Monitoring DNS with open-source solutions

Felipe Espinoza - Javier Bustos-Jiménez
NIC Chile Research Labs
How is DNS Monitored?

- Pre-Aggregated Data:
  - DNS Statistics Collector (DSC)
    - QTYPE
    -_OPCODE
    - RCODE
    - ...
  - DNS-STATS

- Disaggregated Data:
  - ENTRADA
    - Transfer pcap files
    - Hadoop Cluster for processing
First Try: Develop our own solution

We developed RaTA DNS (Real Time Analysis of DNS packets)

- Capture and reduce information.
- Transfer results over REDIS Queue.
- Show the information on our own presenter.

Were we reinventing the wheel?

Fun fact: dnsadmins didn’t liked it because the visual interface was too much white and clean.
Second Try: Use Open Source Software

- Instead of developing everything, integrate different open source software.
- Many parts of a monitoring system have already been developed.
- Many of them are used in production.
Tested Software

Capture
- PacketBeat
- Collectd
- Fievel
- DSC
- gopassivedns
- DnsZeppelin

Storage
- Prometheus
- Druid
- ClickHouse
- InfluxDB
- ElasticSearch
- OpenTSDB

Visualization
- Kibana
- Grafana
- Graphite
Architecture

- DNS Server
- Capture
- DnsZeppelin
- ClickHouse
- Storage
- Visualization

DnsZeppelin

ClickHouse
Grafana Panel
Grafana Panel
Performance

- Single Server Setup:
  - Packets/Second: ~7,000 pps
  - Time running: 24 Hours
  - Total packet count: ~618,000,000
  - Total uncompressed data: 34 GB
  - Total compressed data: 4.7 GB
  - Compressed packet size: ~8.3 Bytes

- Packet Flood:
  - Packets/Second: 120,000 pps
  - Average Database CPU Usage: 30%
Monitoring DNS with open-source solutions

Source code:
https://github.com/niclabs/dnszeppelin-clickhouse

Felipe Espinoza - fdns@niclabs.cl
Javier Bustos - jbustos@niclabs.cl