Foreman - Feature #3511

As a security person, I would like Foreman to run in FIPS mode

10/25/2013 11:33 AM - Anonymous

Status:	Resolved		
Priority:	Normal		
Assignee:			
Category:	Security		
Target version:			
Difficulty:		**Fixed in Releases:**	1.20.0
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Related issues:

Related to Katello - Feature #5313: FIPS compliancy	**Rejected**	
Related to Foreman - Feature #21748: Replace crypto- and hash-functions unapp...	**Closed**	**11/23/2017**
Related to Foreman - Feature #21749: Create CI environment with FIPS enabled	**New**	**11/23/2017**
Related to Foreman - Feature #21750: Investigate Rails caching with FIPS enabled	**Resolved**	**11/23/2017**
Related to Foreman - Feature #21751: Investigate interoperability with Salt w...	**New**	**11/23/2017**
Related to Foreman - Feature #21752: Investigate interoperability with BMC/IP...	**New**	**11/23/2017**
Related to Foreman - Feature #21753: Introduce verification of 3rd-party ssl ...	**New**	**11/23/2017**
Related to Foreman - Feature #21754: Investigate interoperability with Puppet...	**Resolved**	**11/23/2017**
Related to Installer - Feature #21755: Update dhcpd puppet module to use FIPS...	**Closed**	**11/23/2017**
Related to Installer - Feature #21756: Update bind puppet module to use FIPS-...	**Rejected**	**11/23/2017**
Related to Foreman - Feature #21875: Add support for sha512 grub passwords to...	**Closed**	**12/05/2017**
Related to Katello - Bug #23363: Katello uses md5hash function incompatible w...	**Closed**	**04/23/2018**
Related to Katello - Bug #24732: FIPS Scheduled synchronization task ends wit...	**Resolved**	
Related to Katello - Bug #24889: Docker repository sync on FIPS system fails ...	**Resolved**	
Related to Installer - Bug #24974: The kafo configure is generating incorrect...	**Duplicate**	
Related to Foreman - Feature #26203: Allow provisioning hosts into FIPS mode	**Closed**	
Related to Discovery - Feature #26204: Allow provisioning hosts into FIPS mode	**Closed**	
Related to Installer - Bug #26088: httpd fails to start after installing caps...	**Closed**	
Has duplicate Foreman - Bug #12314: Foreman does not work with FIPS enabled	**Duplicate**	**10/26/2015**
Blocked by Foreman - Bug #22583: Replace MD5 by SHA1 for apipie cache checksum	**Closed**	**02/14/2018**
Blocked by Foreman - Bug #23128: Deface uses MD5 and doesn't work in FIPS-ena...	**Resolved**	
Blocked by OpenSCAP - Bug #23130: unable to install theforeman-foreman_scap_...	**Rejected**	**04/05/2018**
Blocked by Packaging - Bug #23312: angular-rails-templates uses MD5 causing p...	**Closed**	
Blocked by Foreman - Tracker #21834: Rails 5.2 upgrade tasks	**Closed**	
Blocked by Foreman - Feature #22119: Replace MD5 hashes with SHA	**Closed**	
Blocked by Foreman - Bug #25447: Unable to create puppet certificate request ...	**New**	

History

#1 - 10/29/2013 02:08 PM - Anonymous

- setup foreman, smart_proxy, and puppet in FIPS mode
- see what breaks

#2 - 08/23/2015 11:07 AM - Eric Helms

- Related to Feature #5313: FIPS compliancy added

#3 - 10/27/2015 04:38 AM - Dominic Cleal

- Has duplicate Bug #12314: Foreman does not work with FIPS enabled added

#4 - 10/27/2015 04:39 AM - Dominic Cleal

Linked ticket #12314 has some specifics.

#5 - 02/25/2016 12:47 PM - Trevor Vaughan

Just wanted to make a note that a lot of the issue here may be that ActiveRecord does not support FIPS mode due to the explicit use of MD5.

Relevant Search: https://github.com/rails/rails/search?utf8=%E2%9C%93&q=md5

#6 - 11/16/2017 06:41 PM - Anonymous

Please see https://groups.google.com/forum/#!topic/foreman-dev/CZFAY5FQl80 for the discussion of potential approaches.

