# PowerDNS @ 2014

some notable features

PowerDNS in short

- Open source, around since 1999
  - We provide software & **high-end 24/7 support**
- Authoritative server (~30% market)
  - database, key/value store, script, http/RESTful driven
  - "One touch DNSSEC" support
    - >90% worldwide market share
  - Internal scripting for zone editing, external scripting for full zone hosting
- Recursor (hundreds of millions of users)
  - High performance, low latency
  - **Robust**
  - Very powerful scripting abilities

POWERDNS

POWERDNS

Total number of DNSSEC delegations in the .NL zone: 1721961

Data last updated 19 minutes ago
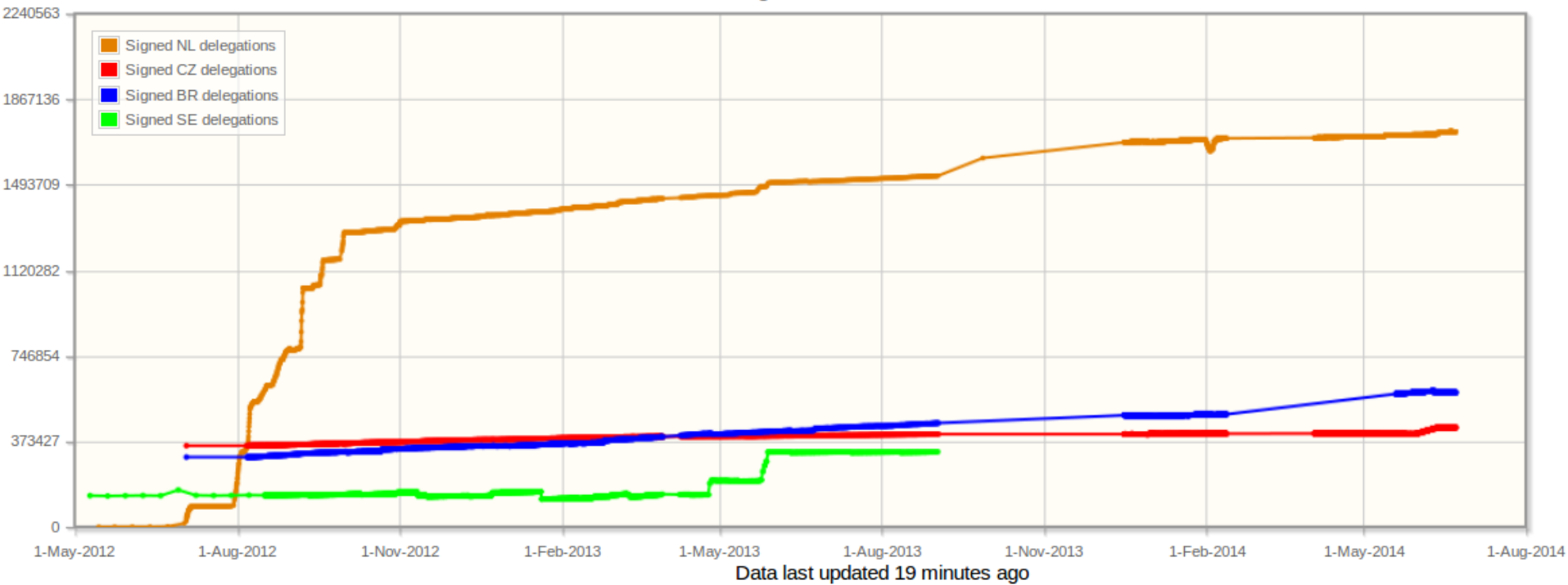
PowerDNS new (provisioning) API

- Provisioning is the DNS ugly stepchild
  - DNS can synchronize zone contents (AXFR, IXFR)
  - But **not** which zones to sync!
- Historically, "provisioning to SQL" has been popular for PowerDNS users
  - Use SQL-level replication, not DNS AXFR
  - Works well for millions and millions of zones
- Lately, we've been recommending our RESTful web-based API
- Uses a built-in webserver to accept provisioning commands
- Also, experimental nsupdate/2136

