Controlling Software Environments with GNU Guix

Ludovic Courtès

Inria Bordeaux Sud-Ouest

November 2016

The difficulty of keeping software environments under control.

#1. Upgrades are hard.

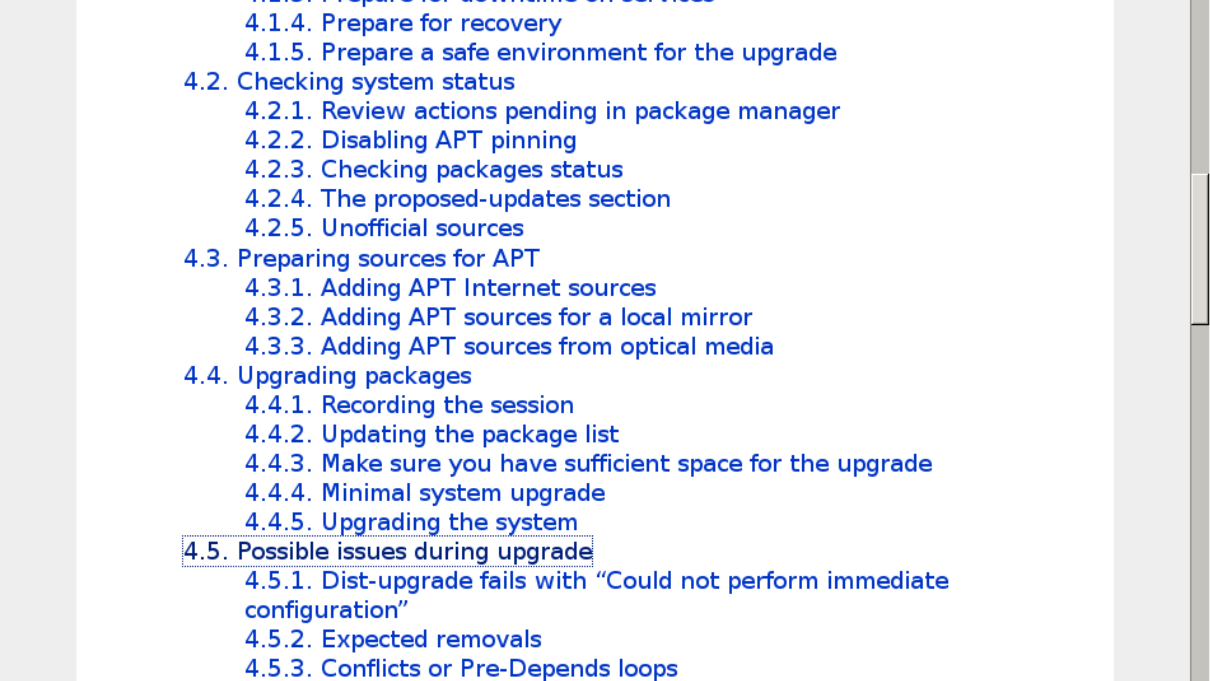
Distribution Upgrade of all the files:

WARNING

Following the upgrade instructions found in the release notes is the best way to ensure that your system upgrades from one major Debian release to another (e.g. from lenny to squeeze) without breakage!

These instructions will tell you to do a `dist-upgrade` (instead of `upgrade`) in the case of apt-get or `full-upgrade` (instead of `safe-upgrade` in the case of aptitude) at least once. So you would have to type something like

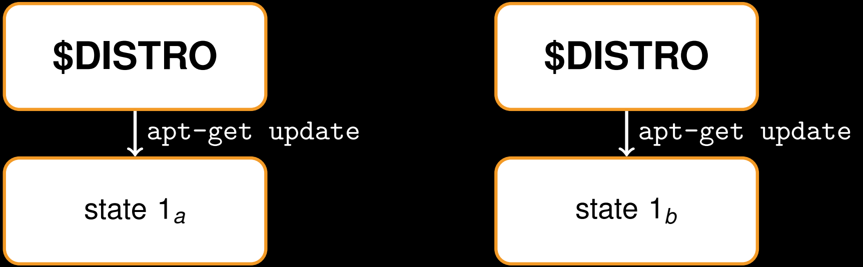
```
# aptitude full-upgrade
```



#2. Stateful system management is intractable.

