Fearless deployments with Guix

Christopher Allan Webber

2016-03-04 Fri
Who am I?
The web we want
The sad reality (centralization)
The sad reality (censorship)
The sad reality (surveillance)
The sad reality (fragility)
The sad reality (fragility)
The sad reality (fragility)
The sad reality (fragility)
So I work on MediaGoblin...
Decentralized media publishing

Caminandes: Gran Dillama

Caminandes is an independently produced short animated series, inspired by the good old Chuck Jones cartoons. Caminandes is produced using FLOSS (Free/Libre Open Source Software) such as Blender, the GIMP, Krita and GNU/Linux.

You can find out more about Caminandes at http://caminandes.com!
Sounds great! But???

4) Bring MediaGoblin to the people!
Stuff is complex to run

"""""""""
"(_o (_o
G ,)
__/ (uuuu)
/ \ '-----'
'--',
\ \ .-- .'
' _3|___| )3

I AM GONNA BE HONEST WITH YA
I AM AFEARED TO UPGRADE MY OWN SOFTWARES
Dependent on phase of the moon
One Language Package Manager Per Child
Have fun managing configuration
So... docker??? (Or something like it?)

Easy for users! "I already built this for you, just pull it down and use it!"
Maybe not :)
Distro-sized static compiling considered hazardous

- Extremely heavy: throws away dynamic linking
- Hard to introspect, rebuild
- Analysis of Docker Hub: over 70% have medium vulnerabilities, 30-40% high (shellshock, heartbleed) vulnerabilities
- Reproducible? Only kinda... Docker’s DSL is not expressive, and..
- Still dependent on "phase of the moon" of distributions!
And so here we are
Enter Guix! Enter GuixSD!
Functional packaging (hold the monads!)
All the way down!
Setting the stage

Enter Guix!

Like git, for your operating system!

cwebber@oolong:~$ ls -l ~/.guix-profile/bin
total 1612
lrwxrwxrwx 3 root guixbuild 65 Dec 31 1969 2to3 -> /gnu/store/xw8ikmsj7b62aimwyd9kwxygxs78hl-python-3.4.3/bin/2to3
lrwxrwxrwx 3 root guixbuild 69 Dec 31 1969 2to3-3.4 -> /gnu/store/xw8ikmsj7b62aimwyd9kwxygxs78hl-python-3.4.3/bin/2to3-3.4
lrwxrwxrwx 16 root guixbuild 66 Dec 31 1969 abbaye -> /gnu/store/9qr1p42rsjpxc08c7q7qa4g15q5pibabbaye-1.13/bin/abbaye
lrwxrwxrwx 3 root guixbuild 69 Dec 31 1969 aclocal -> /gnu/store/rr3wsxa5q3hkvw9q8km114clrv7rdk-automake-1.15/bin/aclocal
lrwxrwxrwx 3 root guixbuild 74 Dec 31 1969 aclocal-1.15 -> /gnu/store/rr3wsxa5q3hkvw9q8km114clrv7rdk-automake-1.15/bin/aclocal
lrwxrwxrwx 22 root 1001 73 Dec 31 1969 aconnect -> /gnu/store/1jqsldmm16j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/aconnect
lrwxrwxrwx 3 root guixbuild 71 Dec 31 1969 acyclic -> /gnu/store/4g4gq0dny1cap0fa0idf248ys7cx2mv-graphviz-2.38.0/bin/acyclic
lrwxrwxrwx 22 root 1001 77 Dec 31 1969 addr2line -> /gnu/store/7m8s5qm2xy730lwxhhaccq7i4pky8i-gcc-toolchain-5.3.0/bin/addr2line
lrwxrwxrwx 22 root 1001 73 Dec 31 1969 alsaline -> /gnu/store/1jqsldmm16j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/alsaline
lrwxrwxrwx 22 root 1001 74 Dec 31 1969 alsaloop -> /gnu/store/1jqsldmm16j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/alsaloop
lrwxrwxrwx 22 root 1001 74 Dec 31 1969 alsamixer -> /gnu/store/1jqsldmm16j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/alsamixer