#7 - 11/22/2017 05:24 PM - James Shewey

- Subject changed from As a securiyt person, I would like Foreman to run in FIPS mode to As a security person, I would like Foreman to run in FIPS mode

I have opened https://github.com/rails/rails/issues/31203 upstream for this issue. Meanwhile, it appears that forman uses Digest::MD5 in the following places:

./migrate/20140912113254_add_password_hash_to_operatingsystem.rb
./migrate/20150428110835_change_os_default_password_hash.rb
./app/controllers/api/v1/operatingsystems_controller.rb
./app/controllers/api/v2/operatingsystems_controller.rb
./app/helpers/unattended_helper.rb
./app/helpers/application_helper.rb
./app/models/setting/email.rb
./app/services/password_crypt.rb
./app/views/unattended/provisioning_templates/snippet/_bmc_nic_setup.erb

https://github.com/theforeman/foreman/search?utf8=%E2%9C%93&q=md5&type=

#8 - 11/23/2017 08:41 PM - Anonymous

- Related to Feature #21748: Replace crypto- and hash-functions unapproved by FIPS with FIPS-approved ones added

#9 - 11/23/2017 08:41 PM - Anonymous

- Related to Feature #21749: Create CI environment with FIPS enabled added

#10 - 11/23/2017 08:42 PM - Anonymous

- Related to Feature #21750: Investigate Rails caching with FIPS enabled added

#11 - 11/23/2017 08:44 PM - Anonymous

- Related to Feature #21751: Investigate interoperability with Salt with FIPS enabled added

#12 - 11/23/2017 08:45 PM - Anonymous

- Related to Feature #21752: Investigate interoperability with BMC/IPMI with FIPS enabled added

#13 - 11/23/2017 08:46 PM - Anonymous

- Related to Feature #21753: Introduce verification of 3rd-party ssl certificates for FIPS-approved hash functions added

#14 - 11/23/2017 08:48 PM - Anonymous

- Related to Feature #21754: Investigate interoperability with Puppet with FIPS enabled added

#15 - 11/23/2017 08:53 PM - Anonymous

- Related to Feature #21755: Update dhcpd puppet module to use FIPS-approved hash function for omapi shared secret added

#16 - 11/23/2017 08:53 PM - Anonymous

- Related to Feature #21756: Update bind puppet module to use FIPS-approved hash function for dhcpd shared secret added

#17 - 11/28/2017 07:28 PM - Anonymous

Email thread with FIPS support discussion: https://groups.google.com/forum/#!search/foreman-dev/foreman-dev/CZFAY5FQl80/Ylxy-I7bBQAJ

#18 - 12/05/2017 11:08 PM - Anonymous

- Related to Feature #21875: Add support for sha512 grub passwords to provisioning templates added

#19 - 02/14/2018 05:45 PM - Ivan Necas

- Blocked by Bug #22583: Replace MD5 by SHA1 for apipie cache checksum added

#20 - 04/05/2018 08:27 AM - Ivan Necas

- Blocked by Bug #23128: Deface uses MD5 and doesn't work in FIPS-enable environment added

#21 - 04/05/2018 11:36 AM - Peter Ondrejka

- Blocked by Bug #23130: unable to install theforeman-foreman_scap_client in FIPS-enabled environment added

#22 - 04/18/2018 02:44 PM - Peter Ondrejka

- Blocked by Bug #23312: angular-rails-templates uses MD5 causing problems FIPS-enabled envrionments added

#23 - 04/23/2018 08:14 AM - Peter Ondrejka

- Related to Bug #23363: Katello uses md5hash function incompatible with FIPS-enabled environments added

#24 - 05/04/2018 05:31 PM - Anonymous

- Blocked by Tracker #21834: Rails 5.2 upgrade tasks added

#25 - 08/28/2018 12:31 PM - Peter Ondrejka

- Related to Bug #24732: FIPS Scheduled synchronization task ends with PG::UniqueViolation: ERROR: duplicate key value violates unique constraint "index_katello_repository_rpms_on_rpm_id_and_repository_id" added

#26 - 09/11/2018 11:34 AM - Peter Ondrejka

- Related to Bug #24889: Docker repository sync on FIPS system fails with TypeError: can't quote ActiveSupport::HashWithIndifferentAccess added

#27 - 10/01/2018 07:57 AM - Ivan Necas

- Blocked by Feature #22119: Replace MD5 hashes with SHA added

#28 - 10/09/2018 03:36 PM - Ivan Necas

Anyone with permissions, could you switch status on this to closed, as we're not aware of anything else right now to address, and things should just work(TM) in 1.20

#29 - 10/09/2018 05:22 PM - Anonymous

- Status changed from New to Resolved

- Fixed in Releases 1.20.0 added

The rest is related mainly to plugins.

#30 - 11/13/2018 03:38 PM - Ondřej Pražák

- Blocked by Bug #25447: Unable to create puppet certificate request from RHEL5 with fips enabled added

#31 - 02/22/2019 04:22 PM - Ivan Necas

- Related to Bug #24974: The kafo configure is generating incorrect 'foreman-proxy-client-bundle.pem' which is not allowing httpd service to start added

#32 - 03/01/2019 01:36 PM - Ivan Necas

- Related to Feature #26203: Allow provisioning hosts into FIPS mode added

#33 - 03/01/2019 01:39 PM - Ivan Necas

- Related to Feature #26204: Allow provisioning hosts into FIPS mode added

#34 - 03/05/2019 05:30 PM - Ewoud Kohl van Wijngaarden

- Related to Bug #26088: httpd fails to start after installing capsule in FIPS mode added