$DISTRO

$DISTRO



$DISTRO

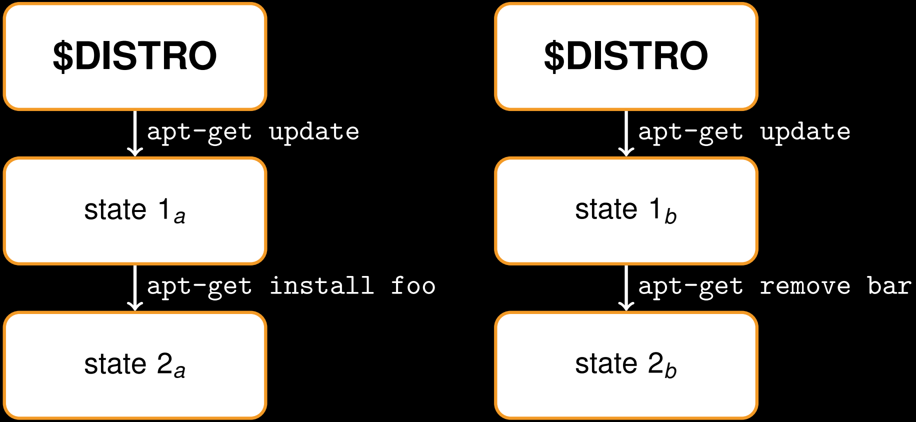
`apt-get update`

state 1_a

$DISTRO

`apt-get update`

state 1_b



$DISTRO

`apt-get update`

state 1_a

`apt-get install foo`

state 2_a

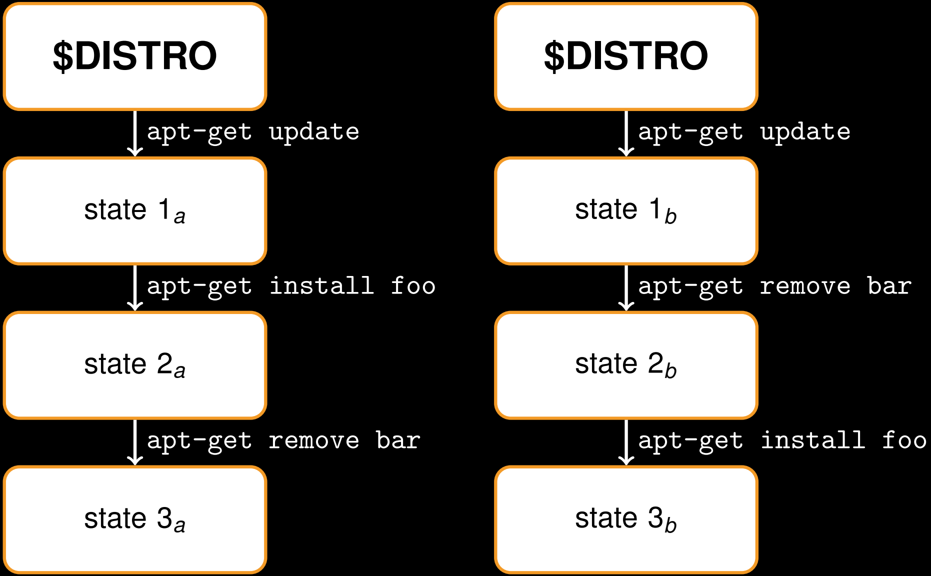
$DISTRO

`apt-get update`

state 1_b

`apt-get remove bar`

state 2_b



$DISTRO

apt-get update

state 1_a

apt-get install foo

state 2_a

apt-get remove bar

state 3_a

$DISTRO

apt-get update

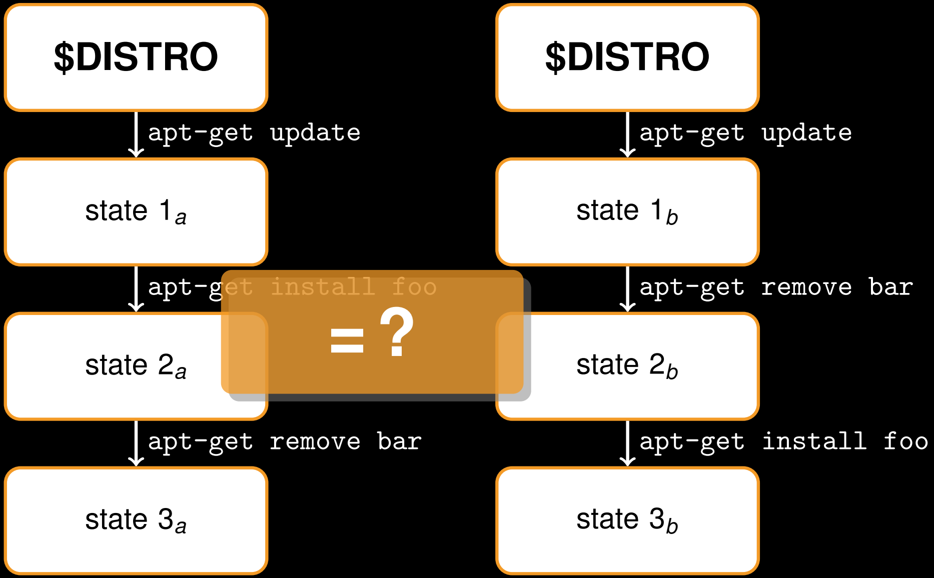
state 1_b

apt-get remove bar

state 2_b

apt-get install foo

state 3_b



$DISTRO

apt-get update

state 1_a

apt-get install foo

state 2_a

apt-get remove bar

state 3_a

$DISTRO

apt-get update

state 1_b

apt-get remove bar

state 2_b

apt-get install foo

state 3_b

=?

#3. Entropy keeps increasing.

Here is an example of loading a module on a Linux machine under bash.

```
% module load gcc/3.1.1
% which gcc
/usr/local/gcc/3.1.1/linux/bin/gcc
```

Now we'll switch to a different version of the module

```
% module switch gcc gcc/3.2.0
% which gcc
/usr/local/gcc/3.2.0/linux/bin/gcc
```

