DNSql
Processing Massive DNS Collections

Stephen Herwig, Dave Levin, Bobby Bhattacharjee, Neil Spring

University of Maryland, College Park
D-root

Operated by UMD

Anycast with 109 replicas

Hourly sampled collection by replica
Problem

Lots of data

~140 GiB / day

Serial processing is slow

~8h to read a month’s worth of collection for CPMD replica

Diverse analyses

Short-term, Long-Term

Aggregation by source, replica, geography, topology
Approach

CREATE TABLE queryresp (
    id INTEGER PRIMARY KEY,
    sec INTEGER,
    usec INTEGER,
    src BLOB,
    sport INTEGER,
    opcode INTEGER,
    qclass INTEGER,
    qtype INTEGER,
    rcode INTEGER,
    qname TEXT
);
CREATE INDEX qname_index ON queryresp(qname);
CREATE INDEX src_index ON queryresp(src);
CREATE TABLE qps (sec INTEGER, n INTEGER);

MapReduce
Processing Speed

CPMD March 2015

- zcat | tcpdump
- dnsqbsite3c
- aggregate.db
- parallel dnsqbsite3c

resp (K) / sec

- single pcap.gz
- month of pcap.gzs
Database Size

CPMD March 2015

- month of pcaps
- month of SQLite3 shards
- aggregate.db

GiB

0 250 500 750 1000 1250 1500 1750

normal
gzip'd
Query Speed

CPMD March 2015

- aggregate.db
- mapreduce

<table>
<thead>
<tr>
<th>QPS</th>
<th>distinct source IPs</th>
<th>source IP frequency</th>
<th>count distinct hashed qnames</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
Additional Data Sources

Percent of Queries to CPMD By Country (March 2015)

MaxMind GeoLite database
7m query time
Per-Source Query Per Minute (QPM) mean vs stddev for CPMD March 2015

466,021 unique sources
1h 10m query time
Discussion

Additional queries?

Optimizations?

Extension to non-root servers?