POWERDNS

PowerDNS API

- Recent versions of PowerDNS ship with this RESTful web based API
  - "opinionated"
- We also ship a simple web based maintenance system based on this API
  - 'pdnscontrol'
- However, we've consciously limited our web based solution to be **basic** since it won't ever fit everyone's needs

  - multi-tenancy, resellers, delegated admins, audit trails, multi-factor auth…
- Choice has paid off already

POWERDNS

Pdnscontrol

- Web based gui for maintaining a whole bunch of PowerDNS servers
- Individual and aggregate graphs & statistics
- Create, Remove, Update of zones and records
- Centralized cache flushing & log searching
- All modifications mediated through the PowerDNS API which rejects 'DNS impossibilities'
- **Soon to be a 'front page product'**

Servers

+

Filter

	Type	Name	Main IP	Version	Up for	Load
☑	Recursor			git-20140619-1266-bee8b93	3 days	
☑	Recursor			git-20140619-1266-bee8b93	3 days	
☑	Authoritative			git-20140502-4842-0832ec0	a month	
☑	Authoritative			git-20140502-4842-0832ec0	a month	
☑	Authoritative			git-20140502-4842-0832ec0	a month	
☑	Authoritative			git-20140502-4842-0832ec0	a month	

Flush cache   **Restart**   **Shutdown**

🔍   Log Message   **Search**

Running version **git-20140619-1266-bee8b93**, up since Thursday, June 19 2014 8:25 PM (3 days).

Log Message   Search

Graphs   Statistics   Zones   Configuration

24h 7d 30d 365d ...

Questions

■ Questions   ■ Answers

24h 7d 30d 365d ...

