Serverless DNS Analytics using ENTRADA 2.0

Maarten Wullink | DNS-OARC31
Austin TX 1 Nov 2019
Challenges

- Previous versions of ENTRADA require Hadoop and you would need:
  • Invest more effort to install and maintain
  • Hadoop knowledge
  • Hardware or virtual Hadoop cluster
ENTRADA 2.0

New features:

• Serverless DNS analytics
• Support for multiple SQL query engines
• Quality of service monitoring, round-trip time (RTT) analysis
• Easy deployment using Docker
Serverless DNS analytics

• No need to deploy any servers
• No hardware/network maintenance cost
• Only pay for amount of data analyzed

ENTRADA will:

• Create database schema
• Convert, upload and optimize data
• **Serverless DNS analytics**

  Support for Amazon Web Services (AWS)
  
  • S3 storage
  
  • Athena SQL-query engine
  
  • Pricing: $5 per TB of scanned data
Quality of service monitoring

Uses passive DNS-data from real world DNS-clients (not probes) to determine Round Trip Time (RTT) between a resolver and the authoritative name server.

High RTT can be caused by:

• Inefficient routing
• Congestion
• Router/switch issues
Quality of service monitoring

Analyze the TCP-handshake

For an average day, TCP use:

- 4-5% of queries
- 22-26% of resolvers

dif(SYN ACK – ACK) = RTT
## High latency ASNs

<table>
<thead>
<tr>
<th>asn</th>
<th>Avg RTT</th>
<th>Samples</th>
<th>Operator</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>45090</td>
<td>1147</td>
<td>3130</td>
<td>Shenzhen Tencent Computer Systems Company Limited</td>
<td>CN</td>
</tr>
<tr>
<td>34205</td>
<td>436</td>
<td>716</td>
<td>PJSC Rostelecom</td>
<td>RU</td>
</tr>
<tr>
<td>24361</td>
<td>357</td>
<td>2326</td>
<td>CERNET2 IX at Southeast University</td>
<td>CN</td>
</tr>
<tr>
<td>4538</td>
<td>298</td>
<td>6256</td>
<td>China Education and Research Network Center</td>
<td>CN</td>
</tr>
<tr>
<td>56044</td>
<td>298</td>
<td>4721</td>
<td>China Mobile communications corporation</td>
<td>CN</td>
</tr>
<tr>
<td>132525</td>
<td>287</td>
<td>1733</td>
<td>HeiLongJiang Mobile Communication Company Limited</td>
<td>CN</td>
</tr>
<tr>
<td>1221</td>
<td>282</td>
<td>4478</td>
<td>Telstra Corporation Limited</td>
<td>AU</td>
</tr>
<tr>
<td>56042</td>
<td>280</td>
<td>738</td>
<td>China Mobile communications corporation</td>
<td>CN</td>
</tr>
<tr>
<td>24444</td>
<td>274</td>
<td>6361</td>
<td>Shandong Mobile Communication Company Limited</td>
<td>CN</td>
</tr>
</tbody>
</table>
Quality of service monitor
Q&A

www.sidnlabs.nl | stats.sidnlabs.nl