DSCng - moderní systém pro monitorování DNS provozu

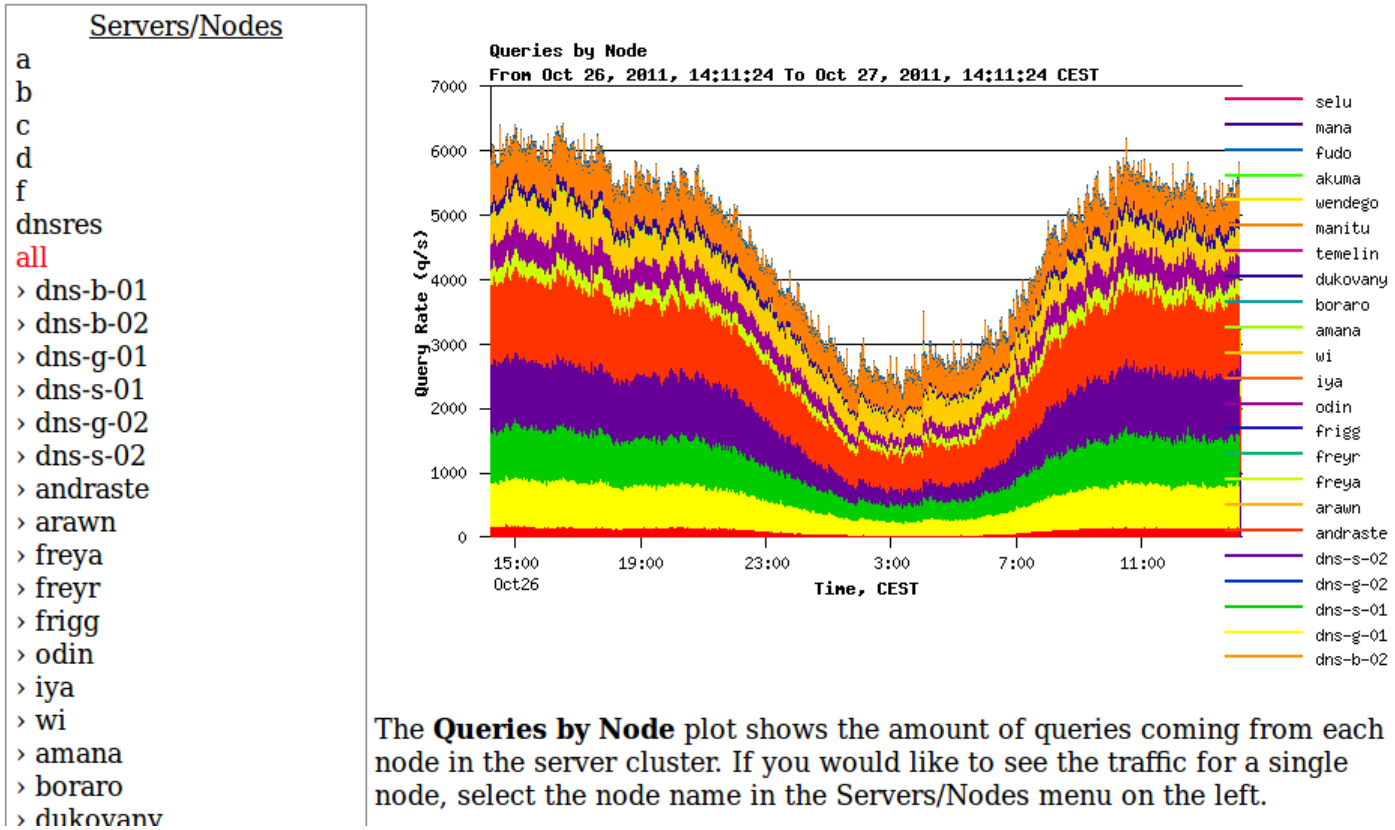
CZ.NIC z.s.p.o.

