



Your world. Our domain.

# DNS Big Data

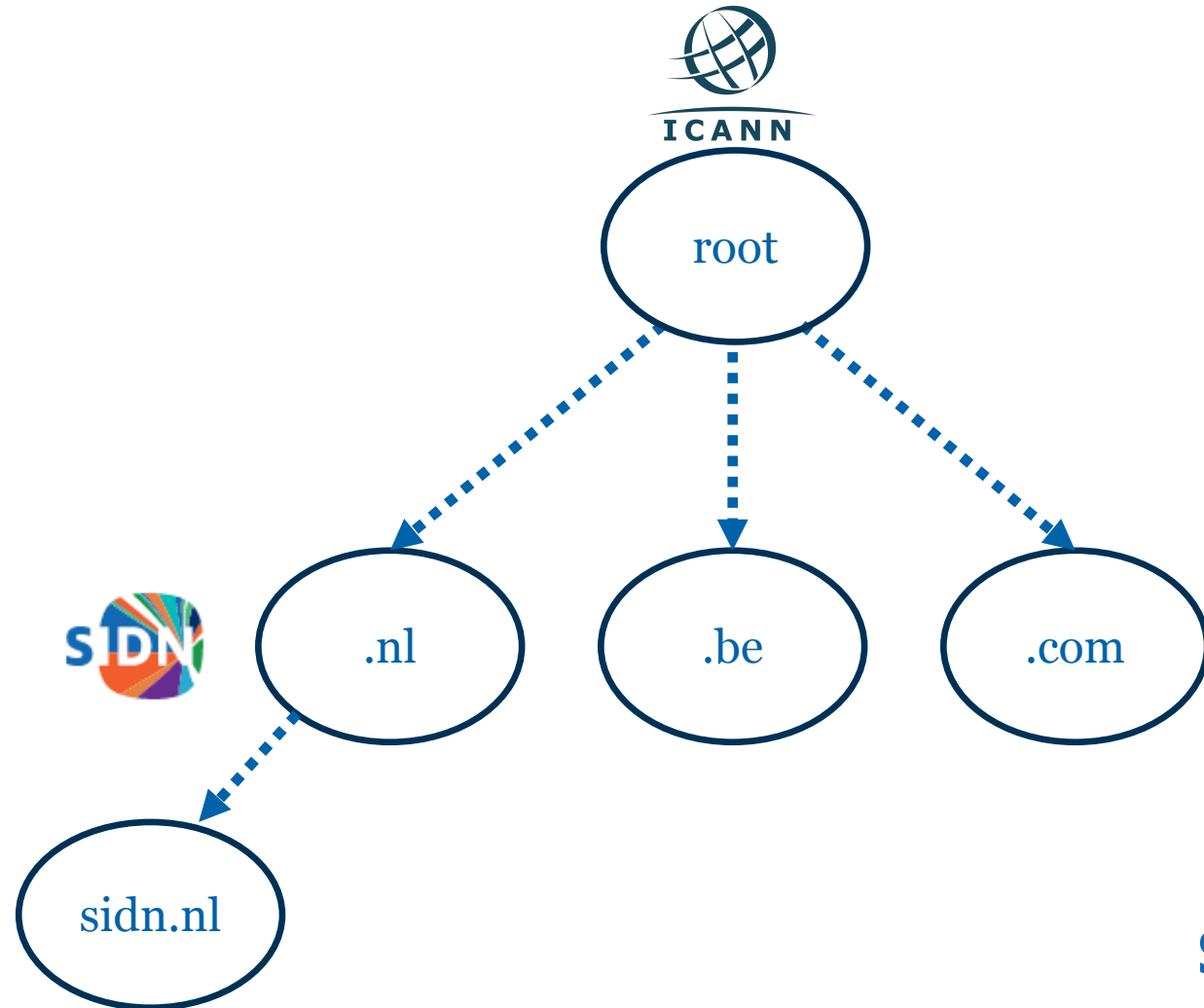
Maarten Wullink | SIDN TechTalk  
Arnhem, 18 september 2019



