rpminspect tag runner

Testing both rpminspect and CentOS Stream at scale

Jim Bair
Senior Software Engineer at Red Hat
Fedora, RHEL and CentOS Stream CI
jbair on IRC
rpminspect is an RPM build deviation analysis tool. It looks at the output of an RPM build (e.g., the output of a Koji build) and examines the contents of the build artifacts to report:

- Policy compliance
- Changes from a previous build to the current build
- General correctness and best practices

rpminspect is run today against CentOS Stream in Zuul against MRs in gitlab. Here’s an example:

- https://gitlab.com/redhat/centos-stream/rpms/mariadb/-/merge_requests/22

rpminspect is responsible for running 189 tests across 44 inspections, and growing as needed.

So, what kind of tests are we talking about?
Here are a few examples of inspections rpminspect is performing on builds:

**license**
- Verify the string specified in the License tag of the RPM metadata describes permissible software licenses as defined by the license database. Also checks to see if the License tag contains any unprofessional words as defined in the configuration file.

**runpath**
- Check for forbidden paths in both the DT_RPATH and DT_RUNPATH settings in ELF shared objects.

**symlinks**
- Symbolic links must be resolvable on the installed system. This inspection ensures absolute and relative symlinks are valid. It also checks for any symlink usage that will cause problems for RPM.

To see a complete list of all inspections and what they do, you can run: `rpminspect -lv`
In CentOS, the Koji build system is used for building and tracking RPMs. Koji organizes packages using tags as documented here:

- [https://docs.pagure.org/koji/HOWTO/#koji-architecture](https://docs.pagure.org/koji/HOWTO/#koji-architecture)

To see the tags in CentOS Stream 9, you can install `koji` and `centpkg` in Fedora and run:

- `koji -p stream list-tags`

To see the packages currently ready to ship to composes in Stream, you can run:

- `koji -p stream list-tagged --latest c9s-pending`
  - The `--latest` flag avoids duplicate packages if multiple updates are available for a given package on the `c9s-pending` tag
Example of koji list-tagged:

```
[jlm@lenovo ~]$
xorg-x11-drv-vmware-13.2.1-18.el9   cgs-pending   ajackson
xorg-x11-drv-wacom-1.8.6-1.el9      cgs-pending   phuttere
xorg-x11-font-utilts-7.5-53.el9   cgs-pending   mboddu
xorg-x11-fonts-7.5-33.el9          cgs-pending   mboddu
xorg-x11-proto-devel-2021.4-2.el9  cgs-pending   mboddu
xorg-x11-server-1.29.11-16.el9     cgs-pending   ofourdand
xorg-x11-server-Xwayland-21.1.3-2.el9  cgs-pending   ofourdand
xorg-x11-server-utils-7.7-44.el9   cgs-pending   mboddu
xorg-x11-util-macros-1.19.3-4.el9  cgs-pending   mboddu
xorg-x11-utils-7.5-40.el9          cgs-pending   mboddu
xorg-x11-xauth-1.1-10.el9          cgs-pending   mboddu
xorg-x11-xtrans-1.1-11-23.el9     cgs-pending   mboddu
xorg-x11-xinit-1.4.9-11.el9       cgs-pending   mboddu
xorg-x11-xtrans-devel-1.4.0-8.el9  cgs-pending   mboddu
xrestop-6.4-29.el9                 cgs-pending   mboddu
xsane-0.999-42.el9                 cgs-pending   mboddu
xterm-366-8.el9                    cgs-pending   tkorbar
xz-5.2.5-8.el9                     cgs-pending   muzfla
xz-java-1.8-14.el9                 cgs-pending   mboddu
yajl-2-2.1-0-28.el9                cgs-pending   jnovy
yara-4.2.1-4.el9                   cgs-pending   mwuth
yasm-1.3.0-15.el9                  cgs-pending   mboddu
yelp-48.3-2.el9                    cgs-pending   mboddu
yelp-tools-48.6-3.el9              cgs-pending   mboddu
yelp-xsl-46.2-1.el9                cgs-pending   klemsber
zaf-0-8.25.280888714svn.el9       cgs-pending   mboddu
zenity-3.32.6-8.el9                cgs-pending   dking
zip-3.8-33.el9                     cgs-pending   jmartis
zl1b-1.2.11-33.el9                 cgs-pending   muzfla
zsh-5.8-9.el9                      cgs-pending   kdudka
zstd-1.3.1-2.el9                   cgs-pending   jmartis
zziplib-0.13.71-5.el9              cgs-pending   mboddu
[jlm@lenovo ~]$  
```
What is rpminspect-tag-runner?