Bedřich Košata / bedrich.kosata@nic.cz

2012-11-24

Co je DSC

- The Measurement Company
- BSD License
- v březnu 2011 předáno oficiálně DNS-OARC



Jak DSC funguje

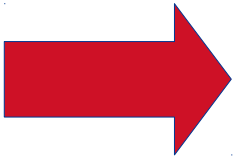
- Sběrač (collector)
  - sedí přímo na a nebo blízko DNS serveru
  - používá libpcap k zachycení a analýze DNS provozu
  - jednou za minutu pošle agregovaná data předvaděči
- Předvaděč (presenter)
  - přijímá data ze sběračů
  - ukládá přechroupaná data na disk v podobě textových souborů
  - pomocí HTML + CGI prezentuje data uživatelům
  - grafika se generuje na serveru v bitmapové podobě

Plán na vylepšení

- Sběrač – v současné době dostačující
- Předvaděč
  - Interaktivní rozhraní
    - HTML5, JavaScript
    - Interaktivní grafy jsou vytvářeny na straně klienta
    - Vylepšení možností analyzovat a srovnávat data
  - Spolupráce s dalšími nástroji
    - např. PacketQ pro detailní analýzu anomálií
  - API pro ukládání a načítání dat
    - možnost generovat vlastní výstupy, analyzovat data v dalších nástrojích, atp.
  - Další možnosti vylepšení
    - upozornění obsluhy na anomálie – emailem, atp.
    - anotace dat - k označení incidentů a dalších významných událostí
    - ...

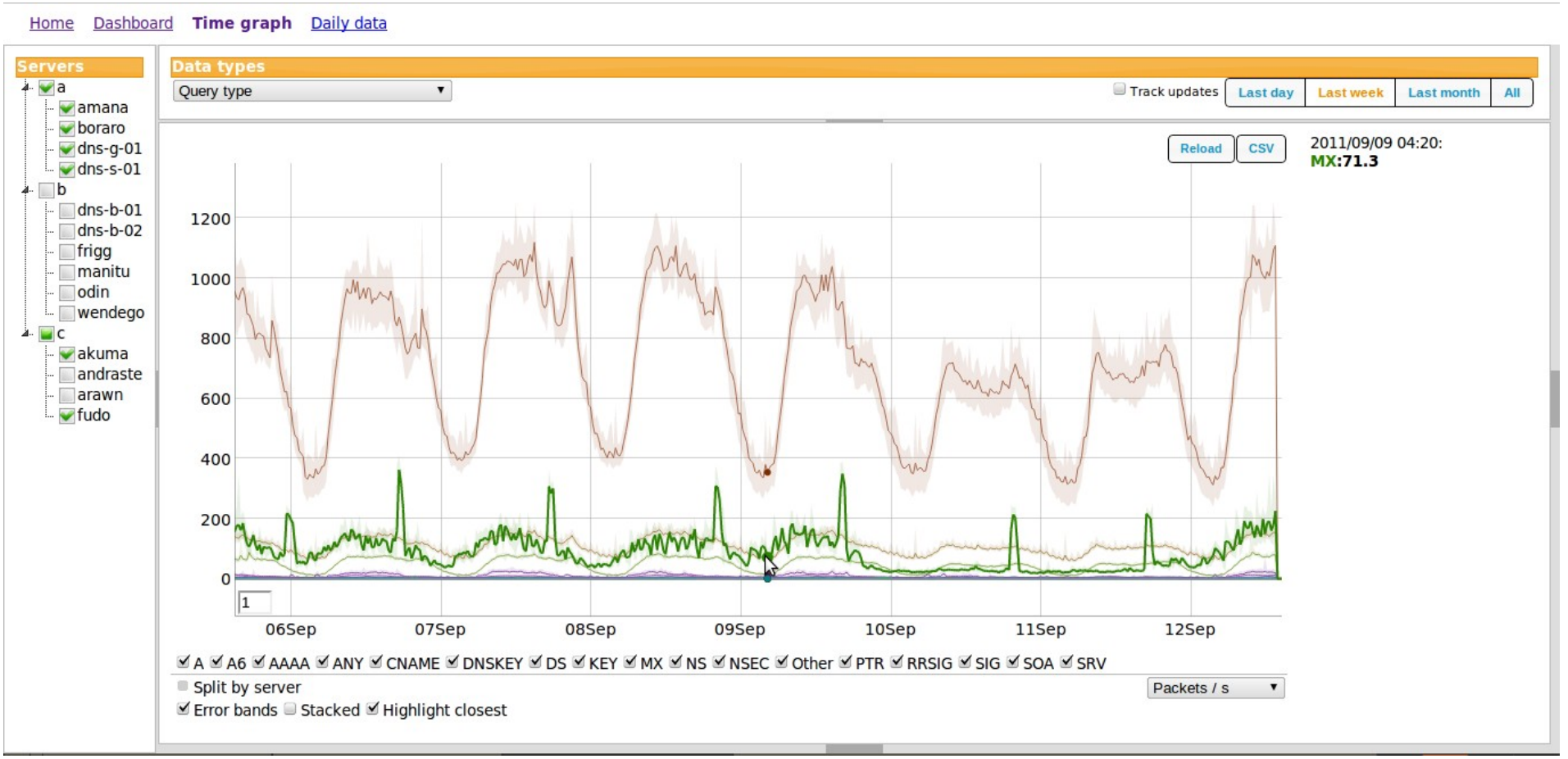
Jak na to?