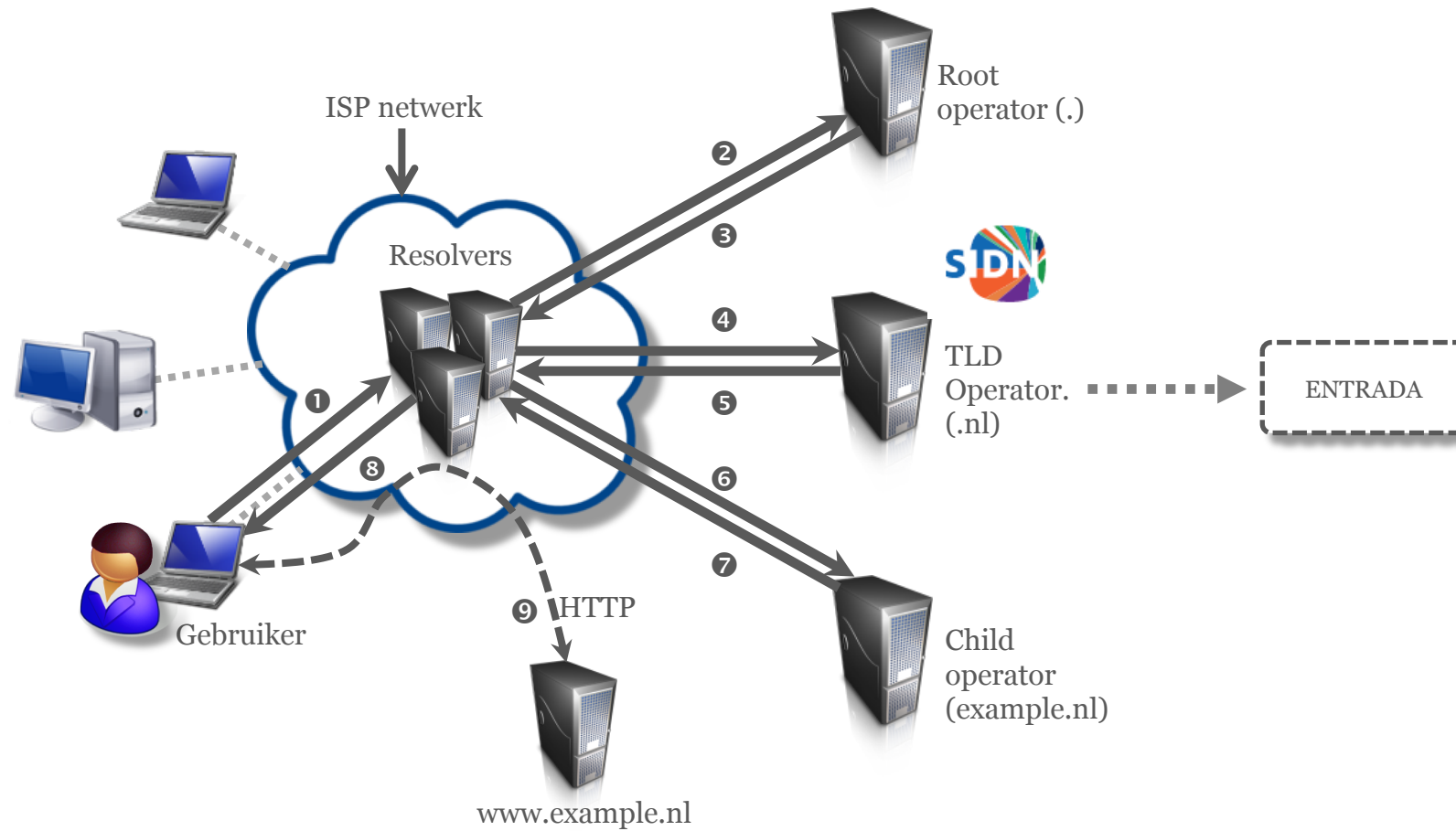
# Wat is het Domain Name System (DNS)

Protocol voor koppelen en opvragen van informatie gerelateerd aan domeinnamen

- Hiërarchisch
- Gedecentraliseerd



# DNS Resolving



# DNS data analyse

1. Capture DNS data met Tcpcdump
2. 1 pcap bestand per 5-10 minuten
3. Analyse met Wireshark/Tshark

Klaar?

