

An apt talk

Julian Andres Klode

Aug 7, 2017

An apt talk

- APT is short for 'Advanced Package Tool', right?
- We could spell 'A', 'P', 'T'
- Maybe we just pronounce it as a word like 'apt'
- Just write 'apt'? What about 'apt(8)'

In any case, this is an apt talk about

APT
Advanced Package Tool
apt

Let's talk about more *important* stuff.

BSD/macOS porting

- Portability is great to catch bugs, thus want to support BSDs
- Good way to ensure things do not break is to do CI
- We use Travis, it only supports Windows, Linux, and macOS

Solution: Port to Mac

- I don't actually have access to a Mac; but
 - Could port to FreeBSD
 - Could get it completely compiling with someone else testing
- Mac is not really a nice UNIX platform, it lacks a lot of functions that Linux and FreeBSD have (especially POSIX.1-2008)
- Not really done yet

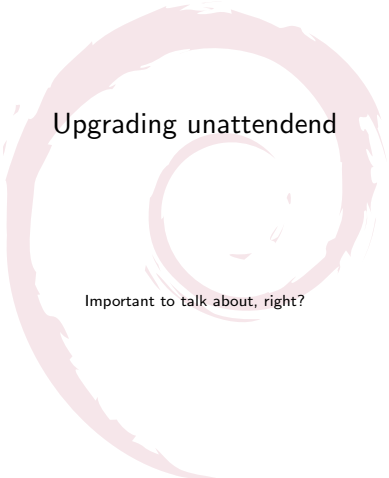
BSD/macOS porting

- Portability is great to catch bugs, thus want to support BSDs
- Good way to ensure things do not break is to do CI
- We use Travis, it only supports Windows, Linux, and macOS

Solution: Port to Mac

- I don't actually have access to a Mac; but
 - Could port to FreeBSD
 - Could get it completely compiling with someone else testing
- Mac is not really a nice UNIX platform, it lacks a lot of functions that Linux and FreeBSD have (especially POSIX.1-2008)
- Not really done yet

OK, this page was not *that* important



Upgrading unattended

Important to talk about, right?

Cron job - Before 1.2.10

- Daily cron job that runs update, unattended-upgrade, and clean
- Cron jobs usually run sometime between 6 and 7 am
- Random sleep up to 30 minutes to reduce mirror load

Cron job - Before 1.2.10

- Daily cron job that runs update, unattended-upgrade, and clean
- Cron jobs usually run sometime between 6 and 7 am
- Random sleep up to 30 minutes to reduce mirror load

Problem: 30 minutes random delay still overloads Ubuntu mirrors

1.2.10: systemd timer

- Runs at 6 am and pm \pm 12 hours - *anytime* to distribute mirror load
- Persistent timer: Will start at boot/resume if real time elapsed

(yes, we still have a cron job for non-systemd systems)

1.2.10: systemd timer

- Runs at 6 am and pm \pm 12 hours - *anytime* to distribute mirror load
- Persistent timer: Will start at boot/resume if real time elapsed

(yes, we still have a cron job for non-systemd systems)

Problems:

- Unattended upgrades starts breaking systems during business hours
- If the service starts at boot or resume, it does not wait for network

1.4.1 to 1.4.6: The big split

- Break timer into two: One for update, and one for upgrade and clean
- Update job runs randomly throughout day, upgrade in 6..7am
- Make the timer depend on the network-online target
- Took about 6 tries to get right (1.4.1 to 1.4.6)

1.4.1 to 1.4.6: The big split

- Break timer into two: One for update, and one for upgrade and clean
- Update job runs randomly throughout day, upgrade in 6..7am
- Make the timer depend on the network-online target
- Took about 6 tries to get right (1.4.1 to 1.4.6)

Remaining problem: network-online only helps at boot

HTTPS support

2006: Added curl-based https methods

- No pipelining support (we sent requests to curl sequentially)
- No support for using https proxies for http urls
- Duplicated code and different functionality

2017: APT 1.5

- https support merged into the http method
- Only difference between https and http now: The TLS layer
→ Abstracted away using decorator pattern

Some things might have stopped working, let us know!

Stop using apt-key

more importantly: apt-key is deprecated, stop using it.

- gnupg might not be installed on new systems anymore; but
- most features require it

To install keyrings:

- drop a public key packet sequence in a .gpg file into trusted.gpg.d (since squeeze); or
- if you only need to support 1.4+ (stretch+), you may use ASCII armored .asc files
- Use `gpg --export` to generate the files
- Do **not** use `gpg --keyring` on those files, `gpg` uses a format called *keybox* for that now

In other news

1.4:

- apt(-get) moo is now reproducible
- SHA1 is now completely untrusted

1.5:

- If values in Release files (like Codename) change, that needs to be confirmed on the client
- auth.conf (netrc for APT) is now documented

Did I mention that you should stop relying on apt-key?