cwebber@oolong:~$ ls /gnu/store | head
001fmr72xkw284d1wd067zyyl2p0-grep-2.21.drv
004fhpfnca119v7zaa4p7rj31bz7f-redland-1.0.17-guile-builder
0267bij0d578gh66scn38bjz44n567d-other.drv
02111ka4a8v87d0ikrm543bl0wd6a7z-guile-static-stripped-2.0.11.drv
030hbb317r4kqsqlb459h3jsl157fkl-libspectre-0.2.7.drv
04ib0h788s3bcjm26q7szvk1k8qszgd-git-manpages-2.6.3.tar.xz.drv
04ppl9mvhi54mvfrid38363pnh2glvz-unzipped-6.0.drv
05z5jrc8yrr8z205gpc5ml3313qpqf-python-2.7.10.drv
099903g12b1pny50a8ccq9yiw9bbniz-libxshmfence-1.1.tar.bz2.drv
0c6nc4n4a66j19k04ngvf9xwy6vmmrnm-shared-mime-info-1.2.tar.xz.drv
cwebber@oolong:~$

Setting the stage
Enter Guix!

Keep the history until you don’t need it

<table>
<thead>
<tr>
<th>N.</th>
<th>Current</th>
<th>Time</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>212</td>
<td>2016-03-03 17:12:31</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-212-link</td>
</tr>
<tr>
<td></td>
<td>211</td>
<td>2016-03-03 13:49:49</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-211-link</td>
</tr>
<tr>
<td>*</td>
<td>210</td>
<td>2016-03-03 10:16:30</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-210-link</td>
</tr>
<tr>
<td></td>
<td>209</td>
<td>2016-03-02 08:23:37</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-209-link</td>
</tr>
<tr>
<td></td>
<td>208</td>
<td>2016-03-02 07:40:41</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-208-link</td>
</tr>
<tr>
<td></td>
<td>207</td>
<td>2016-03-02 07:35:21</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-207-link</td>
</tr>
<tr>
<td></td>
<td>206</td>
<td>2016-03-02 07:35:02</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-206-link</td>
</tr>
<tr>
<td></td>
<td>205</td>
<td>2016-03-02 07:34:24</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-205-link</td>
</tr>
<tr>
<td></td>
<td>204</td>
<td>2016-03-02 07:33:51</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-204-link</td>
</tr>
<tr>
<td></td>
<td>203</td>
<td>2016-03-01 19:18:01</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-203-link</td>
</tr>
<tr>
<td></td>
<td>202</td>
<td>2016-03-01 15:03:39</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-202-link</td>
</tr>
<tr>
<td></td>
<td>201</td>
<td>2016-03-01 14:27:47</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-201-link</td>
</tr>
<tr>
<td></td>
<td>200</td>
<td>2016-03-01 12:25:25</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-200-link</td>
</tr>
<tr>
<td></td>
<td>199</td>
<td>2016-03-01 12:23:29</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-199-link</td>
</tr>
<tr>
<td></td>
<td>198</td>
<td>2016-03-01 12:13:22</td>
<td>/var/guix/profiles/per-user/cwebber/guix-profile-198-link</td>
</tr>
</tbody>
</table>

```
--- #<buffer> *Guix* guix-profile: generation 210*
+++ #<buffer> *Guix* guix-profile: generation 212*
@@ -1,40 +1,40 @@
    abbaye-1.13:out       /gnu/store/9qr1p42rsjp20cpk7q7qza4g15g5pibi-abbaye-1.13
    alsa-utils-1.1.0:out  /gnu/store/ljgslldmml6j0hhwl2mjhky1z7z01p75-alsa-utils-1.1.0
-aspell-0.60.6.1:out    /gnu/store/d6y35430s9sagx0cccl1fz5j92w91x0a-aspell-0.60.6.1
+aspell-0.60.6.1:out    /gnu/store/dhj0k9sk83479x1259nq18p51kk48cg6-aspell-0.60.6.1
    aspell-dict-en-2016.01.19-0:out /gnu/store/c1352syqqw8wq1pdpw161qzc83jhasmy-aspell-dict-en-2016.01.19-0
-assword-0.8:out        /gnu/store/4h145h9n9mqwqqd2kvslijqhx4p21w6s-assword-0.8
-autoconf-2.69:out      /gnu/store/bj59z4k62ksmmwnwsc53d2pi9dw7k-autoconf-2.69
-automake-1.15:out      /gnu/store/3c88rbypnfbcrvprx8wpw98vmd7yycf-automake-1.15
+assword-0.8:out        /gnu/store/qkyv8zd03zd24vzsz4g8do1layvrgpzd-assword-0.8
+autoconf-2.69:out      /gnu/store/mbr57wq24drlrqksab5szyyhs2a47b5q4-automake-2.69
+automake-1.15:out      /gnu/store/rr3wsxa5q53hkvw9q8kmm14clrv7rd-automake-1.15
```
You are now a time wizard.