TCPDUMP & LIBPCAP

WIRESHARK

The screenshot shows the Wireshark interface with a list of captured DNS packets. The selected packet (No. 74) is expanded to show its details:

- Frame 74: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits)
- Ethernet II, Src: ns1.dns.nl (b4:b5:2f:39:f1:49), Dst: JuniperN\_5f:4c:80 (a8:d0:e5:5f:4c:80)
- Internet Protocol Version 4, Src: ns1.dns.nl (194.0.28.53), Dst: 173.194.169.3 (173.194.169.3)
- User Datagram Protocol, Src Port: 53, Dst Port: 49089
- Domain Name System (response)
  - Transaction ID: 0x034a
  - Flags: 0x8410 Standard query response, No error
  - Questions: 1
  - Answer RRs: 2
  - Authority RRs: 0
  - Additional RRs: 1
  - Queries
    - hema.nl: type DS, class IN
      - Name: hema.nl
      - [Name Length: 7]
      - [Label Count: 2]
      - Type: DS(Delegation Signer) (43)
      - Class: IN (0x0001)

Wireshark voorbeeld



# ENTRADA

## ENhanced Top-Level Domain Resilience through Advanced Data Analysis

- **Doel:** verhogen van de veiligheid en stabiliteit van de .nl-zone
- **Requirements:**
  - Goede performance
  - Hoge beschikbaarheid
  - Semi real-time data warehouse
  - **SQL support**

# Technologie selectie

## SQL and NoSQL oplossingen geëvalueerd (2015)

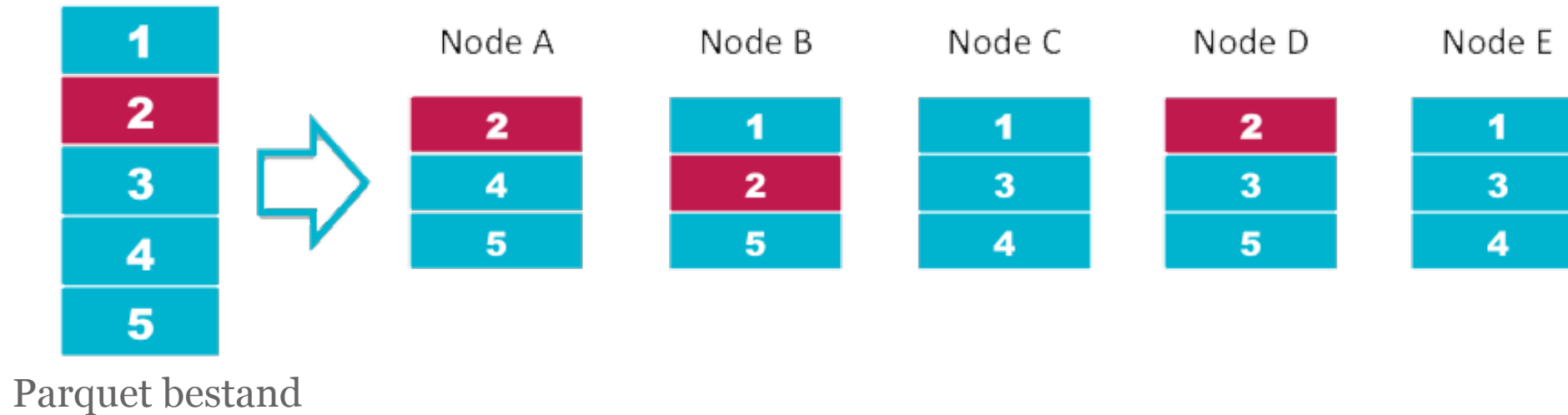
- Relationale SQL (PostgreSQL)
- MongoDB
- Cassandra
- Elasticsearch
- Hadoop (HBASE + Apache Phoenix of Hive)
- **SQL on Hadoop (HDFS + Impala + Parquet)**



# HDFS

- Hadoop gedistribueerd bestandssysteem
- Hoge beschikbaarheid doormiddel van data replicatie
- Schaalbaar tot >100 PB en >1K servers

