DSCng: new incarnation of a popular DNS monitoring tool

CZ.NIC z.s.p.o.

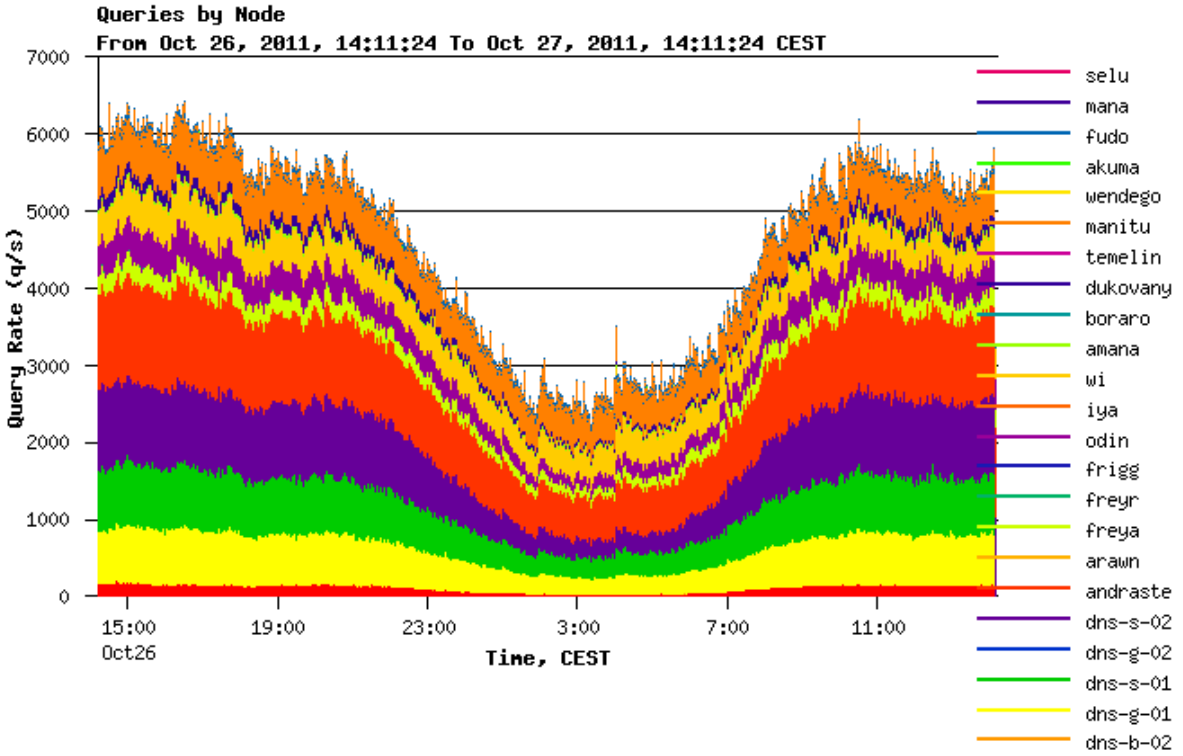
Bedřich Košata / bedrich.kosata@nic.cz

2011-10-29

About DSC

DSC = DNS STATISTICS COLLECTOR

Servers/Nodes
a
b
c
d
f
dnsres
all
› dns-b-01
› dns-b-02
› dns-g-01
› dns-s-01
› dns-g-02
› dns-s-02
› andraste
› arawn
› freya
› freyr
› frigg
› odin
› iya
› wi
› amana
› boraro
› dukovany



The **Queries by Node** plot shows the amount of queries coming from each node in the server cluster. If you would like to see the traffic for a single node, select the node name in the Servers/Nodes menu on the left.

DSC history and legal status

- The Measurement Company
- BSD License
- handed over to DNS-OARC in San Francisco in March 2011

DSC technical overview

- Collector
  - sits on or near the DNS server
  - uses libpcap to capture and analyze traffic
  - once per minute sends aggregated data to the presenter
- Presenter
  - receives data from collector(s)
  - stores parsed data in text files on disk
  - uses HTML + CGI to present the data
  - graphics created on the server as bitmaps

