cbs.centos.org
Community Build Service

FROM SOURCES TO RPMS

On behalf of CentOS infra team and all contributors.

Presented by Thomas ‘alphacc’ Oulevey / @thomasnomas
and Brian Stinson / @bstinsonmhk
Who am I?

- I am ‘alphacc’ on freenode
- Worked for ESO, ISO, CERN
- Service Manager at CERN (www.cern.ch) since 2011

Past: Openstack storage evaluation (gluster, ceph, netapp), Scientific Linux CERN.

Current: IT Koji service, More SLC, CERN CentOS 7 migration, puppetization...

(As people asked: https://jobs.web.cern.ch/)
AGENDA

- Introduction,
- Koji,
- Repositories & mash,
- Signing,
- Centpkg.
Introduction

Started in July 2014.

2 main use cases:

• Build Special Interest Group (SIG) RPMs:
  
  Short term : Build from src.rpm
  
  Long term : Build from git.centos.org

• Distribute RPMs:
  
  Short term : yum repos for dev/testers consumption
  
  Long term : automatic workflow for SIGs RPMs distribution.
An agile user

I want to build mypkg

aiadm$ koji build ai6 mypkg

SCM

task done!

mynode$ yum install --enablerepo=ai6-testing mypkg
The big picture

git: https://git.centos.org (gitblit http://gitblit.com/)
koji: https://fedorahosted.org/koji/ (fedora/epel)
mash: https://git.fedorahosted.org/cgit/mash/
Components:

- **kojihub:**
  XML-RPC server running under mod_wsgi Broker that abstract postgresql and filesystem.
- **kojid:** polls build requests and handles them in a fresh buildroot thanks to mock.
- **kojira:** keeps your repos updated.
- **clients:** cli & kojiweb for user/admin tasks.

All components/client communicate with certs (our "self-signed" CA).
## Build Targets

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>atomic7-el7.centos</td>
</tr>
<tr>
<td>13</td>
<td>bananas5-el5</td>
</tr>
<tr>
<td>14</td>
<td>bananas5-el5_10</td>
</tr>
<tr>
<td>15</td>
<td>bananas5-el5.centos</td>
</tr>
<tr>
<td>10</td>
<td>bananas6-el6</td>
</tr>
<tr>
<td>11</td>
<td>bananas6-el6_5</td>
</tr>
<tr>
<td>12</td>
<td>bananas6-el6.centos</td>
</tr>
<tr>
<td>7</td>
<td>bananas7-el7</td>
</tr>
<tr>
<td>8</td>
<td>bananas7-el7_0</td>
</tr>
<tr>
<td>9</td>
<td>bananas7-el7.centos</td>
</tr>
<tr>
<td>2</td>
<td>buildsys5</td>
</tr>
<tr>
<td>1</td>
<td>buildsys6</td>
</tr>
<tr>
<td>3</td>
<td>buildsys7</td>
</tr>
<tr>
<td>21</td>
<td>cloud5-el5</td>
</tr>
<tr>
<td>22</td>
<td>cloud6-el6</td>
</tr>
<tr>
<td>23</td>
<td>cloud7-el7</td>
</tr>
<tr>
<td>25</td>
<td>infrastructure6-el6</td>
</tr>
<tr>
<td>24</td>
<td>infrastructure7-el7</td>
</tr>
<tr>
<td>27</td>
<td>scl6-el6-mariadb100</td>
</tr>
</tbody>
</table>
Hosts

State: on

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Arches</th>
<th>Enabled?</th>
<th>Ready?</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>x86_64-0.centos.org</td>
<td>x86_64 i386</td>
<td>✔️</td>
<td>✔️</td>
<td>2015-01-31 11:02:49</td>
</tr>
<tr>
<td>2</td>
<td>x86_64-1.cbs.centos.org</td>
<td>x86_64 i386</td>
<td>✔️</td>
<td>✔️</td>
<td>2015-01-31 11:02:46</td>
</tr>
<tr>
<td>3</td>
<td>x86_64-2.cbs.centos.org</td>
<td>x86_64 i386</td>
<td>✔️</td>
<td>✔️</td>
<td>2015-01-31 11:02:54</td>
</tr>
</tbody>
</table>

