**New**	**2009-05-13**
Related to Redmine - Defect #8068: LDAP Authentificaton doesn't verify certif...	**Closed**	**2011-04-05**

Associated revisions

Revision 17505 - 2018-09-23 15:28 - Jean-Philippe Lang

Support self-signed LDAPS connections (#29606).

Patch by Gregor Schmidt.

Revision 17506 - 2018-09-23 15:33 - Jean-Philippe Lang

Adds translation strings (#29606).

History

#1 - 2018-09-13 15:36 - Gregor Schmidt

Screen Shot 2018-09-13 at 14.24.18.png

#2 - 2018-09-13 15:58 - Holger Just

- Related to Defect #24970: Net::LDAP::LdapError is deprecated added

#3 - 2018-09-13 15:58 - Holger Just

- Related to Defect #29476: Update net-ldap to 0.16.0 added

#4 - 2018-09-13 15:59 - Holger Just

- Related to Defect #27071: Error testing LDAPS Connection: "Unable to connect (hostname X.X.X.X does not match the server certificate)" added

#5 - 2018-09-13 15:59 - Holger Just

- Related to Patch #3358: Advanced LDAP authentication added

#6 - 2018-09-14 01:28 - Go MAEDA

- Category set to Accounts / authentication

- Target version set to 4.0.0

Using self-signed certificates is not so uncommon for on-premises. Setting the target version to 4.0.0.

#7 - 2018-09-14 01:28 - Go MAEDA

- Assignee set to Jean-Philippe Lang

#8 - 2018-09-14 10:04 - Gregor Schmidt

- File 0001-Allow-unchecked-LDAPS-TLS-connections.patch added

After some internal discussion at Planio, we've decided to further clarify the wording. Attached you may find an updated patch. It only differs in the locale files.

It should be now more clear, that LDAPS *with* certificate check should be considered proper LDAPS, while the option *without* certificate check is merely an exception for special use cases.

I've also replaced authorization with authentication in the new texts.

#9 - 2018-09-16 02:36 - Go MAEDA

- Related to Defect #8068: LDAP Authentificaton doesn't verify certificate validity added

#10 - 2018-09-23 08:48 - Go MAEDA

- Category changed from Accounts / authentication to LDAP

#11 - 2018-09-23 15:33 - Jean-Philippe Lang

- Status changed from New to Closed

Committed, thanks.

Files

Screen Shot 2018-09-13 at 14.24.18.png	19.4 KB	2018-09-13	Gregor Schmidt
0001-Allow-unchecked-LDAPS-TLS-connections.patch	8.1 KB	2018-09-13	Gregor Schmidt
0001-Allow-unchecked-LDAPS-TLS-connections.patch	8.09 KB	2018-09-14	Gregor Schmidt