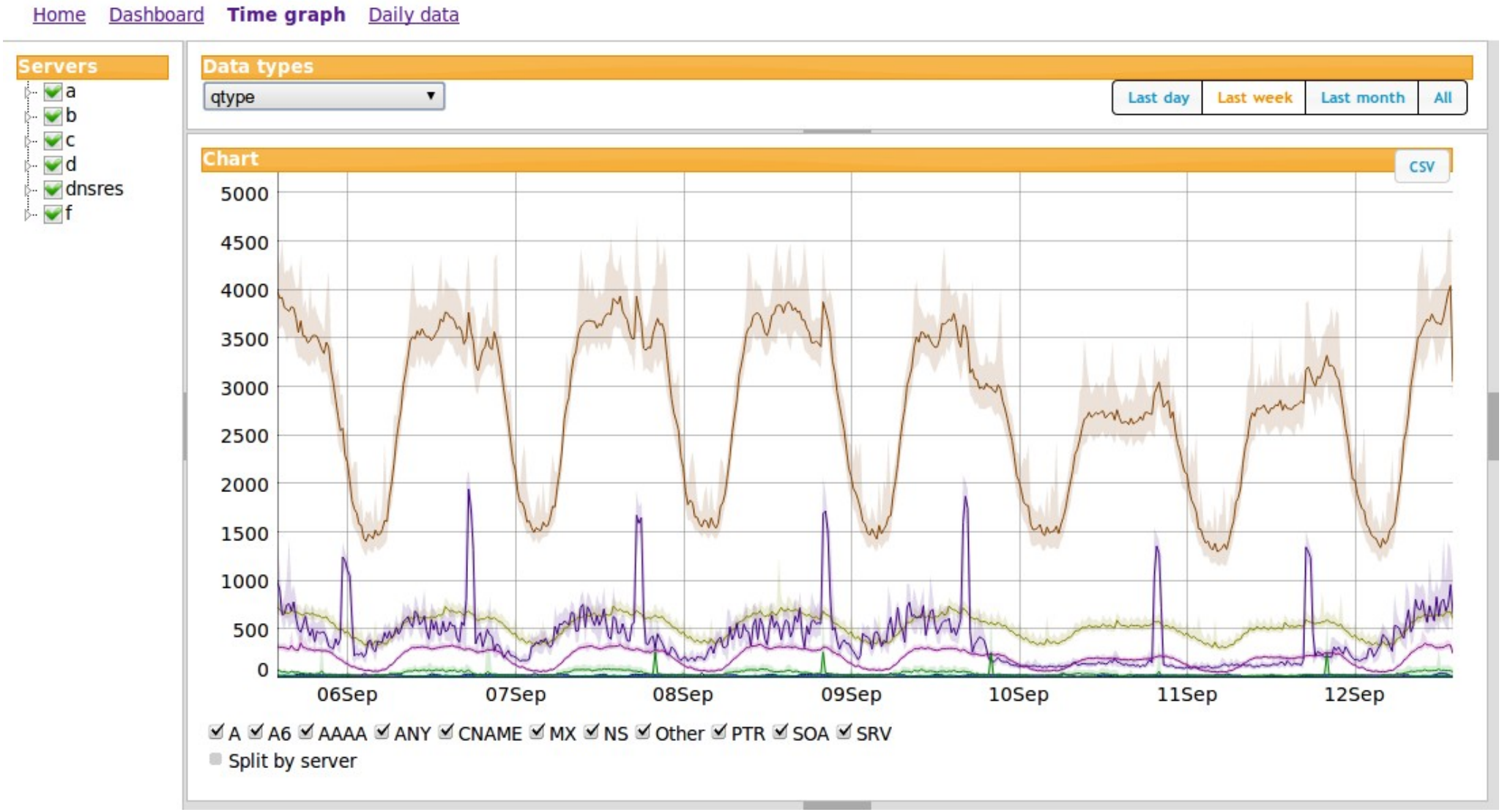
Uplift plan

- Collector – good enough for now
- Presenter
  - Interactive interface
    - HTML5, JavaScript
    - Interactive charts created on client side
    - Combination of charts, analysis tools, etc.
  - Cooperation with other tools
    - e.g. PacketQ for in depth analysis
  - Storage API for retrieval of data
    - custom reports and analysis
  - Other improvements
    - rich authorization model – different view for different users
    - alerts – via email, etc.
    - ...

