TAMPERE UNIVERSITY OF TECHNOLOGY

Caddy & Santa Came To Town

FinMacAdmin 2017

Antti Pettinen
IT Services
Tampere University of Technology
@apettinen
antti.pettinen@tut.fi

$ whoami

- Antti Pettinen
  - System Analyst @ tut.fi
    - macOS & iOS, other mobile devices (Airwatch), IT Security
    - administering TCSC computation cluster
  - Ph.D in CS (comp. neuroscience)
    - i.e. ex-{researcher, hospital_phycisist} turned to sysadmin in 2012
    - Linux/Unix since early 2000, Macs since 2009
  - @apettinen in Twitter, Slack, Github etc.
  - dad, husband, football, music, beer

IT-Services @ TUT

- responsible for all IT in TUT
  - ~ 2500 clients, ~250 Macs, hundreds of servers
- 54 employees divided to different branches
  - IT-helpdesk & Workstation Management
  - ICT-infrastructure
  - System Services
  - Telephone services

“Serve The Web Like It's 2017”

- apache, nginx, etc. are battle tested, but…
  - configuring can be hard and error prone
- munki requires just a simple file server
- simple alternative?

  => https://caddyserver.com/

Caddy Web Server

- written in go, https://github.com/mholt/caddy/
- available for Windows, Mac, Linux, and BSD
- automatic HTTPS via Let's Encrypt!
  - all sites served over HTTPS by default!
- great for static files - e.g. Munki

Features

Caddy makes web development faster, easier, and more productive for busy people with busy websites.

HTTP/2

It's time for a faster web. Caddy supports HTTP/2 right out of the box. No thought required.

Automatic HTTPS

Caddy uses Let's Encrypt to serve your sites over HTTPS without any hassle. Supports SNI.

Easy Deployment

Caddy is a single executable with no dependencies. Any platform.

Multi-core

When the going gets tough, Caddy gets going on more CPUs.

WebSockets

Caddy can pipe stdin and stdout from any program to WebSocket clients.

Markdown

Serve Markdown documents rendered on-the-fly as HTML.

IPv6

Runs full well in an IPv6 environment.

Logging

Caddy takes copious notes according to your favorite log format.

FastCGI

Serve PHP by proxying requests to FastCGI servers like php-fpm.

Headers

Send custom response headers just by adding a line to your Caddyfile.

Reverse Proxy

Forward requests to other endpoints with reverse proxy and load balancing.

Rewrites & Redirects

Rewrite requests internally or configure HTTP redirects.

Clean URLs

Elegantly serve files without needing the extension in the URL.

Gzip

Compress responses to save bandwidth.

Directory Browsing

List the contents of folders according to your own template.

Virtual Hosts

Serve multiple sites from the same address with a single Caddyfile.

Setting up Caddy

1. download Caddy (or build it yourself)
   - customize your build
2. make a Caddyfile (optional!)
   - analogous to httpd.conf or nginx.conf
3. run Caddy
   - nohup will get you far! (launchd/systemd/init even further)

Demotime

- do we use Caddy?
  - running in prod for a few months - no errors so far
  - fast even on old mac mini
  - runs as non-root
    - some ipfw “magic” required on macOS

Hey bin, Santa is watching!

- binary white-/blacklisting system for macOS
  - kernel ext + userland daemon + GUI agent + command-line tool
- based on rules in SQLite db
  - local-only rules or db sync with server
- developed by Google, https://github.com/google/santa

Santa features

- multiple modes:
  - monitor (blacklist)
  - lockdown (whitelist)
- event logging (log aggregation)
- rules:
  - certificate or path based
  - failsafe for blocking macOS components
    - App Store apps can be blocked!

Why Santa?

- protect users from themselves
  - block malicious binaries beforehand!
- stop spread of malware with centrally managed rules
- defence-in-depth
- Google MacOps run Santa in lockdown in prod.

Demotime

- install santa (`autopkg run santa.install`)
- to blacklist rule:

```
sudo santactl rule --blacklist --path /usr/bin/yes
--message "Computer says NO"
```

- to remove rule:

```
sudo santactl rule --remove --path /usr/bin/yes
```

Thanks!

- Join the community:
  - macadmin.fi
  - github.com/macadminfi
  - macadmins.org Slack #finland!
- Slides will be available in github.com/macadminfi/finmacadmin2017