Redmine - Defect #30171

Decrypting LDAP and SCM passwords fail if the plaintext password is longer than 31 bytes

2018-12-10 07:43 - Go MAEDA

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Database	**Estimated time:**	0.00 hour
Target version:	3.4.8		
Resolution:	Fixed	**Affected version:**	

Description

This issue is originally reported to the community repository on GitHub by Nik II.

https://github.com/redmine/redmine/pull/112/files

> *encode64 adds \n every 60 symbols, switch to strict_encode64 method, because .strip not working*

Related issues:

Related to Redmine - Feature # 7411: Option to cipher LDAP ans SCM passwords ...	**Closed**	**2011-01-22**

Associated revisions

Revision 17763 - 2018-12-17 05:49 - Go MAEDA

Decrypting LDAP and SCM passwords fail if the plaintext password is longer than 31 bytes (#30171).

Patch by Nik II.

Revision 17764 - 2018-12-17 05:52 - Go MAEDA

Test for r17763 (#30171).

Patch by Go MAEDA.

Revision 17765 - 2018-12-18 00:43 - Go MAEDA

Merged r17763 from trunk to 4.0-stable (#30171).

Revision 17766 - 2018-12-18 00:44 - Go MAEDA

Merged r17764 from trunk to 4.0-stable (#30171).

Revision 17767 - 2018-12-18 00:47 - Go MAEDA

Merged r17763 from trunk to 3.4-stable (#30171).

Revision 17768 - 2018-12-18 00:48 - Go MAEDA

Merged r17764 from trunk to 3.4-stable (#30171).

History

#1 - 2018-12-10 07:43 - Go MAEDA

- Related to Feature #7411: Option to cipher LDAP ans SCM passwords stored in the database added

#2 - 2018-12-10 07:46 - Go MAEDA

- Subject changed from Passwords encryption does not work if the password is longer than 31 characters to Passwords encryption does not work if the password is longer than 31 bytes

#3 - 2018-12-10 08:11 - Go MAEDA

- Status changed from New to Confirmed

Confirmed the problem.

```
Index: test/unit/lib/redmine/ciphering_test.rb
===================================================================
--- test/unit/lib/redmine/ciphering_test.rb    (revision 17702)
+++ test/unit/lib/redmine/ciphering_test.rb    (working copy)
@@ -92,15 +92,16 @@
   end

   def test_decrypt_all
+    long_password = SecureRandom.alphanumeric(32)
     Repository.delete_all
     Redmine::Configuration.with 'database_cipher_key' => 'secret' do
       Repository::Subversion.create!(:password => 'foo', :url => 'file:///tmp', :identifier => 'foo')
-      Repository::Subversion.create!(:password => 'bar', :url => 'file:///tmp', :identifier => 'bar')
+      Repository::Subversion.create!(:password => long_password, :url => 'file:///tmp', :identifier => 'bar')

       assert Repository.decrypt_all(:password)
       r = Repository.order('id DESC').first
-      assert_equal 'bar', r.password
-      assert_equal 'bar', r.read_attribute(:password)
+      assert_equal long_password, r.password
+      assert_equal long_password, r.read_attribute(:password)
     end
   end
 end
```

```
laphroaig:redmine-trunk maeda$ ruby test/unit/lib/redmine/ciphering_test.rb
Run options: --seed 15544

# Running:

.F

Failure:
Redmine::CipheringTest#test_decrypt_all [test/unit/lib/redmine/ciphering_test.rb:103]:
--- expected
+++ actual
```

```
@@ -1,2 +1,2 @@
-# encoding: US-ASCII
-"YW1zLuz0jcoHerKvHsApD9GVCrRMKXc8"
+"aes-256-cbc:a99hBE62VjbiZNoexSoakctQIKCAO31BoSVOw5krfBF24VUoMBpzrsytazMl
+tP+j--+TqRamucQbcZfeaeGIBLxA=="
```

```
bin/rails test test/unit/lib/redmine/ciphering_test.rb:94

.....

Finished in 0.354780s, 22.5492 runs/s, 42.2797 assertions/s.
8 runs, 15 assertions, 1 failures, 0 errors, 0 skips
```

#4 - 2018-12-10 08:16 - Go MAEDA

- Target version set to 3.4.8

#5 - 2018-12-14 10:09 - Federico Vera

This issue also affected Vault Plugin and was fixed in Issue 43

Since Vault uses Redmine's encryption, perhaps it could help.

Regards

#6 - 2018-12-16 06:04 - Go MAEDA

- File test-for-30171.diff added

Updated the test in order to catch the problem.

#7 - 2018-12-17 05:53 - Go MAEDA

- Subject changed from Passwords encryption does not work if the password is longer than 31 bytes to Decrypting LDAP and SCM passwords fail if the plaintext password is longer than 31 bytes
- Status changed from Confirmed to Resolved
- Resolution set to Fixed

Committed the patches.

#8 - 2018-12-18 00:54 - Go MAEDA

- Status changed from Resolved to Closed

#9 - 2019-01-21 05:13 - Go MAEDA

- Assignee set to Go MAEDA

Files

0001-Update-ciphering.rb.patch	849 Bytes	2018-12-10	Go MAEDA
test-for-30171.diff	831 Bytes	2018-12-16	Go MAEDA