DSCng presenter technical overview

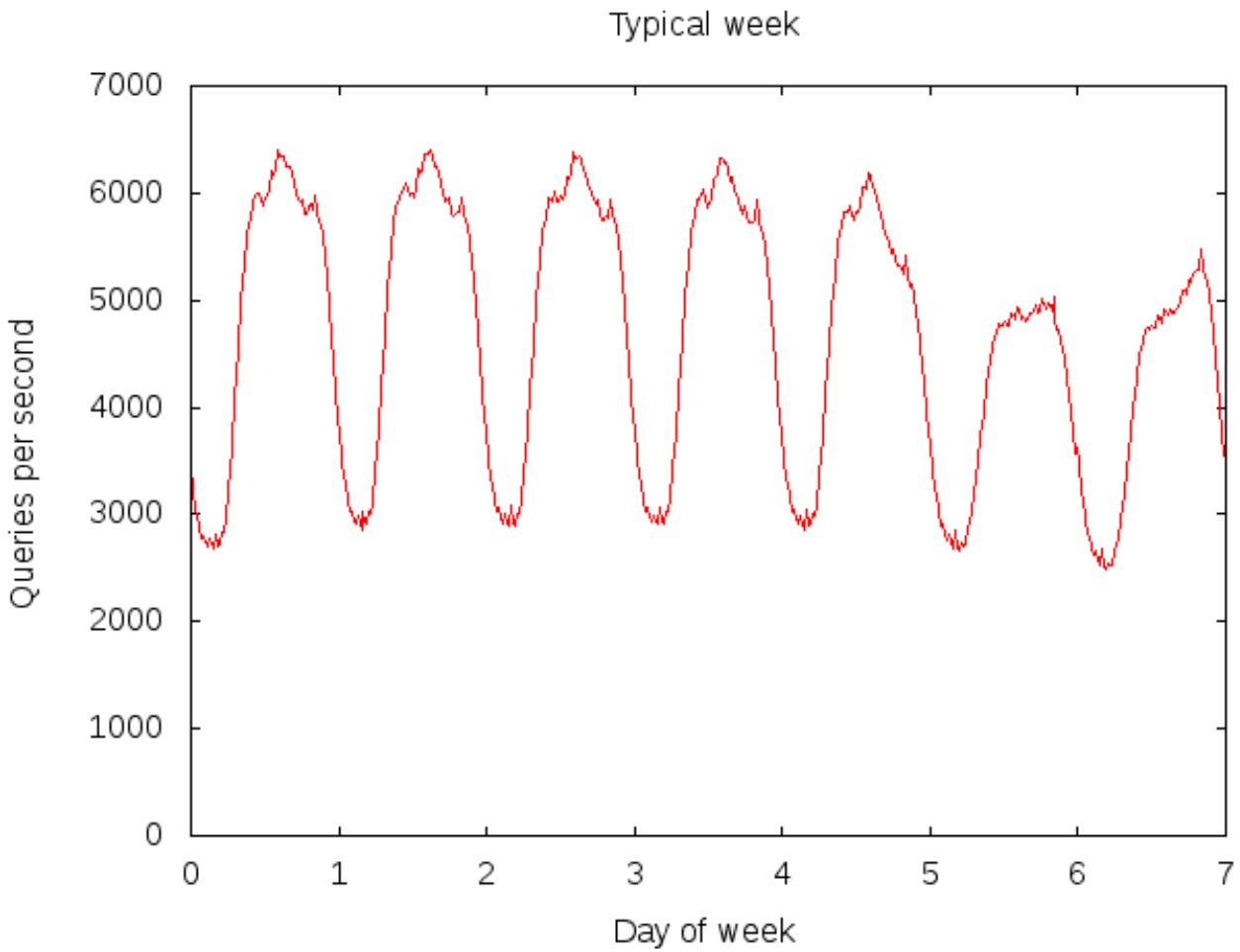
- Storage
  - PostgreSQL
  - Generic storage API as ultimate goal
- Presentation
  - Django (Python web framework)
  - JQuery
  - Dygraphs
  - Google visualization tools

Live demo


Home
Dashboard
Time graph
Daily data
Servers
a
b
c
d
dnsres
f
Data types
qtype
Last day
Last week
Last month
All
Chart
CSV
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
06Sep
07Sep
08Sep
09Sep
10Sep
11Sep
12Sep
A
A6
AAAA
ANY
CNAME
MX
NS
Other
PTR
SOA
SRV
Split by server