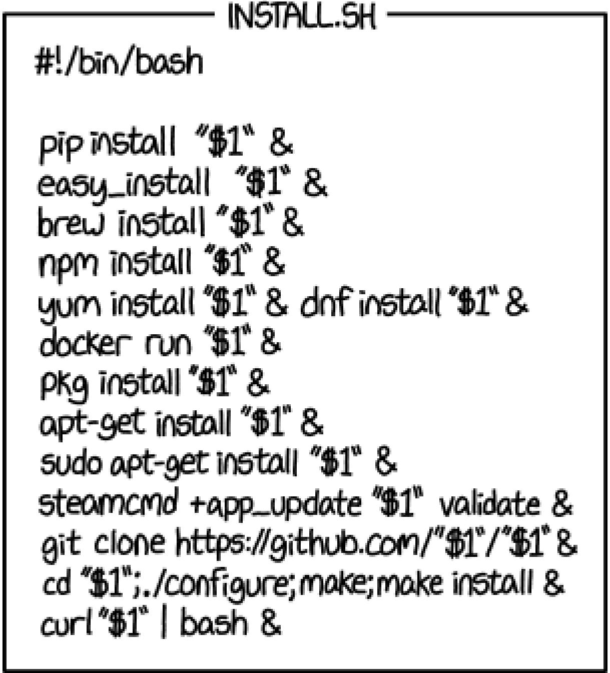
Application-level package managers [edit]

- Anaconda - a package manager for Python
- Assembly - a partially compiled code library for use in Common Language Infrastructure (CLI) deployment, versioning and security.
- Biicode - a file-focused dependency manager for C/C++ languages and platforms (PC, Raspberry Pi, Arduino).
- Bower - a package manager for the web.
- UPT - a fork of Bower that aims to be a universal package manager, for multiple evironments and unlimited kind of package
- Cabal - a programming library and package manager for Haskell
- Cargo - a package manager for Rust (programming language)
- CocoaPods - Dependency Manager for Objective-C and RubyMotion projects
- Composer - Dependency Manager for PHP
- CPAN - a programming library and package manager for Perl
- CRAN - a programming library and package manager for R
- CTAN - a package manager for TeX
- DUB - a package manager for D

As of `npm@2.6.1`, the `npm update` will only inspect top-level packages. Prior versions of `npm` would also recursively inspect all dependencies. To get the old behavior, use `npm --depth 9999 update`, but be warned that simultaneous asynchronous update of all packages, including `npm` itself and packages that `npm` depends on, often causes problems up to and including the uninstallation of `npm` itself.

To restore a missing `npm`, use the command:

```
curl -L https://npmjs.com/install.sh | sh
```



INSTALL.SH

```bash
#!/bin/bash

pip install "$1" &
easy_install "$1" &
brew install "$1" &
npm install "$1" &
yum install "$1" & dnf install "$1" &
docker run "$1" &
pkg install "$1" &
apt-get install "$1" &
sudo apt-get install "$1" &
steamcmd +app_update "$1" validate &
git clone https://github.com/"$1"/"$1" &
cd "$1";./configure;make;make install &
curl "$1" | bash &
```

http://xkcd.com/1654/

Giving up?

Giving up?

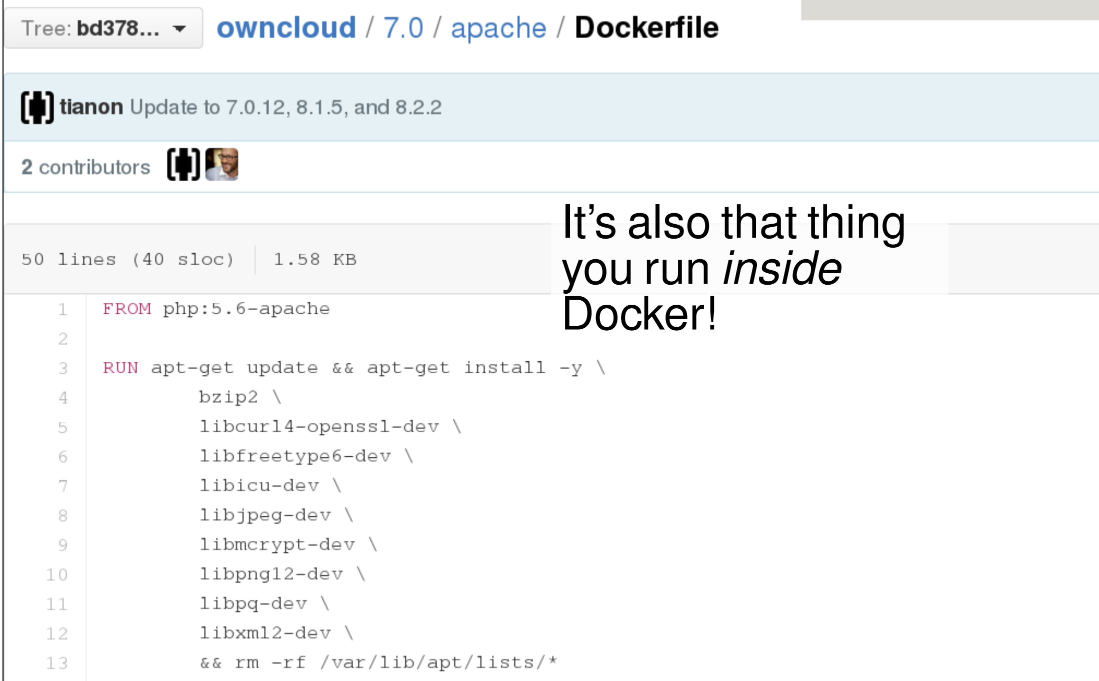
→ “app bundles” (Docker images & co.)

“Debian and other distributions are going to be ***that thing you run docker on****, little more.”*

— Jos Poortvliet, ownCloud developer

`http://lwn.net/Articles/670566/`

It’s also that thing you run *inside* Docker!



