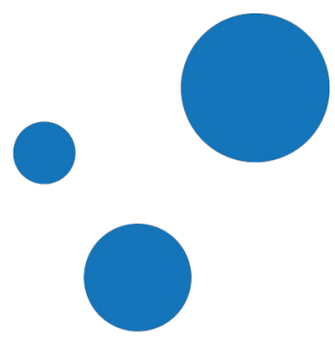
VARNISH SOFTWARE

Hitch TLS

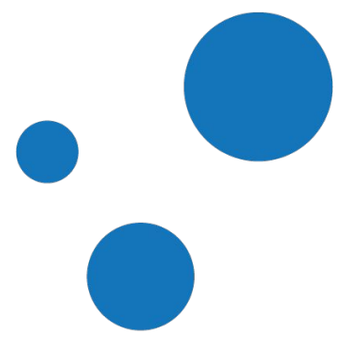
Dag Haavi Finstad
Varnish Software

daghf@varnish-software.com



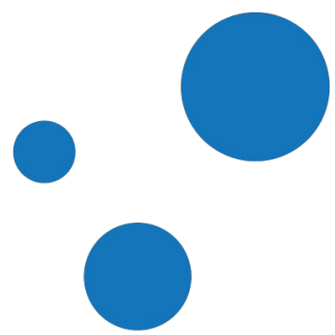
About me

- Software engineer
- Varnish Software since 2012
- Worked on VS products, VMODs, other stuff
- Enjoy all things Varnish



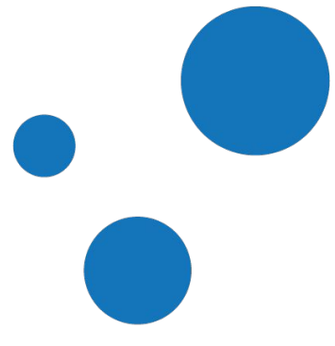
TLS basics

- TLS - standardised encryption protocol for streams.
- Lives between TCP and HTTP, adding authentication, integrity and confidentiality.
- TLS is originally based on SSL.
- All SSL versions are broken. Avoid if you can.
- TLS 1.2 is the one you should use.



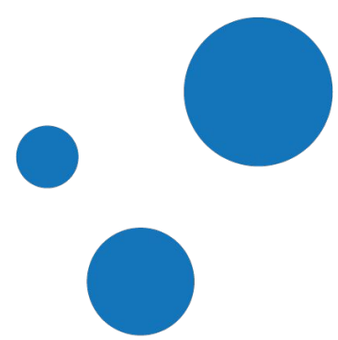
Hitch TLS

- A small and fast TLS terminator
- Developed by Varnish Software
- Based on the “stud” project by Bump Technologies.
- Freely available. BSD license



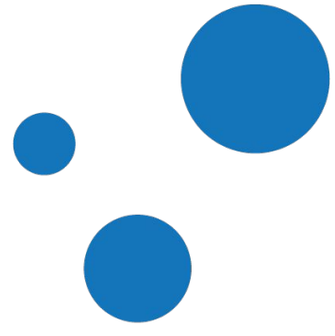
Hitch TLS (ii)

- Event-driven using `libev`
- One main management process
- N child processes, responsible for the actual heavy lifting



Setup and configuration

- Packages available for Debian and RHEL/Fedora (big thanks to Ingvar and Stig!)
- Latest version 1.1.0 (released last month)
- **Configuration in** `/etc/hitch/hitch.conf`

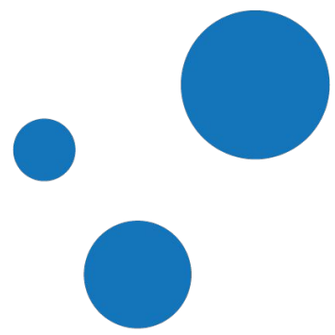


PROXY protocol

- Transmit client endpoints in a tiny header
- Originally from Willy Tarreau/HAProxy
- Example PROXYv1 header:

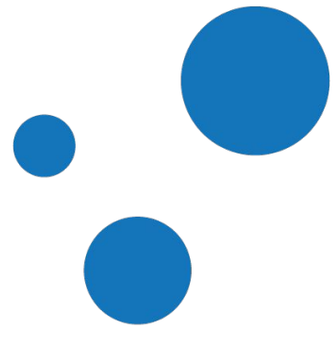
```
PROXY TCP4 192.168.0.1 192.168.0.11 56324 443\r\n
```

- Supported in Varnish 4.1.0
- .. and in Hitch, of course.



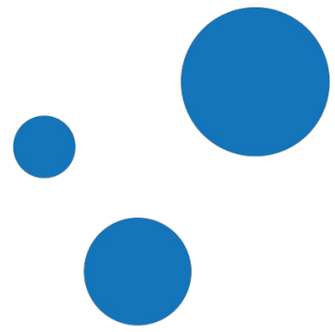
Run-time reloads

- Newly developed Hitch feature
- Seamlessly load new certificates and listen endpoints without interrupting service.
- Hitch will re-read its config on SIGHUP



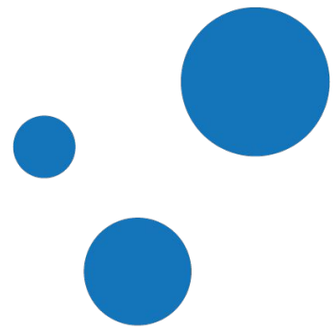
Performance

- In short: very good.
- Scales with any (reasonable) number of cpu cores.
- Up to 3000 new connections per second per core. (“SSL accelerator” cards not needed.)
- Fills 10Gbit ethernet without much effort.
- Tested with 500K certificates



Future improvements

- OCSP stapling
- Configuration: Setting different ciphers/TLS options per cert/listen endpoint
- ALPN/NPN for HTTP/2
- Shared session cache improvements



Questions?

daghf@varnish-software.com

https://hitch-tls.org/