Stop demonizing curl | bash

Or, installing software is hard

Joshua Timberman
Code Cleric, Chef Software, Inc.
@jtimberman
joshua@chef.io

What is curl | bash?

```
curl http://www.example.com/install.sh | sudo bash
curl -sSL https://get.rvm.io | bash -s stable
ruby -e "$(curl -fsSL https://raw.github.com/Homebrew/
homebrew/install)"
wget --no-check-certificate http://install.ohmyz.sh -O -
| sh
curl -L https://npmjs.org/install.sh | sh
wget -qO- https://toolbelt.heroku.com/install-ubuntu.sh |
sh
curl https://static.rust-lang.org/rustup.sh | sudo bash
curl -L https://www.chef.io/chef/install.sh | sudo bash
```

For more: http://curlpipesh.tumblr.com/

CHEF

Why is it bad?

- Running arbitrary code is bad
- Running arbitrary code as root is bad
- Running arbitrary code as root from an unencrypted source is bad
- Running arbitrary code as root from an unencrypted source may yield different results in six months than it does today (and that's bad)!
- Also, shell scripts aren't inherently convergent or idempotent, so the author has to implement that too

Packages are a better way to install software

- Packages come from a trusted source
- You trust your distribution, right?
- They would never do something unexpected in a post installation script right?

sudo apt-get install mysql-server

```
....
Setting up mysql-server-5.5 (5.5.41-0ubuntu0.14.04.1) ...
150417  1:18:12 [Warning] Using unique option prefix
key_buffer instead of key_buffer_size is deprecated and will
be removed in a future release. Please use the full name
instead.
mysql start/running, process 18491
$ ps awux | grep mysql
mysql 18491  0.3 12.0 623912 44984 ?  Ssl  01:18   0:00 /usr/
sbin/mysqld
$ less /var/lib/dpkg/info/mysql-server-5.5.postinst
#... lots of configuration via shell, then:
invoke-rc.d mysql start
```

CHEF

Cynicism! Here's CentOS & RPM...

```
$ sudo rpm -ivh https://github.com/danielsdeleo/cynical/blob/master/cynical-1.0.0-1.x86_64.rpm?raw=true
Retrieving https://github.com/danielsdeleo/cynical/blob/master/cynical-1.0.0-1.x86_64.rpm?raw=true
Preparing...                ########################################### [100%]
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 18990  100 18990    0     0  45464      0 --:--:-- --:--:-- --:--:--  185k
Downloading Chef  for el...
downloading https://www.opscode.com/chef/metadata?v=&prerelease=false&nightlies=false&p=el&pv=6&m=x86_64
  to file /tmp/install.sh.2810/metadata.txt
trying wget...
url https://opscode-omnibus-packages.s3.amazonaws.com/el/6/x86_64/chef-12.2.1-1.el6.x86_64.rpm
md5 750c9509b04f3b8bb997bab2bb1831ee
sha256 e428180890b381382caa71f726e5790bbc1b86551050ae214bb1a9812373f2a3
downloaded metadata file looks valid...
downloading https://opscode-omnibus-packages.s3.amazonaws.com/el/6/x86_64/chef-12.2.1-1.el6.x86_64.rpm
  to file /tmp/install.sh.2810/chef-12.2.1-1.el6.x86_64.rpm
trying wget...
Installing Chef
installing with rpm...
warning: /tmp/install.sh.2810/chef-12.2.1-1.el6.x86_64.rpm: Header V4 DSA/SHA1 Signature, key ID 83ef826a:
NOKEY
Preparing...                ########################################### [100%]
   1:chef                   ########################################### [100%]
Thank you for installing Chef!
   1:cynical                ########################################### [100%]
```

CHEF


https://www.flickr.com/photos/xavier33300/9124156847

The thing is... curl retrieves text

```
curl http://www.example.com/install.sh | less
#!/bin/bash
# This script handles installing our
# software because we want to maximize the
# value of your time. It is intended to be
# easy to do with a curl|bash installation,
# so you can start using it quickly.
# Besides, you're using a test machine,
# right?
# Sincerely, The Authors
```

CHEF

How to do it right, step 1

- Build a package for your users
- Even better, create a package repositories
- Better yet, use Package Cloud (packagecloud.io): they did the hard stuff for you
- (Don't do anything in postinstall, either!)

How to do it right, step 2

- Serve your install script over HTTPS
- Make sure your certificate is valid
- Watch out for wget on RHEL 5 when using Subject-Alternative-Names (SAN), though

How to do it right, step 3

- Verify the content of the package
- Use cryptographically secure checksums (e.g., SHA256)
- Serve checksums over HTTPS, too

Chef has done it right! ;)

- Default installation is via install.sh
- Detects the OS
- Talks to an API service
- Packages available on PackageCloud*

*We're working on chef client packages

CHEF

Chef's Omnitruck API

```
$ curl -L 'https://www.chef.io/chef/metadata?p=el&pv=7&m=x86_64'

url  https://opscode-omnibus-packages.s3.amazonaws.com/el/6/x86_64/
chef-12.2.1-1.el6.x86_64.rpm
md5  750c9509b04f3b8bb997bab2bb1831ee
sha256 e428180890b381382caa71f726e5790bbc1b86551050ae214bb1a9812373f2a3
```

CHEF

Here's the thing...