Tree: bd378... owncloud / 7.0 / apache / **Dockerfile**

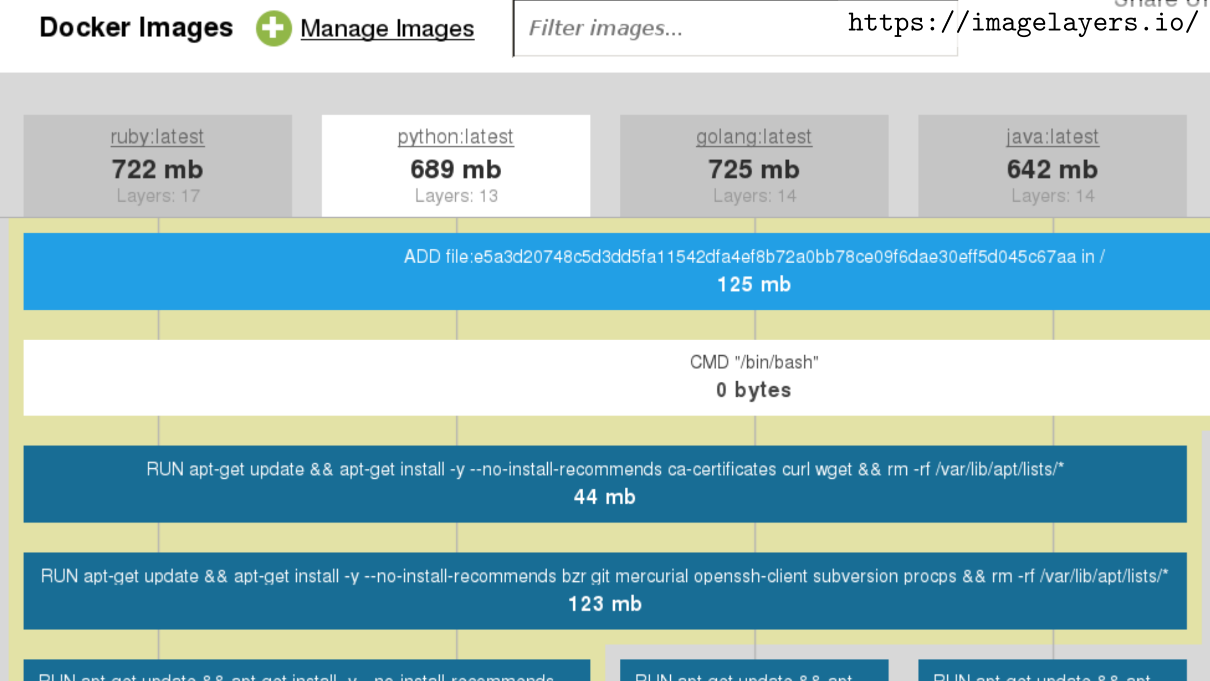
tianon Update to 7.0.12, 8.1.5, and 8.2.2

2 contributors

50 lines (40 sloc) | 1.58 KB

```
FROM php:5.6-apache

RUN apt-get update && apt-get install -y \
        bzip2 \
        libcurl4-openssl-dev \
        libfreetype6-dev \
        libicu-dev \
        libjpeg-dev \
        libmcrypt-dev \
        libpng12-dev \
        libpq-dev \
        libxml2-dev \
        && rm -rf /var/lib/apt/lists/*
```

https://imagelayers.io/



Docker Images

Manage Images

Filter images...

ruby:latest	python:latest	golang:latest	java:latest
722 mb	689 mb	725 mb	642 mb
Layers: 17	Layers: 13	Layers: 14	Layers: 14

ADD file:e5a3d20748c5d3dd5fa11542dfa4ef8b72a0bb78ce09f6dae30eff5d045c67aa in /
125 mb

CMD "/bin/bash"
0 bytes

RUN apt-get update && apt-get install -y --no-install-recommends ca-certificates curl wget && rm -rf /var/lib/apt/lists/*
44 mb

RUN apt-get update && apt-get install -y --no-install-recommends bzr git mercurial openssh-client subversion procps && rm -rf /var/lib/apt/lists/*
123 mb

RUN apt-get update && apt-get install -y --no-install-recommends

RUN apt-get update && apt-

RUN apt-get update && apt-

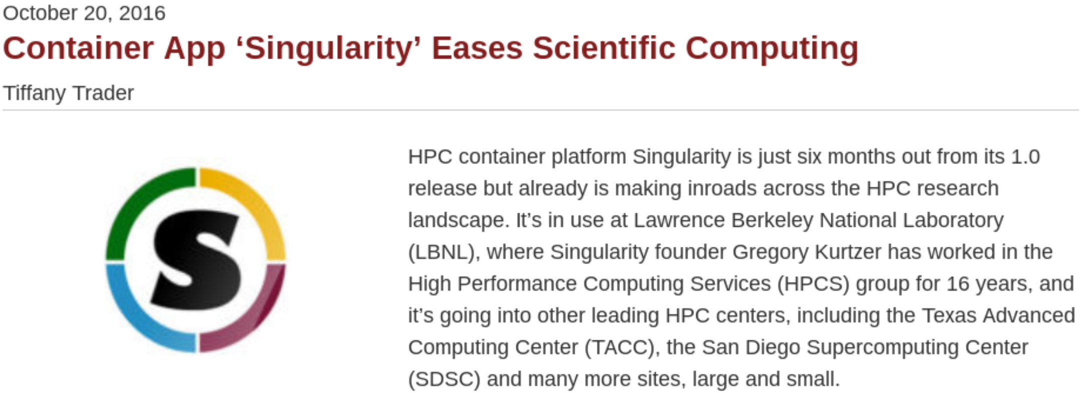
℮ 700 g

Over 30% of Official Images in Docker Hub Contain High Priority Security Vulnerabilities

Docker Hub is a central repository for Docker developers to pull and push container images. We performed a detailed study on Docker Hub images to understand how vulnerable they are to security threats. Surprisingly, we found that more than 30% of images in official repositories are highly susceptible to a variety of security attacks (e.g., Shellshock, Heartbleed, Poodle, etc.). For general images – images pushed by docker users, but not explicitly verified by any authority – this number jumps up to ~40% with a sampling error bound of 3%.

