Packaging - Refactor #13642

Issue new archive signing GPG key

02/10/2016 08:27 AM - Dominic Cleal

Status:	Resolved		
Priority:	High		
Assignee:	Dominic Cleal		
Category:	Debian/Ubuntu		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The GPG key used to sign the Foreman apt archives is valid until 2016-06-30 (http://theforeman.org/security.html#GPGkeys), so we need to start preparing to cycle it now.

History

#1 - 02/11/2016 06:48 AM - Dominic Cleal

Debian issues a new GPG key per release and signs each release's Release file with the release it's for and the keys of the previous release (so Wheezy's is signed by the Wheezy and Squeeze keys, Jessie by Jessie and Wheezy).

Freight seems more limited as it only uses a single GPG key for signing the archive. Ideally we'd generate a new key now and have a period of 3-4 months (including a new stable release) with them both signing the archive until the old one expires and we remove it.

It seems like we'd have to do a hard switch over, or patch Freight. (I think I'll probably work on the latter, it looks trivial - though the patch won't be accepted at the moment as it's unmaintained.)

#2 - 02/11/2016 08:06 AM - Dominic Cleal

https://github.com/rcrowley/freight/pull/69 adds support for signing with multiple GPG keys.

#3 - 03/15/2016 08:39 PM - Anonymous

starting with apt 1.2.7:

```
W: gpgv:/var/lib/apt/lists/deb.theforeman.org_dists_jessie_Release.gpg: The repository is insufficiently signe
d by key 7059542D5AEA367F78732D02B3484CB71AA043B8 (weak digest)
W: gpgv:/var/lib/apt/lists/deb.theforeman.org_dists_plugins_Release.gpg: The repository is insufficiently sign
ed by key 7059542D5AEA367F78732D02B3484CB71AA043B8 (weak digest)
```

The Debian recommended gpg settings for generating a new key would be:

```
# Prioritize stronger algorithms for new keys.
default-preference-list SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES CAST5 BZIP2 ZLIB ZIP Uncompressed
# Use a stronger digest than the default SHA1 for certifications.
cert-digest-algo SHA512
```

and to use SHA512 per default for signing:

```
personal-digest-preferences SHA512
```

#4 - 04/08/2016 05:52 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

I've generated and added the new key to the configuration, fingerprint AE0A F310 E2EA 96B6 B6F4 BD72 6F86 00B9 5632 78F6. It's currently on the regenerated stagingdeb server and will run on deb.tf.org on its next push. Both keys will be used to sign the archives until the expiry of the 2014 key at the end of June.

If there are no obvious problems from it, I'll send an e-mail to -announce/-users on Monday.

#5 - 04/13/2016 04:18 AM - Dominic Cleal

- Status changed from Assigned to Resolved

Announced at https://groups.google.com/forum/#!topic/foreman-announce/InFeaMsl7fk.