[https://github.com/rpminspect/rpminspect-tag-runner](https://github.com/rpminspect/rpminspect-tag-runner)

**rpminspect tag runner** allows for rapid, concurrent testing across thousands of packages in a given tag.

- We generate a list of all builds ready to ship in CentOS Stream 9
- We run rpminspect against the builds we find in a threaded manner
  - Assuming no hiccups, this takes ~3.5 hours on a 10C20T Fedora desktop
- We use adjustable command-line arguments that help with debugging
- We capture as much data as we can!
  - test results, stdout, stderr, runtime, exit code, and the command we ran
- For every successful inspection, we then find the previous build of the package and run an rpminspect **comparison** between the **old** and **new** builds
Example of tag-runner:

```bash
[jbair@awvr demo]$ git clone https://github.com/rpminspect/rpminspect-tag-runner.git
Cloning into 'rpminspect-tag-runner'...
remote: Enumerating objects: 68, done.
remote: Counting objects: 100% (68/68), done.
remote: Compressing objects: 100% (54/54), done.
remote: Total 68 (delta 35), reused 37 (delta 14), pack-reused 0
Receiving objects: 100% (68/68), 25.46 KiB | 6.82 MiB/s, done.
Resolving deltas: 100% (35/35), done.
[jbair@awvr demo]$ cd rpminspect-tag-runner/
[jbair@awvr rpminspect-tag-runner]$ ./generate-list.sh
Thu Jun 16 10:50:32 AM EDT 2022 - INFO: Generating list.txt
[jbair@awvr rpminspect-tag-runner]$ ./tag_runner.sh
```
**Example of tag-runner:**

```bash
Thu Jun 16 10:52:18 AM EDT 2022 - Testing NetworkManager-1.39.6-1.el9
Thu Jun 16 10:52:19 AM EDT 2022 - Testing NetworkManager-libreswan-1.2.14-1.el9.3
Thu Jun 16 10:52:20 AM EDT 2022 - Testing PEGTL-2.8.3-4.el9
Thu Jun 16 10:52:20 AM EDT 2022 - Testing PackageKit-1.2.4-2.el9
Thu Jun 16 10:52:21 AM EDT 2022 - Testing PyYAML-5.4.1-6.el9
Thu Jun 16 10:52:21 AM EDT 2022 - Testing SDL2-2.0.20-2.el9
Thu Jun 16 10:52:22 AM EDT 2022 - Testing WALinuxAgent-2.7.0.6-1.el9
Thu Jun 16 10:52:22 AM EDT 2022 - Testing Xaw3d-1.6.7-1.el9
Thu Jun 16 10:52:23 AM EDT 2022 - Testing as2dec-0.7.4-42.el9
Thu Jun 16 10:52:24 AM EDT 2022 - 29 rpmInspect jobs currently running:
2895881 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh 389-ds-base-2.0.14-1.el9
2895888 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh Box20-2.4.1-7.el9
2895906 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh CUnit-2.1.3-25.el9
2895930 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh Cython-0.29.22-7.el9
2895960 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh GnomeHistogram-2.1.2-3.el9
2895988 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh GnomeHistogram-c-6.11.0-6.el9
2896920 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh Judy-1.0.5-10.el9
2896864 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh LibRaw-0.9.20-2.5.el9
2896113 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh ModernManager-1.18.2-3.el9
2896164 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh NetworkManager-1.39.6-1.el9
2896217 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh NetworkManager-libreswan-1.2.14-1.el9.3
2896272 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh OpenIPMI-2.0.32-3.el9
2896337 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh PEGTL-2.8.3-4.el9
2896394 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh PackageKit-1.2.4-2.el9
2896452 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh PyYAML-5.4.1-6.el9
2896527 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh SDL2-2.0.20-2.el9
2896582 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh WALinuxAgent-2.7.0.6-1.el9
2896637 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh Xaw3d-1.6.3-7.el9
2896695 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh as2dec-0.7.4-42.el9
2896762 pts/10 S+ 0:00 /bin/bash /run_rpmInspect.sh aajohan-comforttaa-fonts-3.001-18.el9
```
A bit of history

Red Hat originally developed an internal QE tool called **rpmdiff** (not the one from rpmlint). This tool was built a long time ago....before things like the cloud, virtualization, or containers.

This tool runs as a service and performs tests on built packages similar to the tests in **rpminspect**:

- Package policy compliance
- Legal checks
- Kernel ABI verification
- Security policies
- Comparisons from one build to the next

**rpminspect** was built as it’s replacement with the goals of being open source, run on the command line and being much more portable along with some much needed refactoring along the way.
rpminspect is at v1.9, with 1.10 in active development:

https://github.com/rpminspect/rpminspect/releases/tag/v1.9

- With 130 commits since this release (and counting!), the speed of development to fully replace rpmdiff means a lot of bug-fixes and improvements
- Inspection failures fall into two categories:
  - A bug to be fixed in rpminspect itself
  - An valid failure that requires an updated build or the creation of an rpminspect.yaml configuration within the build
- Updated copr builds improve accuracy of our inspections and tag-runner helps us discover newly-passing builds quickly
- tag-runner has helped to improve the stability of the upcoming 1.10 release:
  - https://github.com/rpminspect/rpminspect/pull/791
  - https://github.com/rpminspect/rpminspect/pull/792
c9s-pending on 16-June-2022

Total runtime: ~8 hours
Total packages: 2542
Inspection pass rate: 86%
Comparison pass rate: 97%

Your feedback helps us to provide better test results!
Requests for features can be found in github: [https://github.com/rpminspect/rpminspect-tag-runner/issues](https://github.com/rpminspect/rpminspect-tag-runner/issues)

Team discussions around creating a pipeline to monitor compose and rpminspect health with tag-runner daily or weekly

Single command runs providing an easy to digest summary/report

Better resiliency for public networks with unexpected timeouts

Allow profiles to define tags and koji end-points for various distributions

Size based sorting; PoC works but it does take some time to run (30+ minutes)
  - I need to bring the PoC into the repo and add cache support (a lot of re-runs against the same builds so a cache helps)

If you try it and find bugs or would like additional features, send us a PR or file an issue
Questions?