- Perl
- Textové soubory
- Na serveru generované PNG



- Python + Django
- PostgreSQL
- AJAX a u klienta generované grafy

Živé demo


Home
Dashboard
Time graph
Daily data
Servers
a
amana
boraro
dns-g-01
dns-s-01
b
dns-b-01
dns-b-02
frigg
manitu
odin
wendego
c
akuma
andraste
arawn
fudo
Data types
Query type
Track updates
Last day
Last week
Last month
All
Reload
CSV
2011/09/09 04:20:
MX:71.3
1200
1000
800
600
400
200
0
1
06Sep
07Sep
08Sep
09Sep
10Sep
11Sep
12Sep
A A6 AAAA ANY CNAME DNSKEY DS KEY MX NS NSEC Other PTR RRSIG SIG SOA SRV
Split by server
Packets / s
Error bands
Stacked
Highlight closest

Výzvy při vývoji

- Množství dat
  - Data se generují každou minutu
  - Desítky serverů, desítky statistik => cca 20 GB textových souborů za cca 5 let
  - Interaktivní rozhraní nemůže na data čekat desítky vteřin
  - Klient je schopen vykreslovat jen omezené množství dat (1 rok = 525600 minut/datových bodů)

Výzvy při vývoji

- Řešení
  - předgenerované agregované hodnoty pro časové úseky od 5 minut do 1 dne
    - podle vybraného časového období se zvolí „jemnost“ dat už na úrovni databáze
    - klient dostane vždy cca 1000 datových bodů pro sérii
  - ukládání dat v polích - jedna hodina není v databázi 60 úzkých řádků, ale 1 dlouhý
    - šetří místo (menší data i indexy)
    - zefektivňuje hledání a načítání dat
    - nelze použít Django ORM, je třeba využít low-level SQL

Výzvy při vývoji

- Knihovny pro zobrazení grafů v prohlížeči často
  - nejsou udržovány
  - mají omezenou funkcionalitu
  - nejsou stavěné na větší množství dat
  - nejsou moc pěkné
  - nejsou volně distribuovatelné

    => pro časově závislá data se ukázal nejzajímavější dygraphs (http://dygraphs.com/)

Stav vývoje

- Import datových souborů z původního DSC (včetně inteligentních updatů) - ukládací .dat i transportní .xml soubory
- Interaktivní uživatelské rozhraní
- Vylepšení proti původnímu DSC
  - Podpora pro dlouhá časová období (zobrazuje data za roky stejně snadno jako za hodiny)
  - Neomezená hloubka stromové struktury serverů
  - CSV export právě zobrazovaných dat
  - Manipulace s daty na straně klienta (např. přepínání „normalního“ a stacked zobrazení, vysvícení vybrané série, skrývání sérií, vyhlazování dat, atp.)
  - Dashboard s rychlým náhledem na aktuální provoz

Co chybí a je v plánu

- Ukázkové vydání (plánováno v 1Q 2013)
  - plná kompatibilita s daty ze sběračů, podpora pro paralelní upload dat z mnoha sběračů
  - stabilní databázová struktura – změny budou vždy doprovázeny migračními skripty
  - plná dokumentace instalace a správy
- Autentizace a autorizace uživatelů (2Q 2013)
  - možnost nastavovat různé přístupy pro různé skupiny uživatelů (např. omezení podle typu dat, časového rozmezí zobrazených dat, skupiny serverů, atp.)
- Podpora pro aktivní upozorňování obsluhy
- Statistiky – trendy, anomálie atp.
- Integrace PacketQ

Kde najít informace

- 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
- Živé demo
  - http://devpub.labs.nic.cz/dscng/

Díky za pozornost