May 2015

https://www.banyanops.com/blog/analyzing-docker-hub/



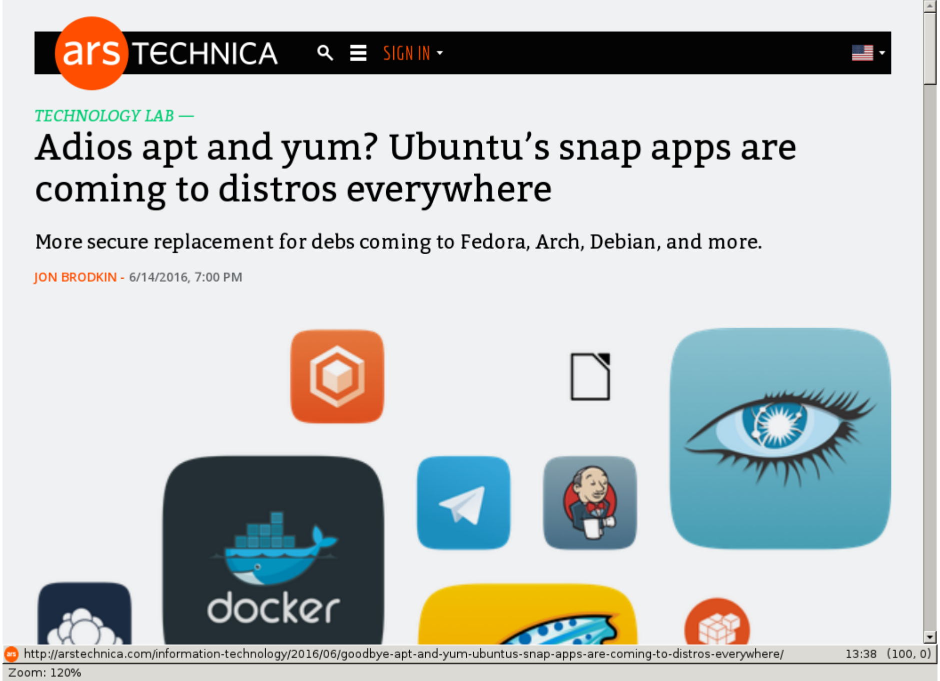
October 20, 2016

Container App ‘Singularity’ Eases Scientific Computing

Tiffany Trader

HPC container platform Singularity is just six months out from its 1.0 release but already is making inroads across the HPC research landscape. It’s in use at Lawrence Berkeley National Laboratory (LBNL), where Singularity founder Gregory Kurtzer has worked in the High Performance Computing Services (HPCS) group for 16 years, and it’s going into other leading HPC centers, including the Texas Advanced Computing Center (TACC), the San Diego Supercomputing Center (SDSC) and many more sites, large and small.

https://www.hpcwire.com/2016/10/20/singularity-containers-easing-scientific-computing



TECHNOLOGY LAB —

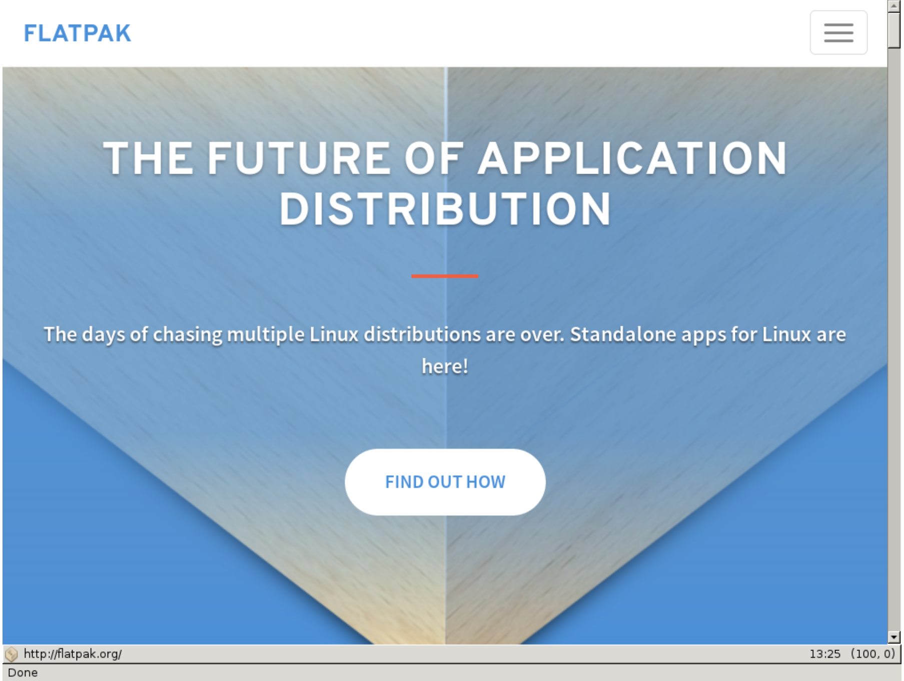
Adios apt and yum? Ubuntu’s snap apps are coming to distros everywhere

More secure replacement for debs coming to Fedora, Arch, Debian, and more.