## HDFS Data Distribution

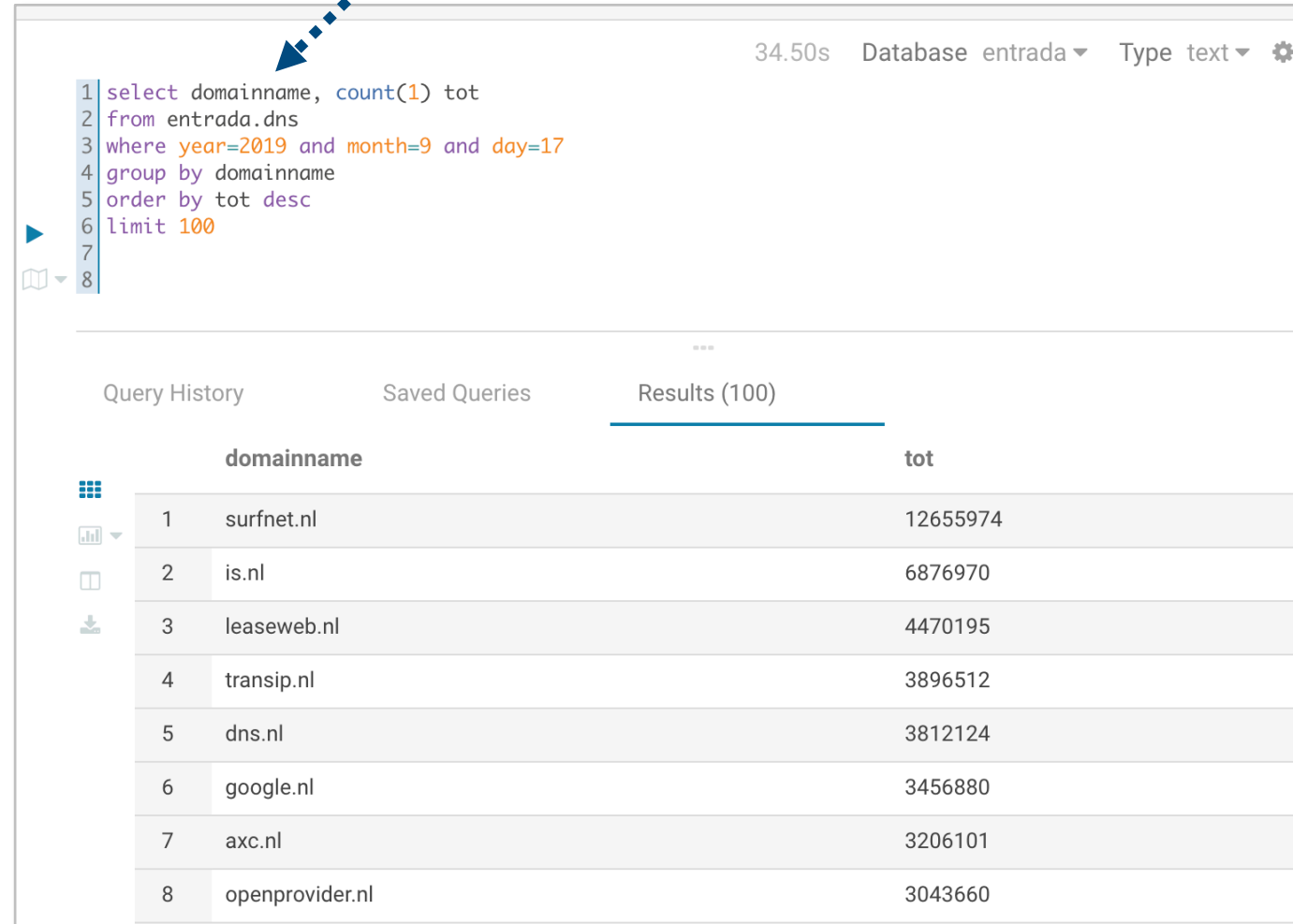




# Apache Impala

- MPP Query engine
- SQL support
- JDBC, WEB, CMD

SQL



The screenshot shows the Apache Impala query interface. At the top right, it displays '34.50s Database entrada Type text'. The SQL query is as follows:

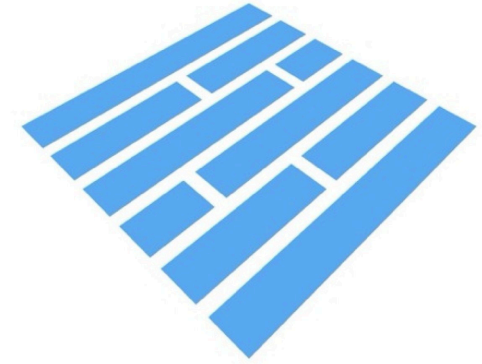
```
1 select domainname, count(1) tot
2 from entrada.dns
3 where year=2019 and month=9 and day=17
4 group by domainname
5 order by tot desc
6 limit 100
```

Below the query, there are tabs for 'Query History', 'Saved Queries', and 'Results (100)'. The 'Results (100)' tab is active, showing a table with two columns: 'domainname' and 'tot'. The results are as follows:

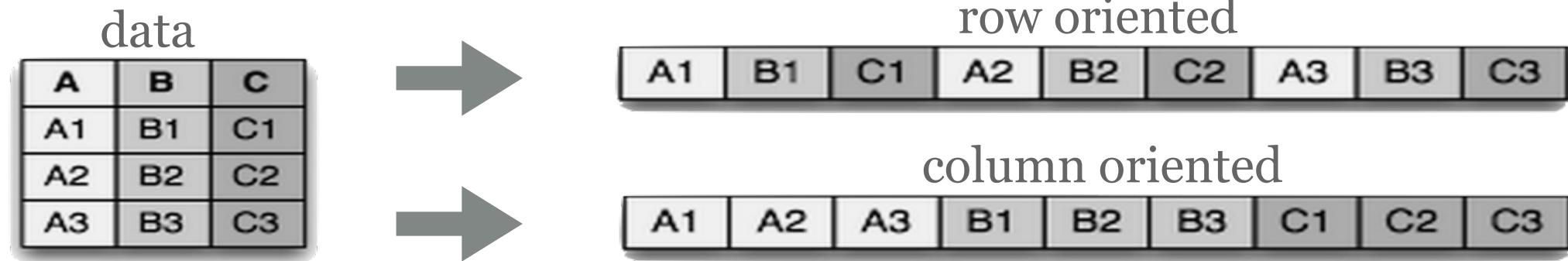
	domainname	tot
1	surfnet.nl	12655974
2	is.nl	6876970
3	leaseweb.nl	4470195
4	transip.nl	3896512
5	dns.nl	3812124
6	google.nl	3456880
7	axc.nl	3206101
8	openprovider.nl	3043660



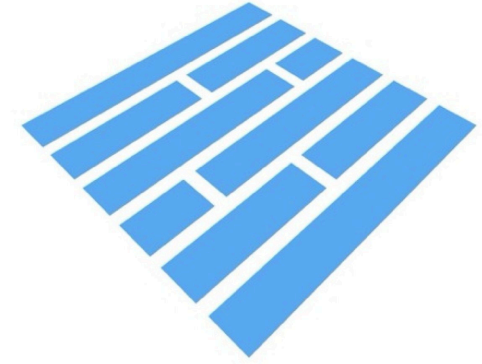
# Apache Parquet



- Columnar storage format
  - Ontwikkeld door Twitter & Cloudera
- Voordelen Parquet
  - Bestanden zijn kleiner en efficiënter te lezen (minder disk IO)