Latency distribution

■ in 0ms Current:3408   Max:6280   Min:1332   ■ in 1ms Current:2276   Max:3490   Min:130   ■ in 10ms Current:91   Max:140   Min:35
■ in 100ms Current:100   Max:165   Min:40   ■ in 1s Current:37   Max:171   Min:15   ■ over 1s Current:63   Max:479   Min:23
■ timeouts Current:75   Max:584   Min:27
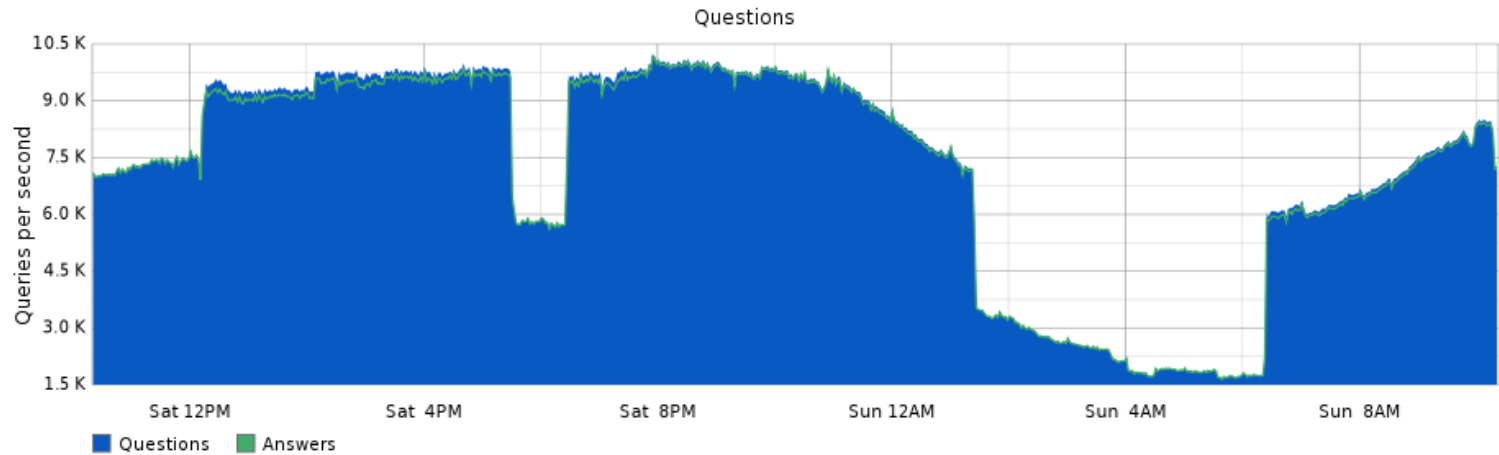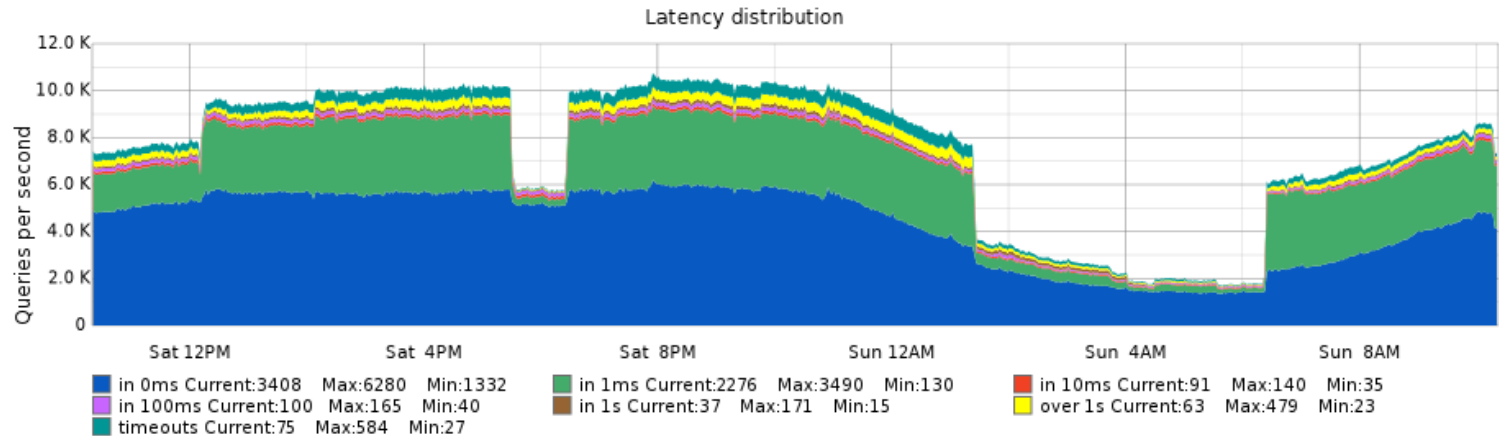
PowerDNS as a responsible netizen: DoS

- DNS is used more and more in a denial of service context
  - Incoming or generating
- Operators (or anyone else) have no **time for this**.
- Our goals are to:
  - Continue providing the intended DNS service
  - Not kill the world with packets
  - Keep our admins asleep at night

POWERDNS

The conflicting challenges in DoS

"Provide 100% answers to legitimate queries"	**"Do not overload third party authoritative servers with queries"**
"Do not flood fake (spoofed) originators of queries with (large) responses"	"Be a low-maintenance fire and forget solution"

Software release/deployment versus botnet timescales

PowerDNS Lua based DoS work

- Instigated by ISP Connect (a Dutch ISP trade group) and SIDN (registry)
  - And funded - thanks!
- PowerDNS did not offer RRL yet, we were asked to implement it
- We have done so, but in consultation, using a more dynamic and general approach
- Many of our users can't quickly deploy new binaries, nor do we want to make them
- Enter - the **Rate Policy Framework**

POWERDNS

PowerDNS Rate Policy Framework

- Full support for RRL as a supplied configuration script
- But not limited to RRL - can measure **and report** any kind of 'rate'
  - And decide policy on it
- Policy can be drop, send to TCP/IP or even return a modified answer
  - that might slow down a botnet for example
- **"offer responsible RRL functionality out of the box, enable dynamic adjustment in the face of new attacks"**

POWERDNS

PowerDNS @ 2014

some notable features

POWERDNS