JON BRODKIN - 6/14/2016, 7:00 PM

http://arstechnica.com/information-technology/2016/06/goodbye-apt-and-yum-ubuntus-snap-apps-are-coming-to-distros-everywhere/ 13:38 (100, 0)

Zoom: 120%



THE FUTURE OF APPLICATION DISTRIBUTION

The days of chasing multiple Linux distributions are over. Standalone apps for Linux are here!

“app bundles” are headed wrong

- difficulty to **compose** software packages
- wrong **abstraction level**: image vs. package
- **hardly reproducible**: we have the bits, not the source
- makes it hard to **customize & experiment**

HOPE

Make packaging great again!

GuixSD

Guix

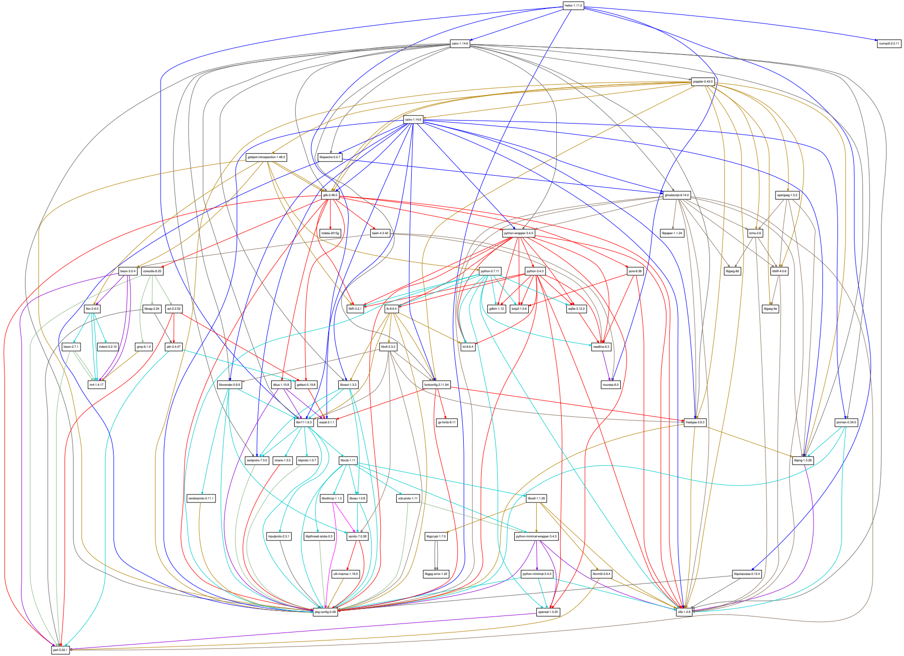
1. transactional package manager
2. software environment manager
3. APIs & tools to customize environments
4. packaging tools

```
$ guix package -i gcc-toolchain coreutils sed grep
…

$ eval ‘guix package --search-paths‘
…

$ guix package --manifest=my-software.scm
…
```

Want to get started hacking on hwloc?

Want to get started hacking on hwloc?

A simple matter of installing the deps, right?


hwloc-1.11.2
numactl-2.0.11
cairo-1.14.6
poppler-0.43.0
cairo-1.14.6
gobject-introspection-1.48.0
libspectre-0.2.7
glib-2.48.0
ghostscript-9.14.0
openjpeg-1.5.2
tzdata-2015g
bash-4.3.42
python-wrapper-3.4.3
libpaper-1.1.24
lcms-2.6
bison-3.0.4
coreutils-8.25
python-2.7.11
python-3.4.3
pcre-8.38
libjpeg-8d
libtiff-4.0.6
flex-2.6.0
libcap-2.24
acl-2.2.52
libffi-3.2.1
tk-8.6.4
gdbm-1.12
bzip2-1.0.6
sqlite-3.12.2
libjpeg-9a
bison-2.7.1
indent-2.2.10
gmp-6.1.0
attr-2.4.47
libxft-2.3.2
tcl-8.6.4
readline-6.3
m4-1.4.17
libxrender-0.9.9
dbus-1.10.8
gettext-0.19.8
libxext-1.3.3
fontconfig-2.11.94
ncurses-6.0
libx11-1.6.3
expat-2.1.1
gs-fonts-8.11
freetype-2.6.3
pixman-0.34.0
xextproto-7.3.0
xtrans-1.3.5
kbproto-1.0.7
libxcb-1.11
libpng-1.5.26
renderproto-0.11.1
libxdmcp-1.1.2
libxau-1.0.8
xcb-proto-1.11
libxslt-1.1.29
inputproto-2.3.1
libpthread-stubs-0.3
xproto-7.0.28
libgcrypt-1.7.0
python-minimal-wrapper-3.4.3
util-macros-1.19.0
libgpg-error-1.22
python-minimal-3.4.3
libxml2-2.9.4
libpciaccess-0.13.4
pkg-config-0.29
openssl-1.0.2h
zlib-1.2.8
perl-5.22.1

```
$ guix environment --container hwloc
…

$ guix environment --container hwloc \
     --ad-hoc git autoconf automake gdb
…
```

```
$ guix build hello
```

isolated build: chroot, separate name spaces, etc.

```
$ guix build hello
/gnu/store/ h2g4sf72... -hwloc-1.11.2
```

