Installer - Bug #20079

Foreman does not verify CA on postgres DB connections with SSL

06/21/2017 05:33 PM - Martin Bacovsky

Status:	Closed		
Priority:	Normal		
Assignee:	Martin Bacovsky		
Category:	Foreman modules		
Target version:	1.16.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	Nightly
Bugzilla link:	1052713	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-foreman/pull/571		

Description

The default sslmode is 'prefer' which allows SSL connection to DB server, but CA of the DB server is not verified.

When using --foreman-db-sslmode 'verify-full' to enforce the CA cert verification there is no way to configure the root cert for the connection.
System CA trust is not supported by libpg and the cert is expected at '/usr/share/foreman/.postgresql/root.crt'.

Add an installer option to setup the root cert and consider if 'prefer' is the right and secure default option.

Related issues:

Related to Installer - Bug #22940: foreman-installer does not create /usr/sha...	**Closed**	**03/20/2018**
Blocks Katello - Feature #19667: Need additional supported database deploymen...	**Closed**	**05/25/2017**

Associated revisions

Revision a8297636 - 06/29/2017 10:56 AM - Martin Bacovsky

Fixes #20079 - SSL secured and verified PGSQL connection

To setup DB with SSL and verification use params:
db_sslmode => 'verify-full',
db_root_cert => 'ca_bundle.pem'

Default DB sslmode is 'prefer' - non-verified SSL with fallback to non-SSL. To use SSL secured connection with CA verification sslmode needs to be set to either 'verify-ca' or 'verify-full'. Underlying libpg uses DB root cert stored at '~/.postgresql/root.crt' which is in case of Foreman at '/usr/share/foreman/.postgresql/root.crt'. There is no way to setup different path (besides using env vars). System CA trust is not supported. The cert needs to be real file as links are not allowed too.

For more details see SSL support in libpg:
https://www.postgresql.org/docs/9.2/static/libpq-ssl.html

History

#1 - 06/21/2017 05:36 PM - Martin Bacovsky

- Blocks Feature #19667: Need additional supported database deployment options for Katello installation: such as External Postgres added

#2 - 06/21/2017 05:38 PM - Martin Bacovsky

- Project changed from Katello to Installer

- Category changed from Installer to Foreman modules

#3 - 06/29/2017 11:01 AM - Martin Bacovsky

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset puppet-foreman|a8297636bf9d38f34f519cf4e13793d2dd472868.

#4 - 03/20/2018 07:21 AM - Ales Dujicek

- Related to Bug #22940: foreman-installer does not create /usr/share/foreman/.postgresql/root.crt added