Monitoring and measuring name servers

Sebastián Castro Avila

DNS Administrator

NIC Chile

Monitoring tools at .CL

- Why monitoring?
  - Mainly to justify provisioning decisions
    - Bandwidth, CPU, memory
- First approach
  - Build your own tool
- Second approach
  - Modify an existing tool to fit your needs
  - DNSTOP came up in the right moment

Monitoring tools at .CL

- Dnstop
  - DNS online curses-based tool
  - Gives the most queried names (TLD and SLD)
  - Gives the most common source address on queries
- Local modifications
  - Accounting by query type
  - Accounting by TLD
    - Specially useful at ns-ext.nic.cl
      - Secondary name server for .PA, .VE, .BO and several .ARPA zones
  - Accounting by origin network
    - Using two BGP peers (one national, one full)
    - To check bandwidth usage
  - Accounting by “direction”
    - incoming/outcoming traffic.

Monitoring tools at .CL

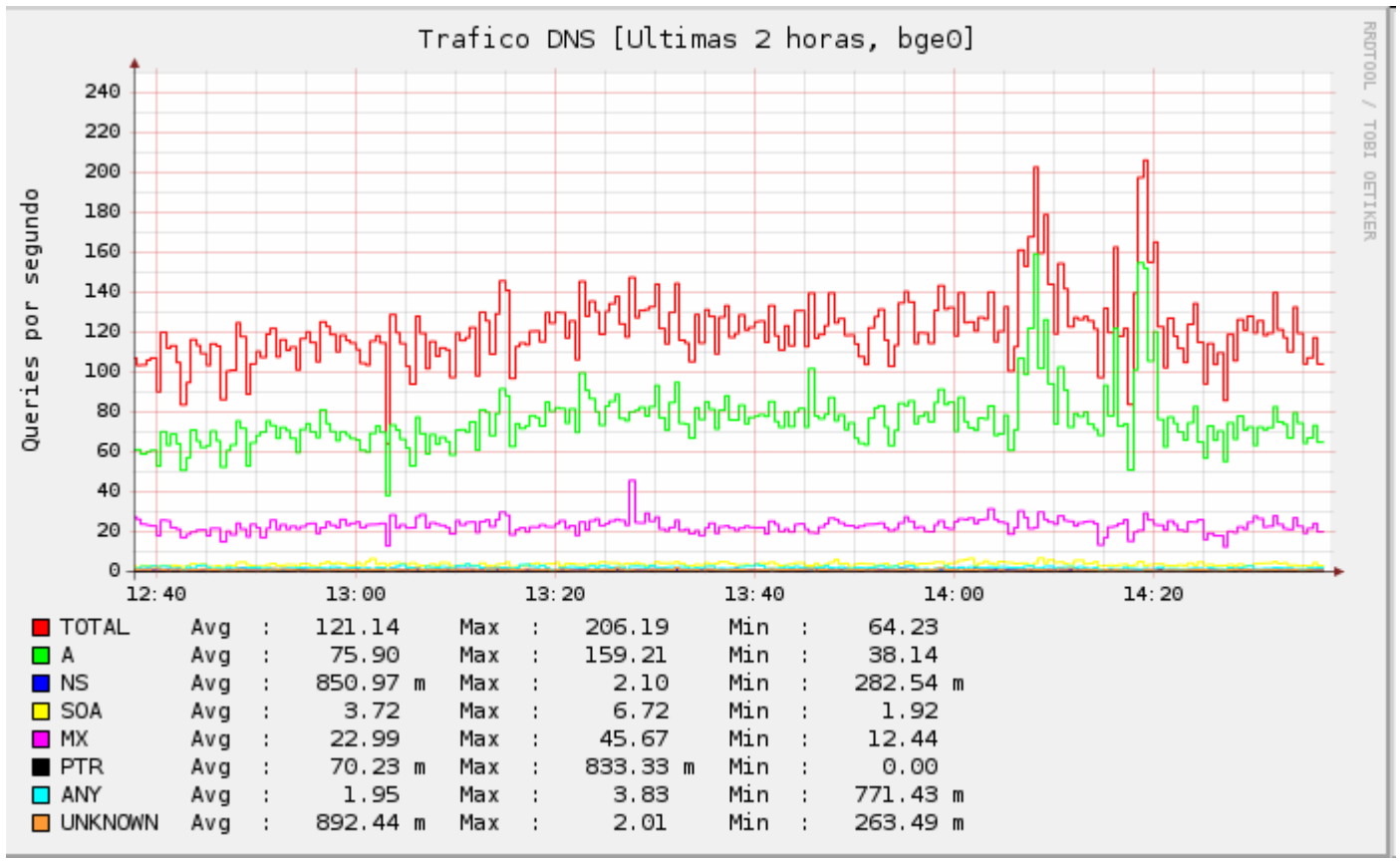
- Usage
  - Running smoothly on FreeBSD and Linux.
  - Regular monitoring: trends, most used server, provisioning planification
  - Trend discovery
    - Has been useful to detect misbehaved ISP resolvers or misconfigured domain names.
  - Anycast checking: correctness and balance