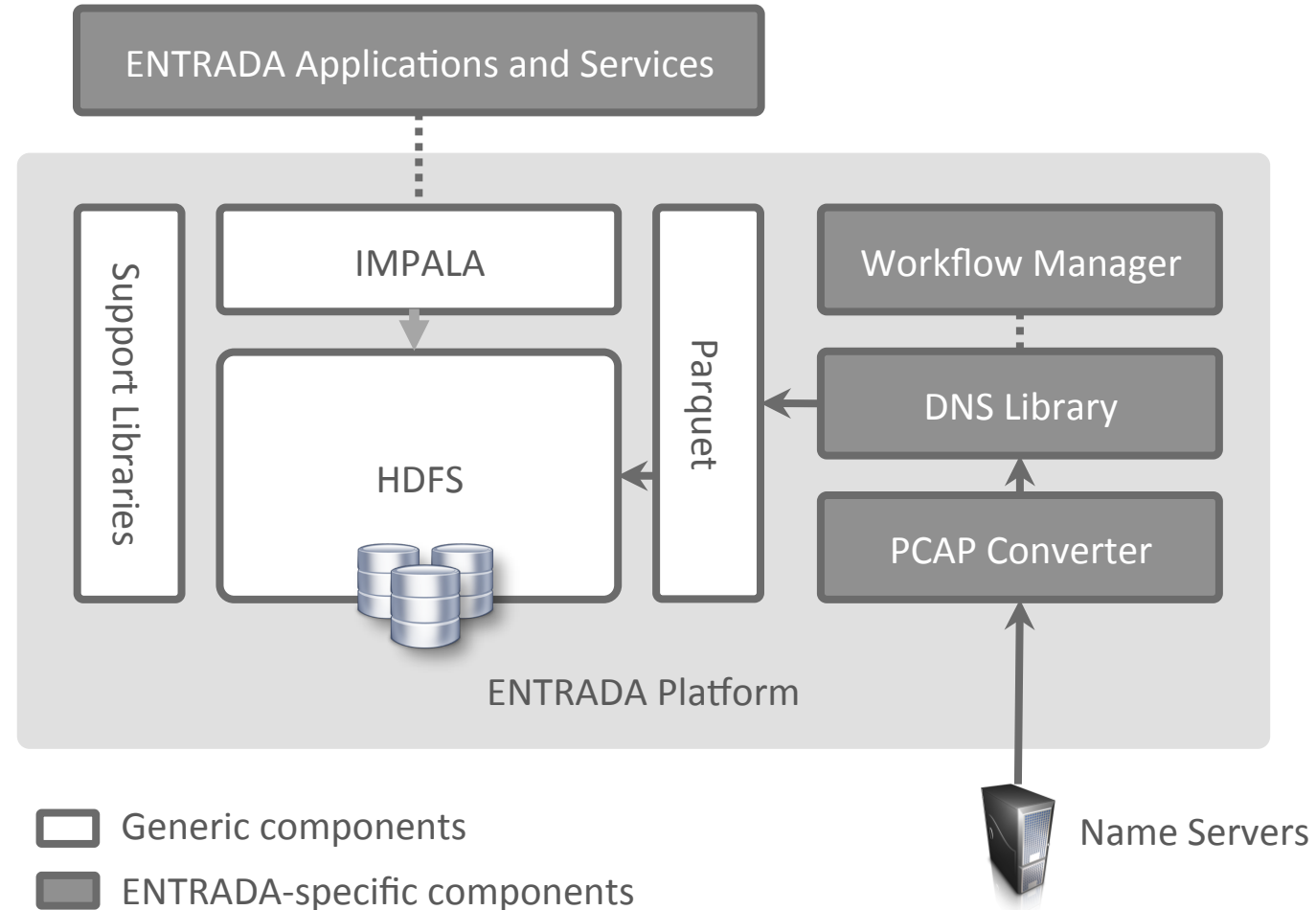


# Apache Parquet (2)

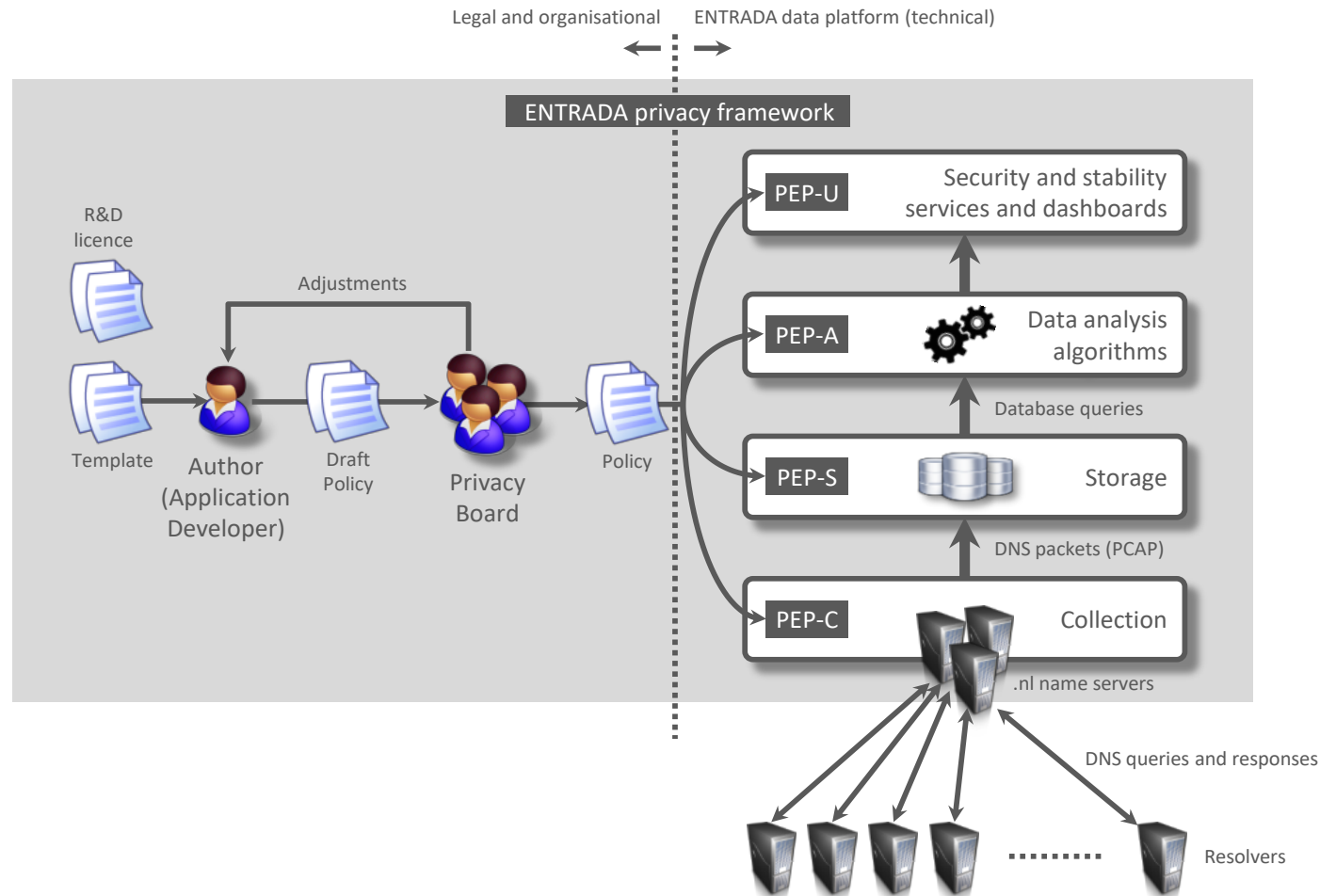


- Efficiente encoding/compressie
  - Verschillende encoding schemes (RLE, DICT ...)
  - Snappy compressie support
- Partitionering van data (jaar, maand, dag, server)
  - Partition pruning, negeer data waar we niet in geïnteresseerd zijn
- Query engine Parquet support ( Impala, Spark, AWS Athena)

