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 ?

CERN IT Department

- 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

CERN IT Department

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

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Introduction

Started in July 2014.

2 main use cases:

- Build Special Interest Group(SIG) RPMs:

  Short term : Build from src.rpm

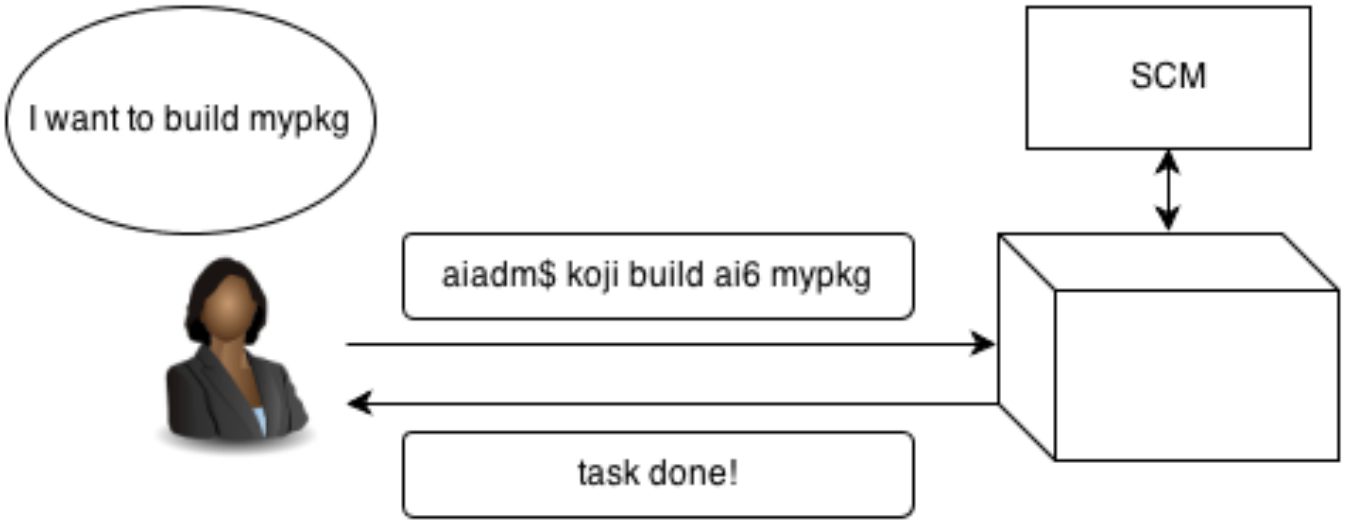
  Long term : Build from git.centos.org

- Distribute RPMs:

  Short term : yum repos for dev/testers consumption

  Long term : automatic workflow for SIGs RPMs distribution.

An agile user



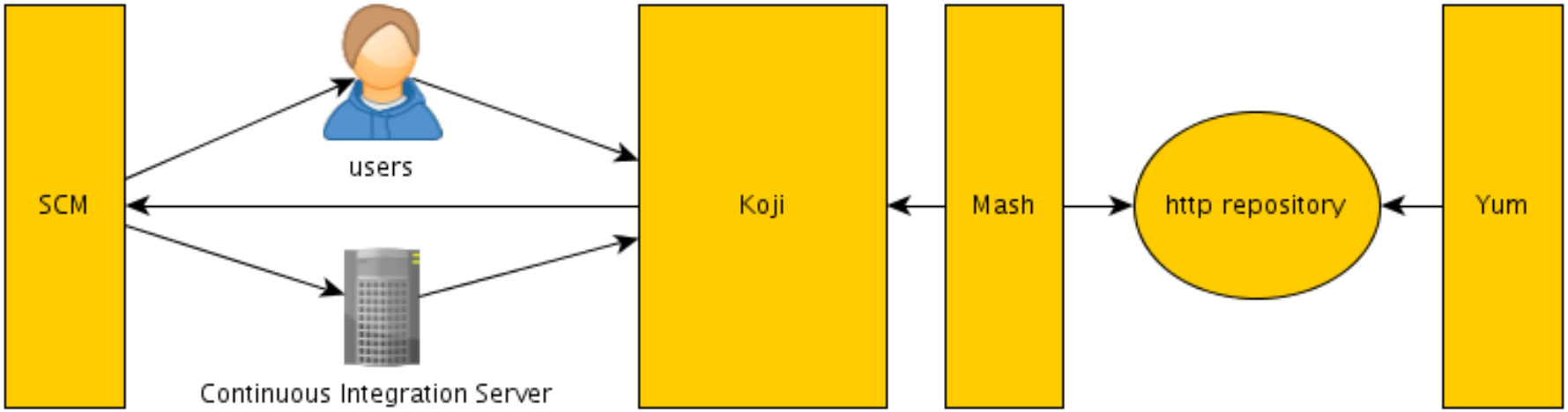
mynode$ yum install --enablerepo=ai6-testing mypkg

The big picture

git : https://git.centos.org (giblit http://gitblit.com/)

koji : https://fedorahosted.org/koji/ (fedora/epel)

mash : https://git.fedorahosted.org/cgit/mash/



Koji

Components :

- kojihub:

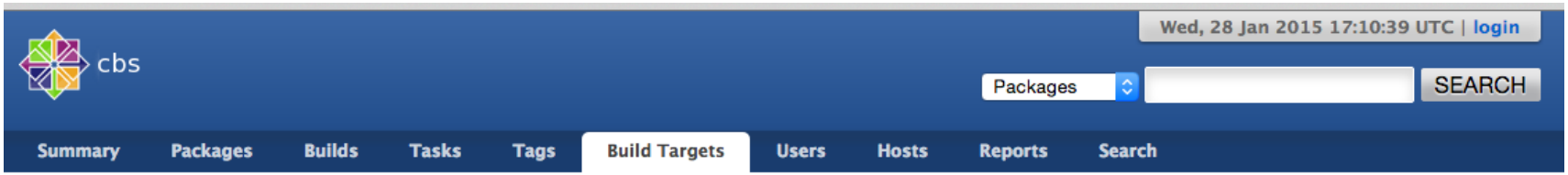
  XML-RPC server running under mod_wsgi

  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).

kojiweb

CERN IT Department



Build Targets

Targets 1 through 26 of 26

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

kojiweb

CERN IT Department

Summary | Packages | Builds | Tasks | Tags | Build Targets | Users | Hosts | Reports | Search

Hosts

State: enabled

Hosts 1 through 3 of 3

ID	Name ▲	Arches	Enabled?	Ready?	Last Update
1	x86_64-0.centos.org	x86_64 i386	✓	✓	2015-01-31 11:02:49
2	x86_64-1.cbs.centos.org	x86_64 i386	✓	✓	2015-01-31 11:02:46
3	x86_64-2.cbs.centos.org	x86_64 i386	✓	✓	2015-01-31 11:02:54

Hosts 1 through 3 of 3

Summary | Packages | Builds | Tasks | Tags | Build Targets | Users | Hosts | Reports | Search

Builds

State: all Built by: everyone

0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | all

Builds 1 through 50 of 653 >>> Page: 1

ID ▼	NVR	Built by	Finished	State
653	openstack-glance-2014.2.1-3.el7	hguemar	2015-01-29 18:25:59	✓
652	python-urllib3-1.10-2.el7	hguemar	2015-01-28 22:39:53	✓
651	docker-registry-0.9.1-1.el7	lsm5	2015-01-28 03:10:56	✓
650	openstack-ironic-discoverd-0.2.5-1.el7	hguemar	2015-01-28 00:47:42	✓
649	openstack-tripleo-image-elements-0.8.10-19.el7	hguemar	2015-01-28 00:44:24	✓

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”
```

koji 101

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:

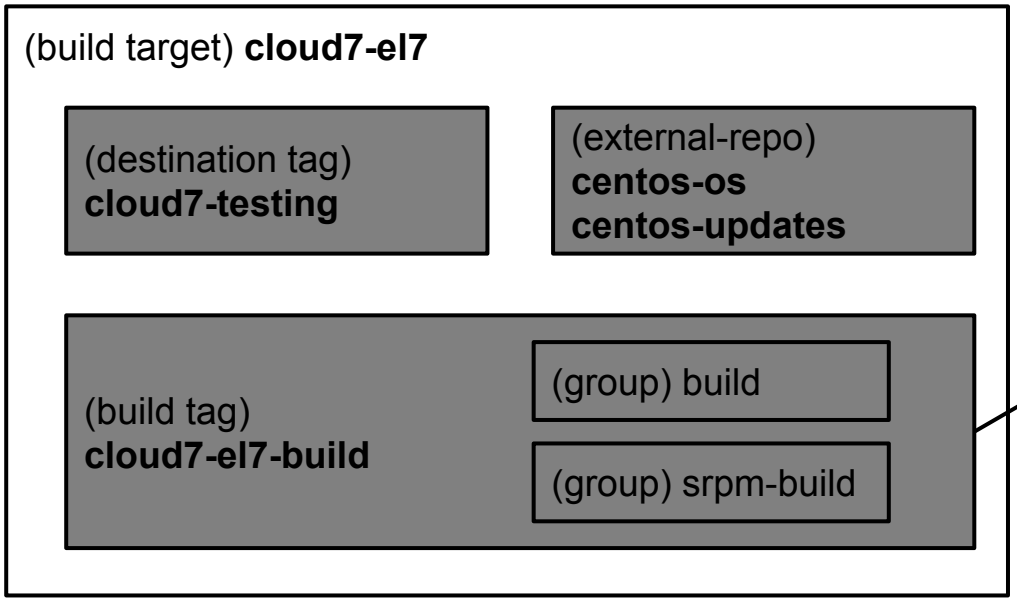
<SIG><MAJOR>-{testing,release}

<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 tag cloud7-el7-build

Name	cloud7-el7-build
ID	51
Arches	x86_64
Locked	no
Permission	none
Inheritance	cloud7-el7-build ~~buildsys7~~ ~~cloud7-testing~~
External repos	centos7-os centos7-updates
Repo created	Thu, 29 Jan 2015 18:26:14 UTC
Packages	294
Builds	311
Targets building from this tag	cloud7-el7
Targets building to this tag	No build targets

Example

CERN IT Department

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)

Step 1 : Administration

CERN IT Department

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)
```

Step 2 : Integration with git.

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

CERN IT Department

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
debuginfo = 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

Sigul 1/2

- 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 2 / 2


```
$ 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
```

Centpkg

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 !