Monitoring tools at .CL

- ToDo List
  - Reduce memory requirements (taking out some code)
  - Count IDN queries
  - Accounting by origin AS
  - Accounting by destination address
  - Other
    - EDNS0 aware resolvers
    - Correctness in queries
    - Accounting on query responses.

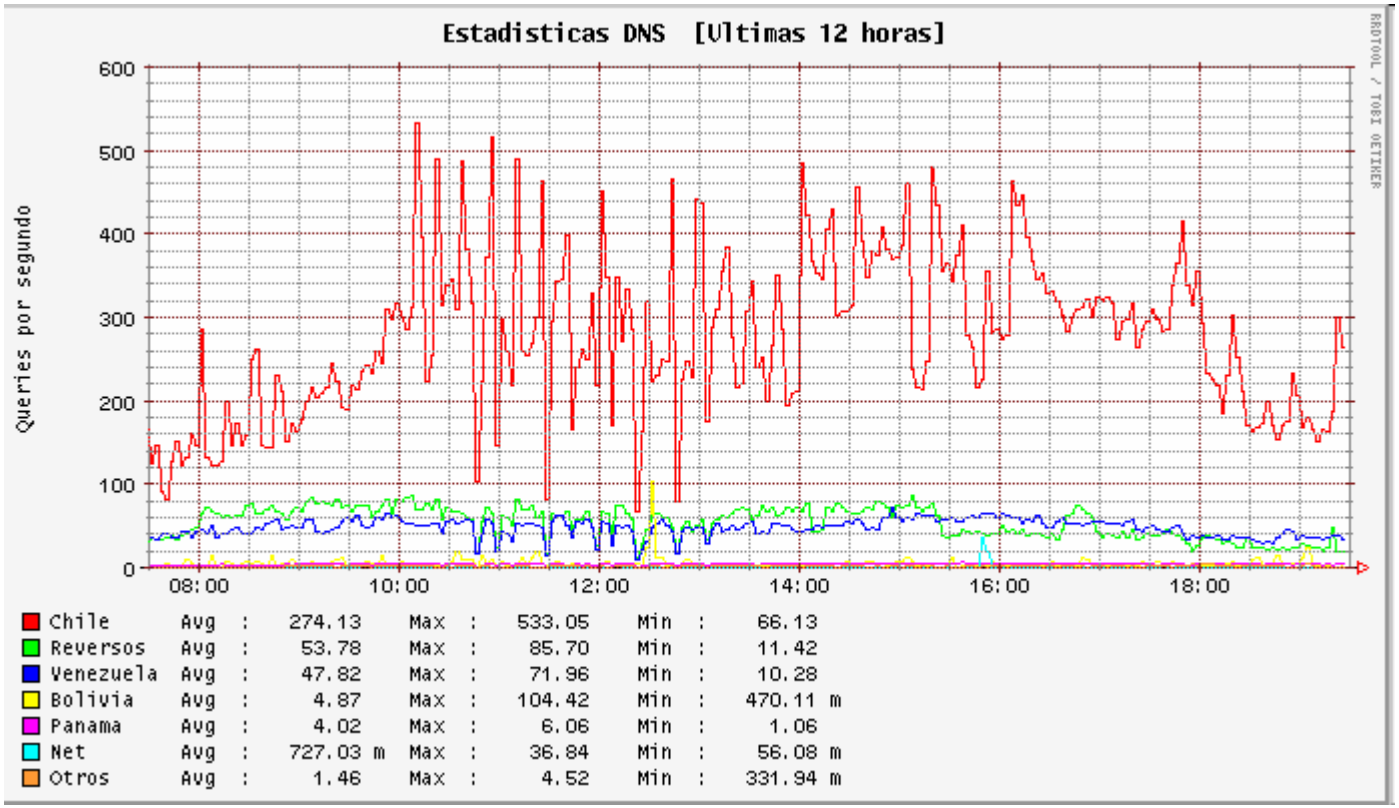
Monitoring tools at .CL

- Snapshots (by query type)