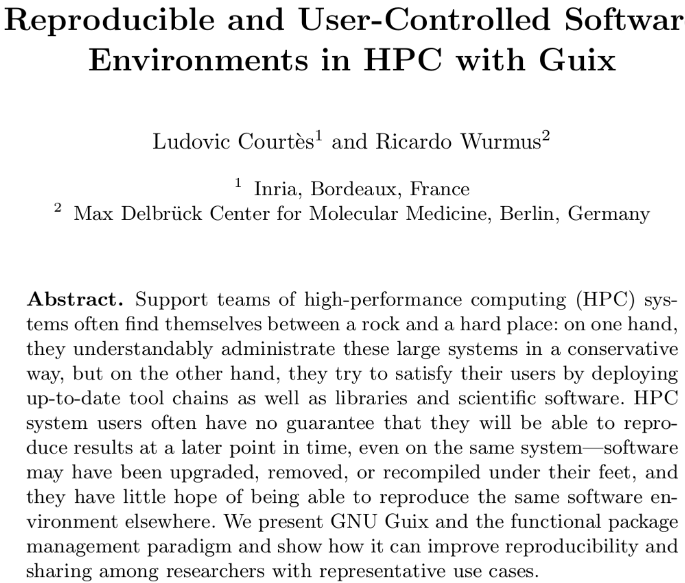
hash of **all** the dependencies

```
$ guix build hello
/gnu/store/ h2g4sf72... -hwloc-1.11.2

$ guix gc --references /gnu/store/...-hwloc-1.11.2
/gnu/store/...-glibc-2.24
/gnu/store/...-gcc-4.9.3-lib
/gnu/store/...-hwloc-1.11.2
```

```
$ guix build hello
/gnu/store/ h2g4sf72... -hwloc-1.11.2

$ guix gc --references /gnu/store/...-hwloc-1.11.2
/gnu/store/...-glibc-2.24
/gnu/store/...-gcc-4.9.3-lib
/gnu/store/...-hwloc-1.11.2
```

(nearly) bit-identical for everyone

Can we go
beyond mere reproducibility
and support **experimentation**?



Reproducible and User-Controlled Software Environments in HPC with Guix

Ludovic Courtès[1] and Ricardo Wurmus[2]

[1] Inria, Bordeaux, France
[2] Max Delbrück Center for Molecular Medicine, Berlin, Germany

Abstract. Support teams of high-performance computing (HPC) systems often find themselves between a rock and a hard place: on one hand, they understandably administrate these large systems in a conservative way, but on the other hand, they try to satisfy their users by deploying up-to-date tool chains as well as libraries and scientific software. HPC system users often have no guarantee that they will be able to reproduce results at a later point in time, even on the same system—software may have been upgraded, removed, or recompiled under their feet, and they have little hope of being able to reproduce the same software environment elsewhere. We present GNU Guix and the functional package management paradigm and show how it can improve reproducibility and sharing among researchers with representative use cases.

https://hal.inria.fr/hal-01161771/en

Creating package variants at the command line

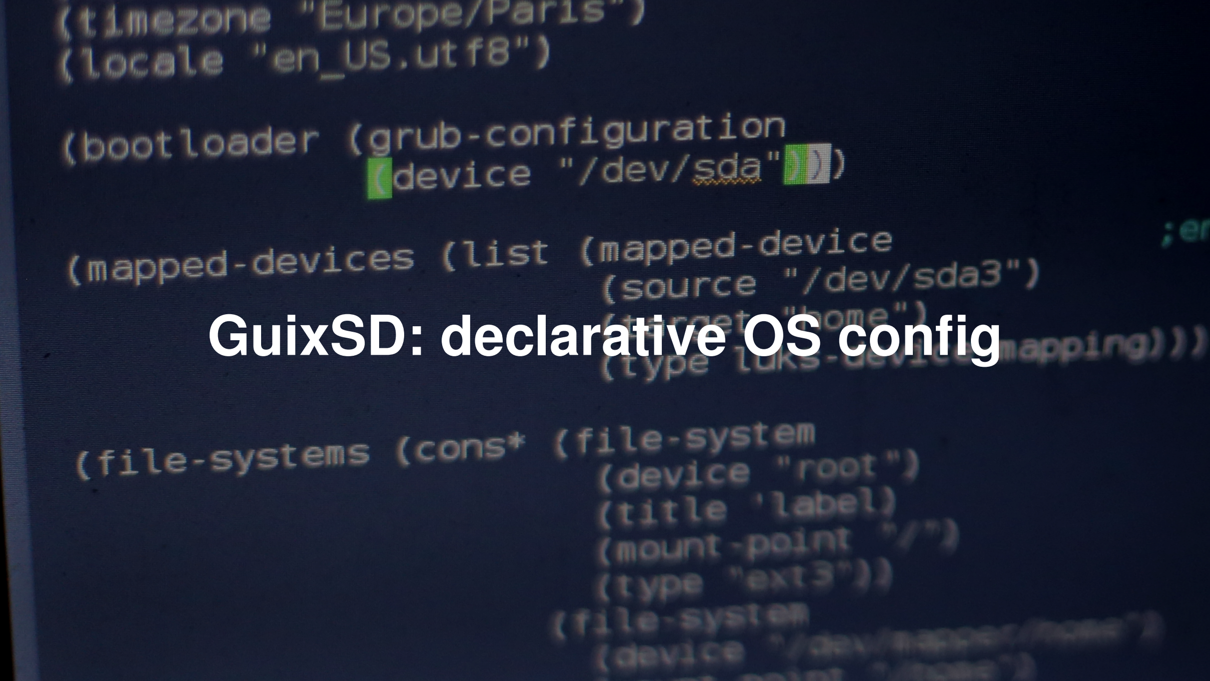
```
$ guix build hwloc \
    --with-source=./hwloc-42.0rc1.tar.gz
...
```

```
$ guix build hwloc \
    --with-source=./hwloc-42.0rc1.tar.gz
…
```

```
$ guix package -i mumps \
     --with-input=scotch=pt-scotch
…
```

Your personal packages or variants in `GUIX_PACKAGE_PATH`!

