OpenINTEL

an infrastructure for long-term, large-scale and high-performance active DNS measurements

UNIVERSITY OF TWENTE.

DACS
Design and Analysis of Communication Systems

SIDN labs

SURFNET
Why measure DNS?

• (Almost) every networked service relies on DNS

• DNS translates human readable names into machine readable information
  
  • e.g. IP addresses, but also: mail hosts, certificate information, …

• Measuring what is in the DNS over time provides information about the evolution of the Internet

• (we started this because we were interested in the rise of DDoS Protection Services)
Goals and Challenges

• Send a comprehensive set of DNS queries for every name in a TLD, once per day

• But can we do this at scale? How does this impact the global DNS?

  .com + .net + .org ≈ over 150 million names (about 50% of the global DNS namespace)

• How do we store and analyse this data efficiently?
Data collection stages

- We distinguish **three stages** for data collection:
  - **Stage 1:** Collection of zone files for TLDs to scan, compute daily deltas
  - **Stage 2:** Main measurement, perform queries for each names, collect meta data, store results
  - **Stage 3:** Prepare data for analysis
High-level architecture

Stage I
- collection server
- database per TLD
- TLD zone repositories

Stage II
- cluster manager per TLD
- metadata server
- Worker cloud per TLD

Stage III
- aggregation server
- NAS for long term storage
- Hadoop cluster
- Internet
What do we query and store?

- We ask for:
  - SOA
  - A, AAAA
    - (apex, ‘www’ and ‘mail’)
  - NS
  - MX
  - TXT
  - SPF
  - DS
  - DNSKEY
  - NSEC(3)

- We store:
  - All records in the answer section
  - CNAME expansions
  - DNSSEC signatures (RRSIG)
  - Metadata (Geo IP, AS)
Impact on the global DNS

- Our measurement is clearly visible in SURFnet’s traffic flows
Impact on the global DNS

- Deeper analysis shows very few top talkers (less than 35 receive more than 100 packets/sec.)
Big data? Yes!

• Calling your research “big data” is all the rage

• So would our work qualify as big data?

• The **human genome** is about $3 \cdot 10^9$ base pairs

• We collect around $1.8 \cdot 10^9$ DNS records **per day**

• Since February 2015, through December 31st we collected $511 \cdot 10^9$ (**511 billion**) results
Some numbers

- Workers: 1 CPU core, 2GB RAM, 5 GB disk

<table>
<thead>
<tr>
<th>TLD</th>
<th>#domains</th>
<th>workers</th>
<th>measure time</th>
</tr>
</thead>
<tbody>
<tr>
<td>.org</td>
<td>10.9M</td>
<td>10</td>
<td>7h19m</td>
</tr>
<tr>
<td>.net</td>
<td>15.6M</td>
<td>10</td>
<td>14h29m</td>
</tr>
<tr>
<td>.com</td>
<td>123.1M</td>
<td>80</td>
<td>17h10m</td>
</tr>
<tr>
<td>.nl</td>
<td>5.6M</td>
<td>3</td>
<td>3h09m</td>
</tr>
</tbody>
</table>

- Data collected daily:

<table>
<thead>
<tr>
<th>TLD</th>
<th>#domains</th>
<th>(failed)</th>
<th>#results</th>
<th>Avro</th>
<th>Parquet</th>
<th>uncompressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>.org</td>
<td>10.9M</td>
<td>(1.2%)</td>
<td>125M</td>
<td>2.6GB</td>
<td>3.2GB</td>
<td>18.5GB</td>
</tr>
<tr>
<td>.net</td>
<td>15.6M</td>
<td>(0.9%)</td>
<td>166M</td>
<td>3.5GB</td>
<td>4.3GB</td>
<td>24.4GB</td>
</tr>
<tr>
<td>.com</td>
<td>124.0M</td>
<td>(0.6%)</td>
<td>1419M</td>
<td>30.0GB</td>
<td>36.8GB</td>
<td>213.4GB</td>
</tr>
<tr>
<td>.nl</td>
<td>5.6M</td>
<td>(0.5%)</td>
<td>112M</td>
<td>8.5GB</td>
<td>11.8GB</td>
<td>27.8GB</td>
</tr>
<tr>
<td>total</td>
<td>156.1M</td>
<td>(0.6%)</td>
<td>1.8B</td>
<td>43.3GB</td>
<td>54.7GB</td>
<td>284.1GB</td>
</tr>
</tbody>
</table>

- We collect almost **16TB** of **compressed** data per year
Big data? Use the right tools

• With 3 partners invested in a Hadoop cluster (SURFnet, SIDN, UTwente)

• Use latest & greatest tools for analysis, **Impala, Spark, Flume, ...**

• Working on making datasets accessible to other network researchers
Query performance

- Example query: top 10 countries A records geo-locate to in the .com TLD

- Storage format matters a lot!

<table>
<thead>
<tr>
<th>Storage format (row oriented)</th>
<th>Compression</th>
<th>Relative size</th>
<th>Query run-time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avro</strong></td>
<td>none</td>
<td>100%</td>
<td>25.1s</td>
</tr>
<tr>
<td></td>
<td>deflate</td>
<td>17%</td>
<td>15.5s</td>
</tr>
<tr>
<td></td>
<td>snappy</td>
<td>23%</td>
<td>9.3s</td>
</tr>
<tr>
<td><strong>Parquet</strong> (columnar)</td>
<td>none</td>
<td>44%</td>
<td>17.5s</td>
</tr>
<tr>
<td></td>
<td>gzip</td>
<td>10%</td>
<td>5.7s</td>
</tr>
<tr>
<td></td>
<td>snappy</td>
<td>17%</td>
<td>4.3s</td>
</tr>
</tbody>
</table>

Sweet spot!
An example: cloud e-mail

• Google largest (4.57M)
• But Microsoft grows much faster!
• Yahoo in decline

• SPF protects against e-mail forgery
• Microsoft users show (near) ubiquitous SPF use
• Google users at only one third
Data access

• Working on ways to make this resource accessible to the measurement research community

• Problem: contracts for zone file access (com/net/org/nl/…) are (very) restrictive

• Current thinking:
  • Publishing aggregate data sets is OK
  • “Toy” cluster with open data (e.g. Alexa 1M) to allow others to write queries & scripts, then execute “on behalf”
  • Anonymisation of data?
Thank you for your attention!

Questions?
(come see us for a live demo)

nl.linkedin.com/in/rolandvanrijswijk
nl.linkedin.com/in/mattijssj
@reseauxsansfil
r.m.vanrijswijk@utwente.nl
m.jonker@utwente.nl

UNIVERSITY OF TWENTE.