# Bad upgrade? No problem!
guix package --roll-back
Your profile, my profile

- User profiles don’t conflict with system profiles
- Local development environments with `guix environment`
- Need a different glibc or gcc or whatever? No problem!
- As many profiles as you want
Wait, why not Nix?

Guix is based on Nix’s ideas! And Nix is super cool! But it’s hard to write tooling...
Guix is just scheme, yo

```
(define-public grep
  (package
   (name "grep")
   (version "2.21")
   (source
    (origin
     (method url-fetch)
     (uri (string-append "mirror://gnu/grep/grep-" version "tar.xz"))
     (sha256
      (base32
       "1pp5n15qwxrw1pbwjjhgsibvyv5cafhamf81wzjygs6y00fa2i2j"))
     (patches (list (search-patch "grep-CVE-2015-1345.patch"))))
    (build-system gnu-build-system)
   (synopsis "Print lines matching a pattern")
   (description
    "grep is a tool for finding text inside files. Text is found by matching a pattern provided
    by the user in one or many files. The pattern may be provided as a basic or extended regular
    expression, or as fixed strings. By default, the matching text is simply printed to the
    screen, however the output can be greatly customized to include, for example, line
    numbers. GNU grep offers many extensions over the standard utility, including, for example,
    recursive directory searching."
    (license gpl3+)
    (home-page "http://www.gnu.org/software/grep/"))
)
```
Oh no parentheses!?
Parentheses: Not so foreign after all!
Guix is a library, too

All datastructures, functions, etc exposed. Hack away!
With very little additional code, Guix(SD) has:

- Declarative config management (like Puppet, Chef, Salt, Ansible)
- Universal language packaging (apt, yum, pip/eggs, gems...)
- Local dev environments (virtualenv, rvm, rbenv...)
- Local VM tooling (Vagrant...)
- Container support (Docker, Rocket...)

Add your own tools here!
This just in: grafts!
State of Guix

- "It’s still beta!"
- But probably more stable than most devops stuff
- A delight to run (I use it!)
- Easy to develop and get involved in
What’s next?

- More packages! (~3350 at time of writing)
- Deployment tools (GuixOps!)
- Good UI tools needed! (Not just emacs and command line :))
- Some day soon we’ll have to tackle the nightmare of npm
- Sandboxed containers!
A short story
Credits (p.1)


- Tar pit image by Ray Bouknight, CC BY 2.0: https://www.flickr.com/photos/raybouk/8341369957

- Snowflake from zfootage, CC BY 4.0: https://www.youtube.com/watch?v=Arw269x4duQ https://i.ytimg.com/vi/Arw269x4duQ/maxresdefault.jpg

- Rena runs aground (container fail image), CC BY 2.0 https://www.flickr.com/photos/nzdefenceforce/6386334175/

- Tree grafting image, CC BY-SA 2.0 https://www.flickr.com/photos/51691575@N00/2540483417
Credits (p.2)

- Caminandes video screenshot by Blender Institute, CC BY 4.0
  http://www.caminandes.com/

- Chemical warehouse image from Pixabay, CC0 https://pixabay.com/en/warehouse-chemistry-industry-629641/

- GuixSD logos by Luis Felipe López Acevedo, CC BY-SA 4.0
  http://www.gnu.org/software/guix/graphics/

- Docker + Twitter image by Karen Rustad

- NixOS logo by NixOS team

- Some parts borrowed from David Tompson’s presentation

- Slight snippet from Guix (grep package), GPLv3 or later

- Everything else by me (I think???)
Thanks! Questions? (Demonstrations?)

© 2016 Christopher Allan Webber <cwebber@dustycloud.org>
This presentation is licensed under the Creative Commons Attribution Share-Alike 4.0 International license.
More on Guix: https://gnu.org/software/guix
More on MediaGoblin: http://mediagoblin.org/