GuixSD: declarative OS config



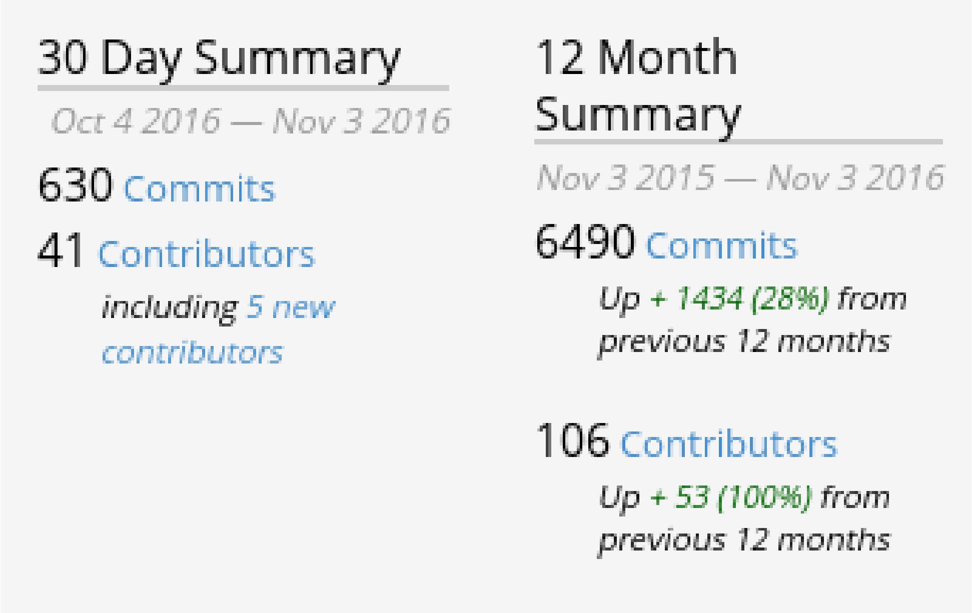
```
(timezone "Europe/Paris")
(locale "en_US.utf8")

(bootloader (grub-configuration
              (device "/dev/sda")))
                                                         ;en
(mapped-devices (list (mapped-device
                        (source "/dev/sda3")
                        (target "home")
                        (type luks-device-mapping))))

(file-systems (cons* (file-system
                       (device "root")
                       (title 'label)
                       (mount-point "/")
                       (type "ext3"))
                     (file-system
                       (device "/dev/mapper/home")
```

Status.

- started in 2012
- **4,400+ packages**, all free software
- **4 architectures**:
  x86_64, i686, ARMv7, mips64el
- binaries at `https://hydra.gnu.org`
- 0.11.0 released in August 2016

cluster deployments & usage

- **Max Delbrück Center** (DE): 250-node cluster + workstations
- **Utrecht Bioinformatics Center** (NL): 68-node cluster (1,000+ cores)
- **GeneNetwork**, “framework for web-based genetics”



30 Day Summary

Oct 4 2016 — Nov 3 2016

630 Commits

41 Contributors

including 5 new contributors

12 Month Summary

Nov 3 2015 — Nov 3 2016

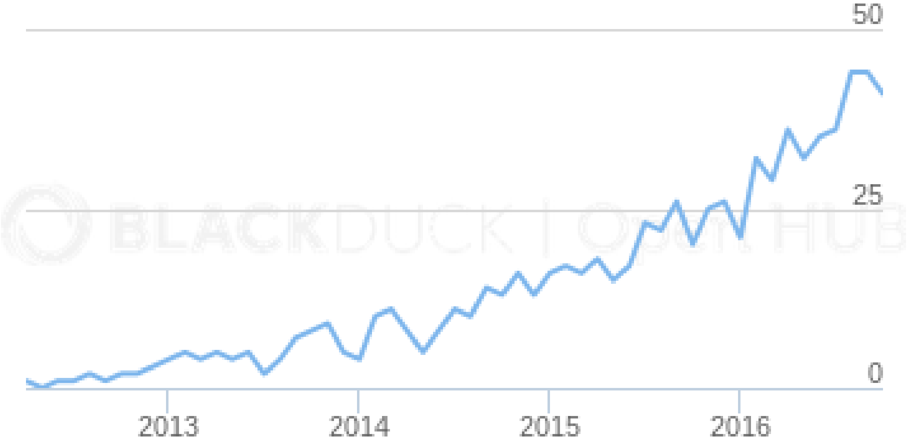
6490 Commits

Up + 1434 (28%) from previous 12 months

106 Contributors

Up + 53 (100%) from previous 12 months

Contributors per Month



Wrap-up.

Summary

- Guix supports **reproducible software environments**
- ... can be extended with **personal packages**
- ... allows for **experimentation** through customization
- ... is entirely **programmable**

GuixSD

ludo@gnu.org

https://gnu.org/software/guix/