- https://docs.chef.io/supported_platforms.html
- Multiple architectures (i386, x86_64, sparc, ppc)
- Multiple versions of each

AIX	Red Hat / CentOS / Oracle
Fedora	SUSE
FreeBSD	SmartOS
Mac OS X	Solaris
OmniOS	Debian / Ubuntu

CHEF

That's > 50 permutations

Six different package types

Not all have repos (AIX, Solaris, OS X...)

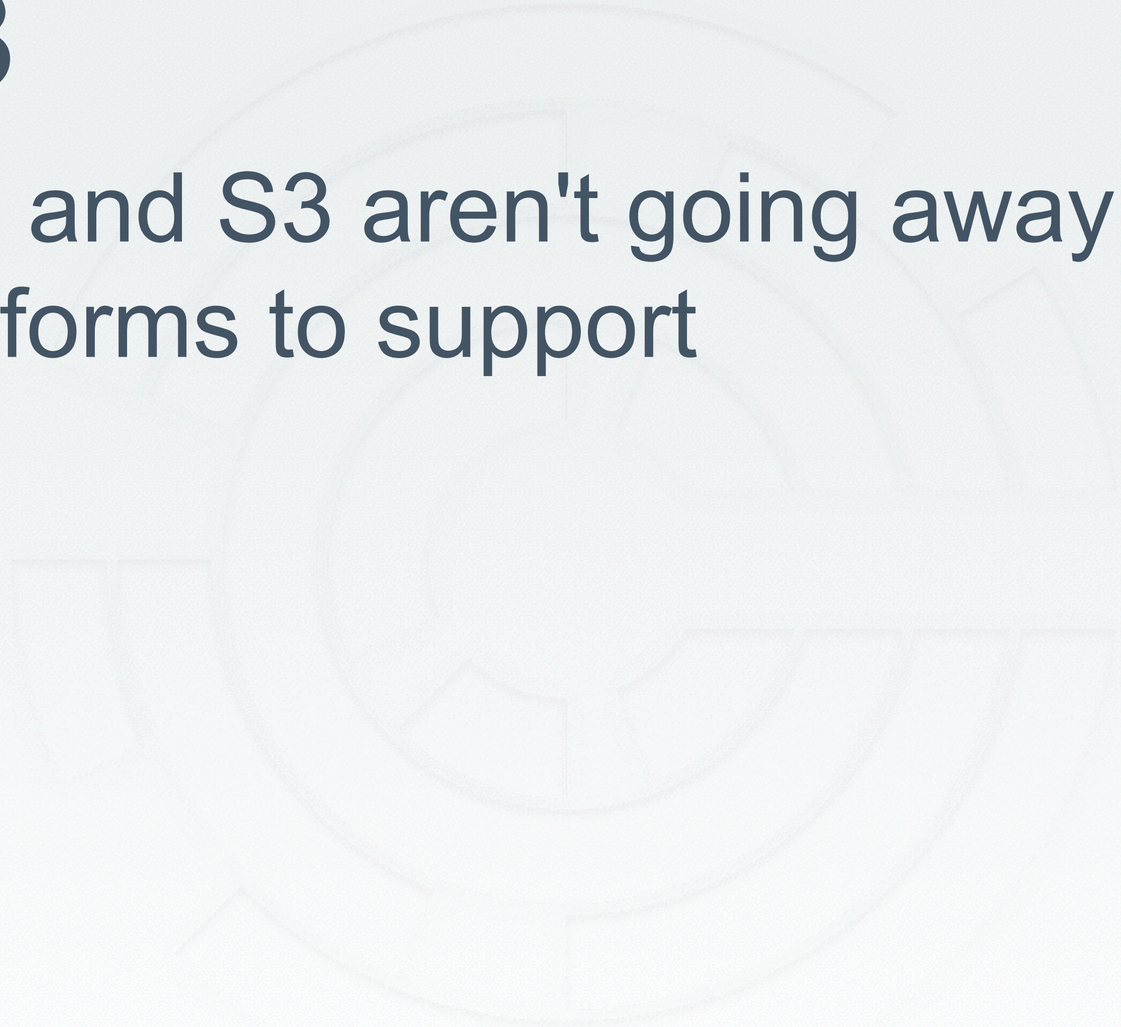
(That doesn't count Windows...)

Package Repositories

- Chef uses Package Cloud for .deb and .rpm packages (accounts for most permutations)
- Client package repositories on Package Cloud are coming soon, we have ChefDK, Chef Server, and premium add-ons like Analytics

Omnitruck and S3

- Omnitruck (the API service) and S3 aren't going away
- We still have dozens of platforms to support



Windows is special

Not usually done via curl | bash...
But, there's Powershell!

```
Import-Module BitsTransfer

Start-BitsTransfer "https://www.chef.io/chef/download-chefdk?
p=windows&pv=2008r2&m=x86_64&v=latest" "chefdk.msi"
Start-Process -FilePath 'msiexec.exe' -ArgumentList "/qn /i chefdk.msi" -Passthru
```

CHEF

curl -L https://www.chef.io.sh/chef/install.sh | sudo bash

- HTTPS, Valid certificate, checksum
- No unexpected postinst
- Use Chef to replace other curl | bash installers :-)
- Or use Chef to configure its own running service...

Moral of the story?

curl | bash to install Chef
Then daemonize Chef

Write recipes for installing NPM, Heroku toolbelt, RVM, or whatever else you used to curl | bash :-).