Builds

State: all

<table>
<thead>
<tr>
<th>ID</th>
<th>NVR</th>
<th>Built by</th>
<th>Finished</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>653</td>
<td>openstack-glance-2014.2.1-3.el7</td>
<td>hguemar</td>
<td>2015-01-29 18:25:59</td>
<td>✔️</td>
</tr>
<tr>
<td>652</td>
<td>python-urlib3-1.10-2.el7</td>
<td>hguemar</td>
<td>2015-01-28 22:39:53</td>
<td>✔️</td>
</tr>
<tr>
<td>651</td>
<td>docker-registry-0.9.1-1.el7</td>
<td>Ism5</td>
<td>2015-01-28 03:10:56</td>
<td>✔️</td>
</tr>
<tr>
<td>650</td>
<td>openstack-ironic-discoverd-0.2.5-1.el7</td>
<td>hguemar</td>
<td>2015-01-28 00:47:42</td>
<td>✔️</td>
</tr>
<tr>
<td>649</td>
<td>openstack-tripleo-image-elements-0.8.10-19.el7</td>
<td>hguemar</td>
<td>2015-01-28 00:44:24</td>
<td>✔️</td>
</tr>
</tbody>
</table>
koji cli

$ koji add-pkg <tag> <NAME>
$ koji build <target> <NAME-RELEASE-VERSION>.src.rpm
OR
$ koji build <target> “git+https://url.git?#COMMIT”
$ koji tag-build <tag> “mybuild”
**tag:** cloud7-testing, cloud7-release.

**external repos:** centos7-os, centos7-updates

**build tag:** cloud7-el7-build

**target:** cloud7-el7 ; a buildroot and a destination tag.

**package:** An RPM name e.g: gcc

**build:** A build in Koji e.g: gcc-4.4-1.el6

**to tag/untag:** associate or not a package to a specific tag and therefore ultimately to a mash repository.
Step 1: Naming

build tags: `<SIG><MAJOR>-<TAG>[-<COLLECTION>,]-build`
  e.g: cloud6-el6-build, scl6-el6-mariadb100-build

targets: `<SIG><MAJOR>-<TAG>[-<COLLECTION>,]`
  e.g: cloud6-el6

destination tags:
  `<SIG><MAJOR>-{testing,release}`
  `<SIG><MAJOR>-<PROJECT>-{testing,release}`
  e.g: cloud6-release, cloud7-rdo-release
Example

$ koji  add-pkg cloud7-testing openstack-glance
$ koji  add-pkg cloud7-release openstack-glance
$ koji build cloud7-el7 “git+https://git.centos.org/rpms?#COMMIT”
$ koji tag-build cloud7-release openstack-glance-2014.2.1-3.el7
Information for build openstack-glance-2014.2.1-3.el7

ID 653
Package Name openstack-glance
Version 2014.2.1
Release 3.el7
Epoch
Summary OpenStack Image Service
Description OpenStack Image Service (code-named Glance) provides discovery, registration, and delivery services for virtual disk images. The Image Service API server provides a standard REST interface for querying information about virtual disk images stored in a variety of back-end stores, including OpenStack Object Storage. Clients can register new virtual disk images with the Image Service, query for information on publicly available disk images, and use the Image Service's client library for streaming virtual disk images. This package contains the API and registry servers.

