.nl ENTRADA

CENTR-tech 33
November 2015
Marco Davids, SIDN Labs
SIDN

- Registry for .nl ccTLD
- ~ 5,6 million domain names
- ~ 2,45 million domain names secured with DNSSEC
- SIDN Labs is the R&D team
ENTRADA
ENhanced Top-Level Domain Resilience through Advanced Data Analysis

- > 300 GB of PCAP data daily
- > 1.3 billion query's daily
- > 3.1 million distinct resolvers
- Currently capturing some 10% of total
Requirements

- SQL support
- Scalability / Extensibility
- Stability / High performance
- Capacity for >1 year of DNS data
- Reasonable budget
Query Engine Options

Evaluated SQL and NoSQL solutions

- Relational SQL (PostgreSQL)
- MongoDB
- Cassandra
- Elasticsearch
- Hadoop (HBASE + Apache Phoenix or Hive)
- SQL on Hadoop (HDFS + Impala + Parquet)
SQL on Hadoop

Best fit for our requirements

- Hadoop Node N
  - IMPALA
  - PARQUET
- Hadoop Node N+1
  - IMPALA
  - PARQUET
- Hadoop Node N+2
  - IMPALA
  - PARQUET

HDFS

Eerste bullet niveau

Tweede bullet niveau

• SQL on Hadoop
  - Best fit for our requirements

• Hadoop Node N
  - IMPALA
  - PARQUET
  - HDFS

• Hadoop Node N+1
  - IMPALA
  - PARQUET
  - HDFS

• Hadoop Node N+2
  - IMPALA
  - PARQUET
  - HDFS
HDFS

- Distributed file system for storing large volumes of data
- High availability through replication of data blocks
- Scalable to hundreds of PB’s and thousands of servers

HDFS Data Distribution

Input File

Node A

Node B

Node C

Node D

Node E
Apache Parquet

- Why not just use the PCAP files?
  - Reading (compressed) PCAP data is just too slow
  - Analytical engines cannot read PCAP files

- Columnar storage format

<table>
<thead>
<tr>
<th>data</th>
<th>row oriented</th>
<th>column oriented</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A1 B1 C1</td>
<td>A1 A2 A3</td>
</tr>
<tr>
<td>A1</td>
<td>B1 C1</td>
<td>B1 B2 B3</td>
</tr>
<tr>
<td>A2</td>
<td>B2 C2</td>
<td>C1 C2 C3</td>
</tr>
<tr>
<td>A3</td>
<td>B3 C3</td>
<td>C1 C2 C3</td>
</tr>
</tbody>
</table>
Apache Parquet (2)

- Columnar storage allows for efficient encoding/compression
  - multiple encoding schemes
  - support for Snappy compression

- Partition data (e.g. by year, month, day and server)
  - Partition pruning allows Impala to skip data we are not interested in

- Other analytical engines, like Apache Spark can use the same Parquet data
Impala query engine

- **MPP** (massively parallel processing)
- Inspired by Google Dremel paper
- Provides low latency and high concurrency for BI/analytic queries on Hadoop
- Excellent performance when compared to other Hadoop based query engines
Impala (2)

Data formats
• Text
• Hadoop formats
• Apache Avro
• Apache Parquet

Interfaces
• Web-based GUI
• Command line (impala-shell)
• Python (Impyla)
• JDBC
ENTRADA Architecture

• ‘DNS big data’ system

• **Goal:** develop applications and services that further enhance the security and stability of .nl, the DNS, and the Internet at large

• ENTRADA main components:
  • Applications and services
  • Platform
  • Data sources
  • Privacy framework
Privacy

Policy elements:
• Purpose
• Data that is used
• Filters on the data
• Retention period
• Access to the data
• Type of application (Research vs. Prod.)

Download paper: https://goo.gl/wec5dR
Workflow

name server → PCAP staging → PCAP decode

- Join
- Filter
- Enrich
- Import

Monitoring

Hadoop
- Impala
- Parquet

Analyst

Query data available for analysis within 10 minutes
Cluster Design
nano sized

location I
management node

<table>
<thead>
<tr>
<th>2Gb/s network</th>
</tr>
</thead>
</table>

location II
data nodes

location III
data nodes
Hardware

Management node
HP ProLiant DL380
Xeon 1.9 GHz 12 core CPU
64GB RAM
3 TB storage

Data node
HP ProLiant DL380
Xeon 1.9 GHz 12 core CPU
64GB RAM
6 TB storage

Scaling
- Vertical by adding more resources
- Horizontal by adding more data nodes
Performance

