Packaging - Bug #16508

Secret/encryption tokens should be generated at first start, not installation

09/12/2016 05:29 AM - Daniel Lobato Garcia

Status:	New		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1346097	**Red Hat JIRA:**	
Pull request:			

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1346097
Version-Release number of selected component (if applicable):

foreman-1.7.2.56-1.el7sat.noarch

How reproducible:

Always.

postinstal:

1. secret token used for cookie signing etc.
   if [! -f /usr/share/foreman/config/initializers/local_secret_token.rb]; then
   touch /usr/share/foreman/config/initializers/local_secret_token.rb
   chmod 0660 /usr/share/foreman/config/initializers/local_secret_token.rb
   chgrp foreman /usr/share/foreman/config/initializers/local_secret_token.rb
   /usr/sbin/foreman-rake security:generate_token >/dev/null 2>&1 || :
   chmod 0640 /usr/share/foreman/config/initializers/local_secret_token.rb
   fi

1. encryption key used to encrypt DB contents
2. move the generated key file to /etc/foreman/ so users back it up, symlink to it from ~foreman
   if [! -e /usr/share/foreman/config/initializers/encryption_key.rb -a \
   ! -e /etc/foreman/encryption_key.rb]; then
   touch /usr/share/foreman/config/initializers/encryption_key.rb
   chmod 0660 /usr/share/foreman/config/initializers/encryption_key.rb
   chgrp foreman /usr/share/foreman/config/initializers/encryption_key.rb
   /usr/sbin/foreman-rake security:generate_encryption_key >/dev/null 2>&1 || :
   chmod 0640 /usr/share/foreman/config/initializers/encryption_key.rb
   mv /usr/share/foreman/config/initializers/encryption_key.rb /etc/foreman/
   fi
   if [! -e /usr/share/foreman/config/initializers/encryption_key.rb -a \
   -e /etc/foreman/encryption_key.rb]; then
   ln -s /etc/foreman/encryption_key.rb /usr/share/foreman/config/initializers/
   fi

Steps to Reproduce:
1. Install to a container or image.
2. Run new instance of container or image.
3.

Actual results:

All container and image instances share the same key/cert.
Expected results:

Each instance should receive a unique key/cert.

Additional info:

This bug is being file because Product Security considers "first run problems" to be bugs with the source package and with the container or image only in the aggregate. This view is in collaboration with upstream Fedora. See: https://fedorahosted.org/fpc/ticket/506

The recommended resolution for services is to follow the "First-time Service Setup" pattern (see: https://fedoraproject.org/wiki/Packaging:Initial_Service_Setup). Other packages may should use a runtime check and generation or similar procedure.

History

#1 - 09/12/2016 05:31 AM - Daniel Lobato Garcia

- Project changed from Docker to Foreman

- Category set to Packaging

#2 - 09/12/2016 05:48 AM - Dominic Cleal

- Project changed from Foreman to Packaging

- Subject changed from foreman creates Rails secret tokens, needs to be unique per instance or install but this value is created at install-time and not during the first run to Secret/encryption tokens should be generated at first start, not installation

- Category deleted (Packaging)