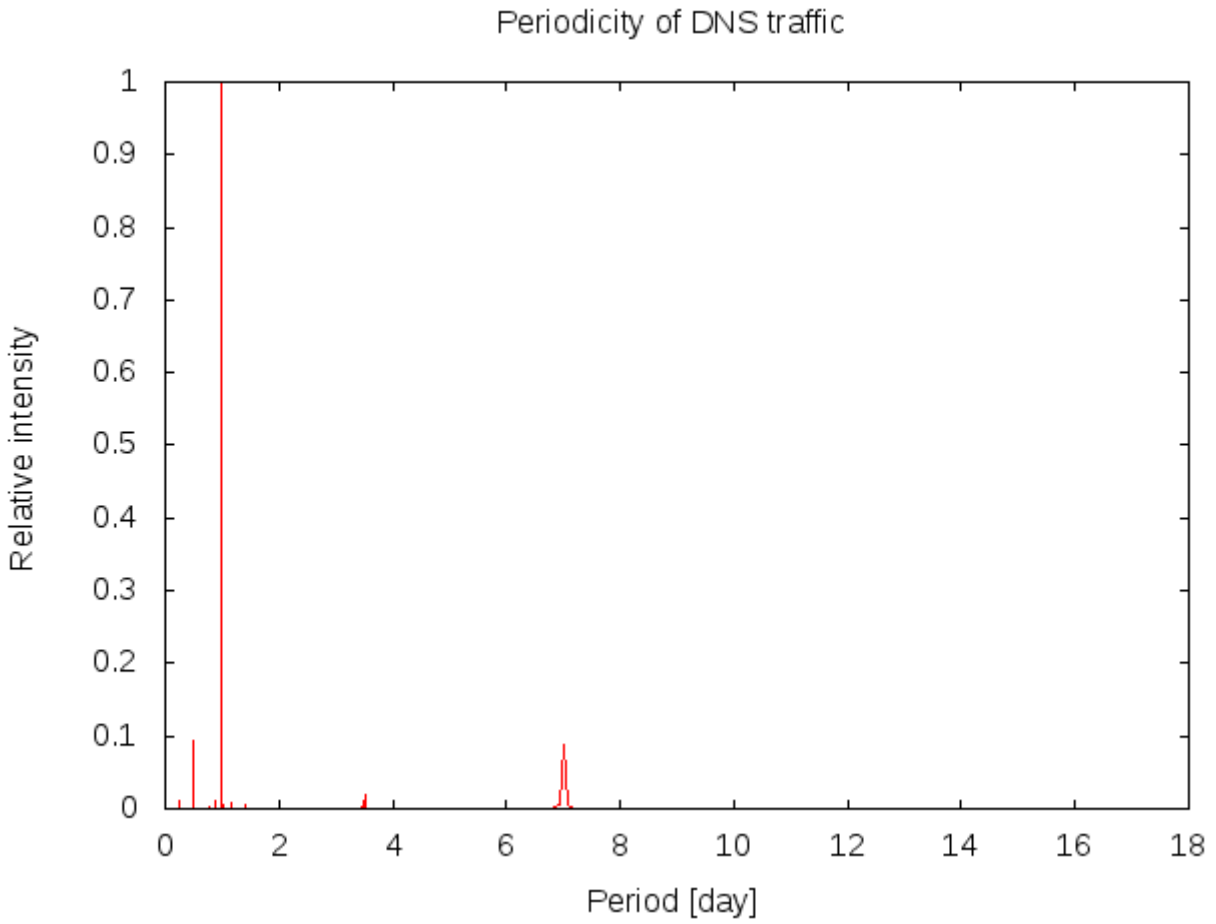
Scripting demo

- small Python script using the DSCng storage API
- Typical week – average values for 1.5 years



Scripting demo

- Periodicity analysis using Fourier transformation of 1.5 years worth of data



Challenges

- Storage of data
  - fast retrieval
  - efficient storage
- Javascript charting
  - many libraries to choose from
  - different advantages and disadvantages in different libraries
  - inconsistent format of data transfer
  - many libraries not maintained anymore

How to participate

- Redmine
  - https://git.nic.cz/redmine/projects/dsc-ng
- GIT
  - git://git.nic.cz/dscng
- Mailing list
  - https://lists.nic.cz/cgi-bin/mailman/listinfo/dscng-dev
- Live demo
  - http://devpub.labs.nic.cz/dscng/

Thank you for your attention