Example query, count # IPv4 queries/day.

```sql
select
cast(concat_ws('-'; day, month, year) as int), count(1)
from dns.queries
where ipv=4
group by
cast(concat_ws('-'; day, month, year) as int)
```

Query response-times

1 Year of data is 2.2TB Parquet ~ 52TB of PCAP
## Status

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name server feeds</td>
<td>2</td>
</tr>
<tr>
<td>Queries per day</td>
<td>~150M</td>
</tr>
<tr>
<td>Daily PCAP volume (gzipped)</td>
<td>~33GB</td>
</tr>
<tr>
<td>Daily Parquet volume</td>
<td>~6GB</td>
</tr>
<tr>
<td>Months operational</td>
<td>18</td>
</tr>
<tr>
<td>Total # queries stored</td>
<td>&gt; 71B</td>
</tr>
<tr>
<td>Total Parquet volume</td>
<td>&gt; 3TB</td>
</tr>
<tr>
<td>HDFS (3x replication)</td>
<td>&gt; 9TB</td>
</tr>
<tr>
<td>Cluster capacity</td>
<td>~150B-200B tuples</td>
</tr>
</tbody>
</table>
Use Cases

Focussed on increasing the security and stability of .nl

- Visualize DNS patterns (visualize traffic patterns for phishing)
- Detect botnet infections
- Real-time Phishing detection
- Statistics (stats.sidnlabs.nl)
- Scientific research (collaboration with Dutch universities)
- Operational support for DNS operators
Example Applications

- DNS security scoreboard
- Resolver reputation
DNS Security Scoreboard

**Goal:** Visualize DNS patterns for malicious activity.

**How:** Combine external phishing feeds with DNS data.
Architecture

Security feed I

Security feed II

Event Analyzer

ewn event
=enrich with DNS data
=save enriched event

Hadoop

PostgreSQL

REST API

Web UI

retrieve event data
Traffic Visualization

Overview

Network

<table>
<thead>
<tr>
<th>Top 10 event</th>
<th>#</th>
<th>ASN</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS15169</td>
<td>55</td>
<td>AS15169</td>
<td>10</td>
</tr>
<tr>
<td>AS2990590</td>
<td>38</td>
<td>AS97717</td>
<td>3</td>
</tr>
<tr>
<td>AS202109</td>
<td>22</td>
<td>AS31334</td>
<td>2</td>
</tr>
<tr>
<td>AS12322</td>
<td>19</td>
<td>AS35952</td>
<td>1</td>
</tr>
<tr>
<td>AS2002018</td>
<td>18</td>
<td>AS7819</td>
<td>1</td>
</tr>
<tr>
<td>AS40260</td>
<td>10</td>
<td>AS7888</td>
<td>1</td>
</tr>
<tr>
<td>AS48539</td>
<td>9</td>
<td>LINKN</td>
<td>1</td>
</tr>
<tr>
<td>AS16909</td>
<td>9</td>
<td>AS66039</td>
<td>1</td>
</tr>
</tbody>
</table>

Location

Unique # ASN
Resolver Reputation (ResRep)

Goal:
Try to detect malicious activity by assigning reputation scores to resolvers.

How:
“Fingerprinting” resolver behaviour.
ResRep Concept

Malicious activity:
- Spam-runs
- Botnets like Cutwail
- DNS-amplification attacks
1. Verwijder de bestaande foto en klik op het icoon, om een foto in te voegen:
2. Zoek de gewenste foto en dubbelklik hierop.
3. Staat de aarde ding er niet goed in?
   Selecteer de foto, klik 'Format' in het lint en selecteer 'Crop'.
4. De aarde ding is nu te verschuiven, door met een linkermuisklik vast te houden op de aarde ding en de muis naar de gewenste richting te bewegen.
Open Data program

https://stats.sidnlabs.nl
Open Data program (JSON files)

https://stats.sidnlabs.nl
Conclusions

Technical:

• Hadoop HDFS + Parquet + Impala is a winning combination!

Contributions:

• Research by SIDN Labs and universities.
• Identified malicious domain names and botnets.
• External data feed to the Abuse Information Exchange.
• Insight into DNS query data.
Future Work

- Combine data from .nl authoritative name server with scans of the complete .nl zone and ISP data.
- Get data from more name servers and resolvers.
- Expand Open Data program.
Please let us know

• Is, or can our aggregated open data (be) useful?
• For whom?
• What can we do to improve things?
Questions and Feedback

Marco Davids
Senior Research Engineer
marco.davids@sidn.nl
@marcodavids

www.sidnlabs.nl