

ICANN DNS-STATS

Current status and future

Mauricio Vergara Ereche - ICANN DNS Engineering

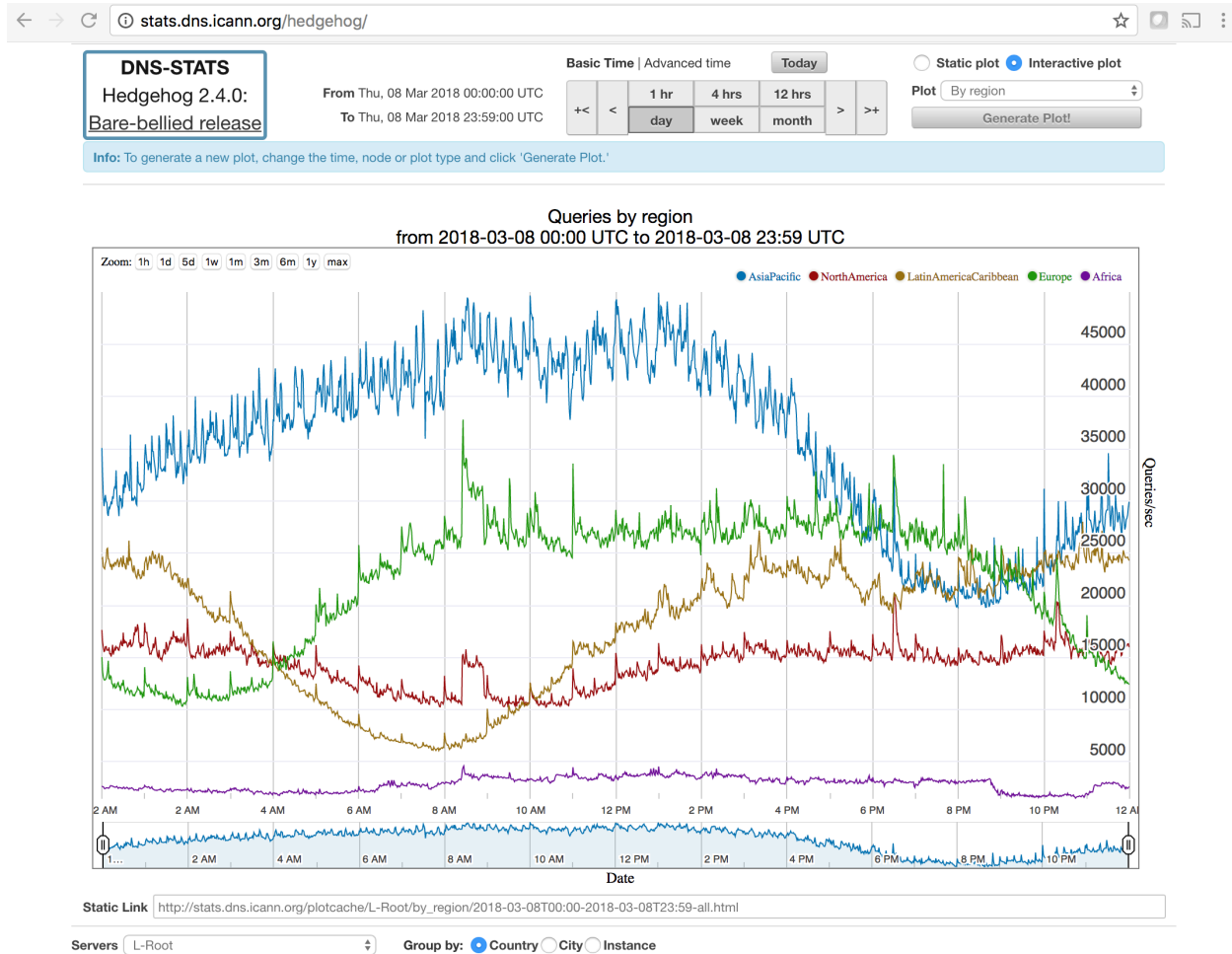
ICANN 61
March 2018



DNS-STATS: A bit of history (part 1)

- DNS-STATS **Presenter** (hedgehog) was originally designed to replace the widely used DSC Presenter
 - Problems scaling Anycast cloud with 100+ nodes
 - Replace files on the DSC Presenter with Postgres DB
 - Developed as an Open Source solution from scratch
 - <http://dns-stats.org>
 - github.com/dns-stats
 - Developed for ICANN by Sinodun IT
 - Currently at version 2.4.0
 - Live version used by ICANN DNS Engineering: <http://stats.dns.icann.org>

DNS-STATS: A bit of history (part 1) - Presenter (Hedgehog)



DNS-STATS: A bit of history (part 2)

- DNS-STATS Compactor was designed to replace DSC Collector
 - Can capture information that the DSC Collector is unable to create statistics on.
 - TCP resets
 - ICMP messages
 - Introduction of C-DNS format (C is for Compacted)
 - C-DNS is an efficient file format to transfer DNS traffic
 - <https://datatracker.ietf.org/doc/draft-ietf-dnsop-dns-capture-format/>
 - IETF current draft on version -06
 - <https://github.com/dns-stats/compactor/wiki>
 - Mozilla Public License v2.0

DNS-STATS Compactor

- DNS-STATS Compactor suite has 2 main programs:
 - **compactor**
 - Similar in usage to `tcpdump`
 - Reads traffic from 1+ interface(s) and outputs *selected* details into C-DNS and PCAP files (ignored, raw)
 - It can also be used to read pre-recorded PCAP files.
 - Can be configured to compress its output (xz or gzip)
 - **inspector**
 - Reconstruct traffic from C-DNS files generated by compactor
 - It outputs one or more PCAP files

DNS-STATS Compactor latest version

- changelog 2018-03-05: **v0.11.0-rc1**
 - Add pseudo-anonymization of output to **inspector**.
 - CBOR - use definite-length items where possible.
 - Small packet receive optimization.
 - Improve detection of malformed EDNS0.
- Just as a reminder:
 - C-DNS uses about 30% of a regular PCAP file

DNS-STATS: Current and future plans

- **DNS-STATS Presenter**

- v3 is currently on development (codename: Wombat)
- Replace PostgreSQL with a cluster of ClickHouse and ZooKeeper
- Use Grafana to plot the data in real time
 - Ability to create your own plots
 - Able to export PCAP files on request.
- Fed with C-DNS files instead of DSC Collector XML files.

- **DNS-STATS Compactor**

- More frequent DITL captures for the ICANN Managed Root-Server
 - Already in conversations with DNS-OARC org.
 - C-DNS format only
- Anonymization schema implementation based on DNS Operations mailing list conversations.
 - General Data Protection Restriction (GDPR) about to enter into effect.

DNS-STATS Presenter - Wombat

