Installer - Bug #3918

Password option is not effective in database.yaml

12/19/2013 03:10 PM - Lukas Zapletal

Status:	Rejected		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

It looks like the pg adapter in Rails uses UNIX sockets, which we configure to trust when ident is set properly.

Here is my pgsql configuration (this is what puppet configured):

```
# grep -v '#' /var/lib/pgsql/data/pg_hba.conf
local   all     postgres                    ident
local   all     all             ident
host    all     postgres        0.0.0.0/0       reject
host    all     all     127.0.0.1/32    md5
host    all     all     ::1/128 md5
```

As you can see, we allow ident authentication for local (UNIX) sockets for all users and then we allow password authentication for TCP on localhost (last two lines). The TCP connection is never used, at least not for me on RHEL6 / Foreman 1.3.

It's not a security incident luckily, we should get this sorted for sure by either disallowing all ident, or removing the (confusing) password from the database.yaml file.

History

#1 - 12/19/2013 03:11 PM - Lukas Zapletal

Reported by Cristian Falcas - thanks.

#2 - 12/19/2013 03:13 PM - Lukas Zapletal

To confirm this, list postgresql processes. In this case, I have running instance of Foreman:

```
postgres  2298  0.0  0.9 216148  7544 ?        Ss   15:00   0:00 postgres: foreman foreman [local] idle
```

And one psql session via TCP with password provided:

```
postgres  2350  0.0  0.3 214960  2900 ?        Ss   15:01   0:00 postgres: foreman foreman ::1(48073) idle
```

#3 - 01/02/2014 07:20 AM - Marek Hulán

Could you check or paste database.yml here? I saw this in case where host: configuration key was missing.

#4 - 01/02/2014 12:19 PM - Lukas Zapletal

Sure, this is not there. We can either add that, or keep sockets (which might be faster? :-)

```
[root@el ~]# cat /etc/foreman/database.yml
### File managed with puppet ###
## Module:         'foreman'
## Template source:  'MODULES/foreman/templates/database.yml.erb'
```

```
# SQLite version 3.x
development:
  adapter: sqlite3
  database: db/development.sqlite3
  pool: 5
  timeout: 5000

# Warning: The database defined as "test" will be erased and
# re-generated from your development database when you run "rake".
# Do not set this db to the same as development or production.
test:
  adapter: sqlite3
  database: db/test.sqlite3
  pool: 5
  timeout: 5000

# Database is managed by foreman::database::postgresql
production:
  adapter: postgresql
  database: foreman
  username: foreman
  password: "m3eMJVZyvguHSopSZtE8sFFUL2QPWucQ"
```

#5 - 01/02/2014 03:34 PM - Dominic Cleal

My intention when implementing it was to use ident + sockets and for the password to not be used, so it could be removed.

#6 - 06/06/2014 05:38 PM - Dominic Cleal

- Project changed from Foreman to Installer

- Category deleted (Packaging)

#7 - 10/06/2017 11:56 AM - Ewoud Kohl van Wijngaarden

- Status changed from New to Rejected

I don't consider this a problem. It's not a security issue and the option is used when connecting to a remote host. This is just how the pg gem works.