Built by hguemar
State complete
Started Thu, 29 Jan 2015 18:22:39 UTC
Completed Thu, 29 Jan 2015 18:25:59 UTC
Task build (cloud7-el7, openstack-glance-2014.2.1-3.el7.src.rpm)
Tags cloud7-testing

RPMs

src
  openstack-glance-2014.2.1-3.el7.src.rpm (info) (download)

noarch (build logs)
  openstack-glance-2014.2.1-3.el7.noarch.rpm (info) (download)
  openstack-glance-doc-2014.2.1-3.el7.noarch.rpm (info) (download)
  python-glance-2014.2.1-3.el7.noarch.rpm (info) (download)

Changelog

* Thu Jan 29 2015 Haïkel Guémar <hguemar@fedoraproject.org> - 2014.2.1-3
  - Usage storage quota bypass - CVE-2014-9623 (RHBZ #1187003)

* Tue Jan 13 2015 Haïkel Guémar <hguemar@fedoraproject.org> - 2014.2.1-2
  - Unrestricted path flow traversal (RHBZ #1174474)
https://git.centos.org/summary/?r=sig-core/cbs-tools.git

$ ./create_sig.sh
usage: ./create_sig.sh -d <distribution> -s <signame(s)> -t <tag(s>)

This script generate new build target in koji for SIGS.

OPTIONS:
- d  Distribution : 5 6 7
- s  SIG name : cloud, storage
- t  DISTTAGS : "el7 el7.centos el7_0"
- c  COLLECTION : mariadb100 (a single collection can be used at this time)
Workflow:

1. user commit to git.centos.org
2. user submit a git url to build system
3. koji builder receive a new job
4. koji builder execute “git clone”
5. run a specific command (get_sources detects the branch and execute get_sources.sh with correct arguments.) to grab binary files from lookaside and generate the src.rpm.
6. build src.rpm

available: in buildsys-tools package in koji and
https://git.centos.org/summary/?r=centos-git-common.git
Step 3: Mash workflow

1. Build RPM with Koji
2. 10 minutes later it appears in -testing repository
3. User can tag it -release repository
4. -release repository signed and ready for consumption.

```
$ cat /etc/mash/cloud6-release.mash
[cloud6-release]
rpm_path = /mnt/kojishare/repos/cloud6-release/%(arch)s/os/Packages
repodata_path = /mnt/kojishare/repos/cloud6-release/%(arch)s/os/
source_path = source/SRPMS
debbuginfo = True
multilib = True
multilib_method = devel
tag = cloud6-release
inherit = False
strict_keys = False
repoviewurl = http://cbs.centos.org/repos/cloud6-release/%(arch)s/os/
repoviewtitle = "CLOUD6-RELEASE"
arches = i386 x86_64
delta = True
```
Over next months

- User training
- Support for software collection
- Patch koji to support different dist-git layout (fedora + centos). All patches upstream now.
- lookaside cache
- imagefactory support
- Added new builders (with puppet)
- centpkg (A bit more on that later...)
- Investigate signing
• Another Fedora project
• Sigul keeps the private keys used for signing on its server. They are not accessible by the clients.
• All requests by Sigul Clients to Sigul Server are sent over the Sigul Bridge which relays them. This allows signing RPMs from various machines, without having access to actual keys being used.
• You never communicate directly with the Server which should be isolated from the rest of the world and only allow connections from/to the Bridge.
$ sigul sign-rpm -o signed.rpm my-gpg-key-name myrpm.rpm

$ sigul sign-rpm --koji-only --store-in-koji --v3-signature my-gpg-key-name myrpm.rpm

OR

$ sigul sign-rpm -o signed.rpm --v3-signature my-gpg-key-name myrpm.rpm
$ koji import-sig ./signed.rpm
$ koji write-signed-rpm --all GPG-KEY-ID
A tool to manage the package building process:

- handles dist-git operations,
- local package building,
- abstract koji operations.

```
$ centpkg clone --branch c7 mypkg
$ cd mypkg

$ centpkg sources

$ centpkg srpm
```
Limitations

• Single namespace
  ….but no collision on package name

• Policy
  in a file / service reload needed.

• Kernel modules
  no easy way to recompile against a specific kernel or having triggers to launch a new build.
Few things I learnt

easy-rsa: https://github.com/OpenVPN/easy-rsa

If you want to roll your own CA, you need to know it exists :) It is part of openvpn project.

git-crypt: https://www.agwa.name/projects/git-crypt/

enables transparent encryption and decryption of files in a git repository
QUESTIONS?

https://git.centos.org/summary/?r=sig-core/cbs-tools.git

Thank you!