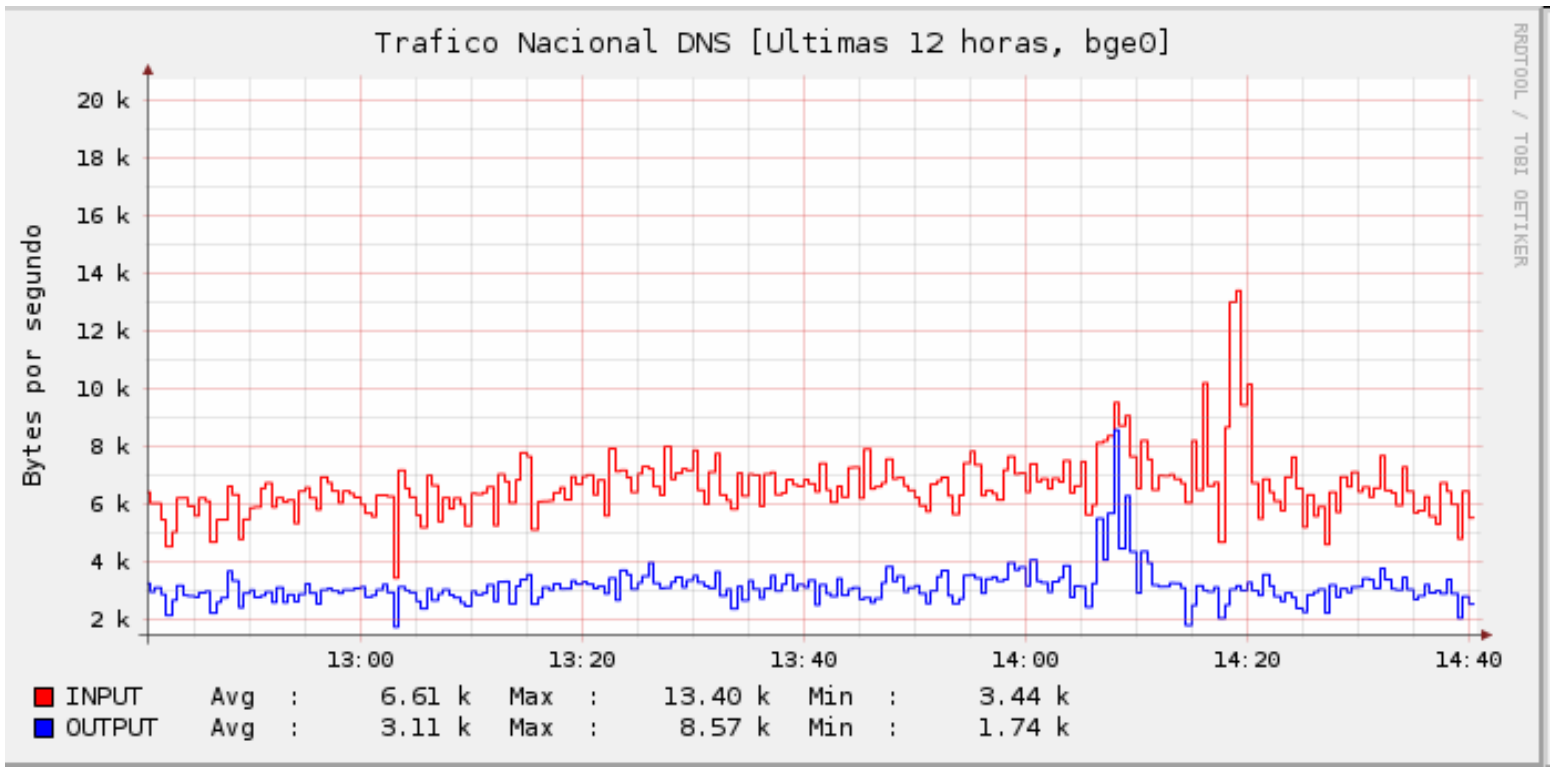
Monitoring tools at .CL

- Snapshots (by TLD)



Monitoring tools at .CL

- Snapshots (by traffic)



Monitoring tools at .CL

- Conclusions
  - DNS monitoring is a “must”
  - This tool has allowed us to detect routing misconfigurations in the national network.
  - Graphically check the behaviour of anycast deployment.
  - Justify bandwidth increases
  - Other tools are recommended: sanity check over secondary name servers (correctness and response time)