# ENTRADA



# Privacy raamwerk



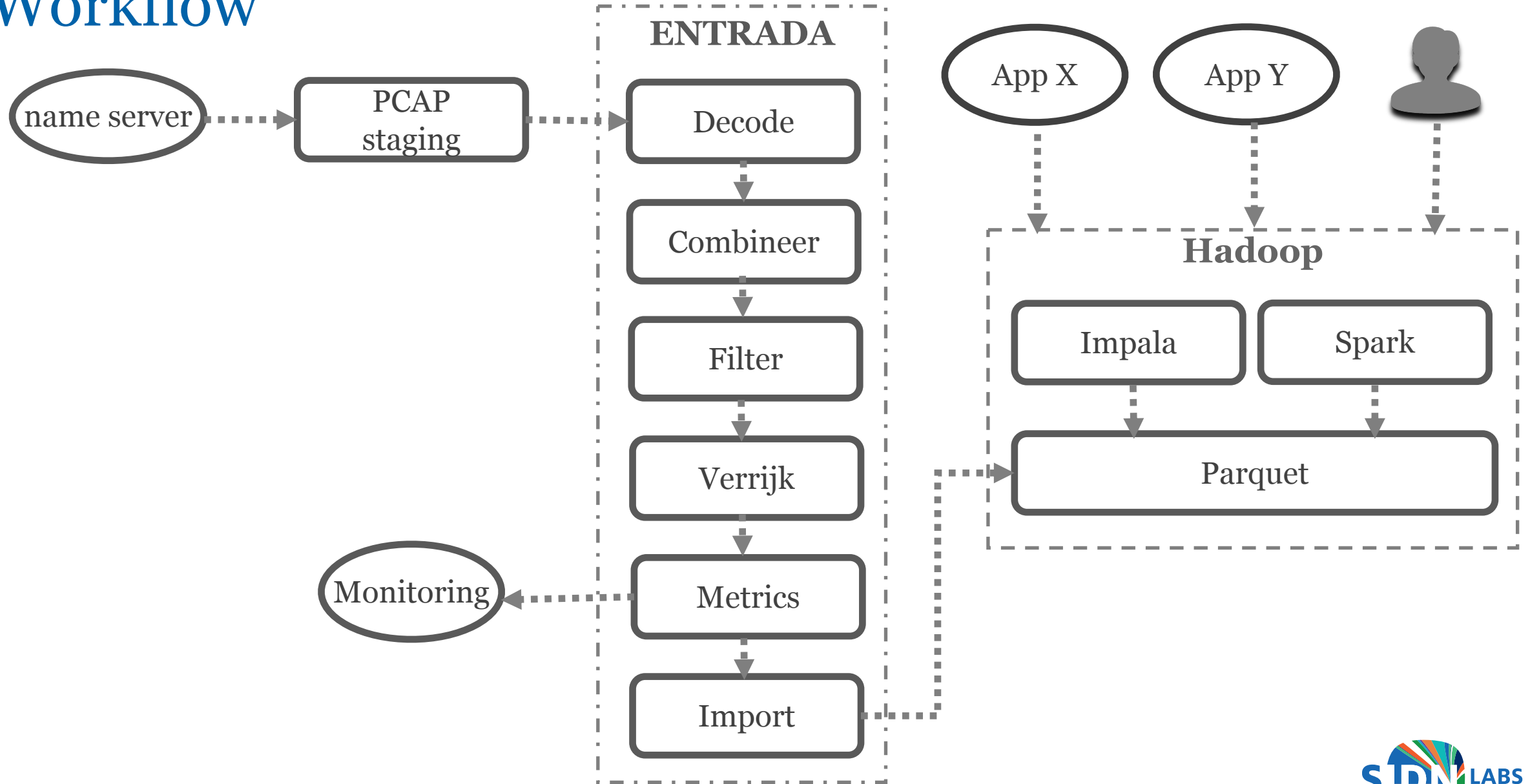
## Belangrijke concepten

Applicatie-specifiek privacy policy  
Privacy Board  
Enforcement Points

## Policy elementen

Doel  
Gebruikte data  
Filters  
Retentie periode  
Type applicatie (R&D vs. production)

# Workflow



DNS data beschikbaar voor analyse in ~10-15 minuten

# ENTRADA@SIDN Labs

- 4 jaar operationeel
- 2 anycast .nl name servers (28 sites)
- 1,2 biljoen ( $1,2 \times 10^{12}$ ) records (DNS query+response)
- 65 TB data (netto)

# Hardware (mini-cluster)

## 1x Management node

Virtual machine (VMWARE)

## 9x Data node

HP ProLiant DL380

Xeon 2.10 GHz 8 core CPU

128GB RAM

25-30 TB storage (SAS + SATA )

2x1Gb network

## Resources

142 CPU cores

~250 TB storage

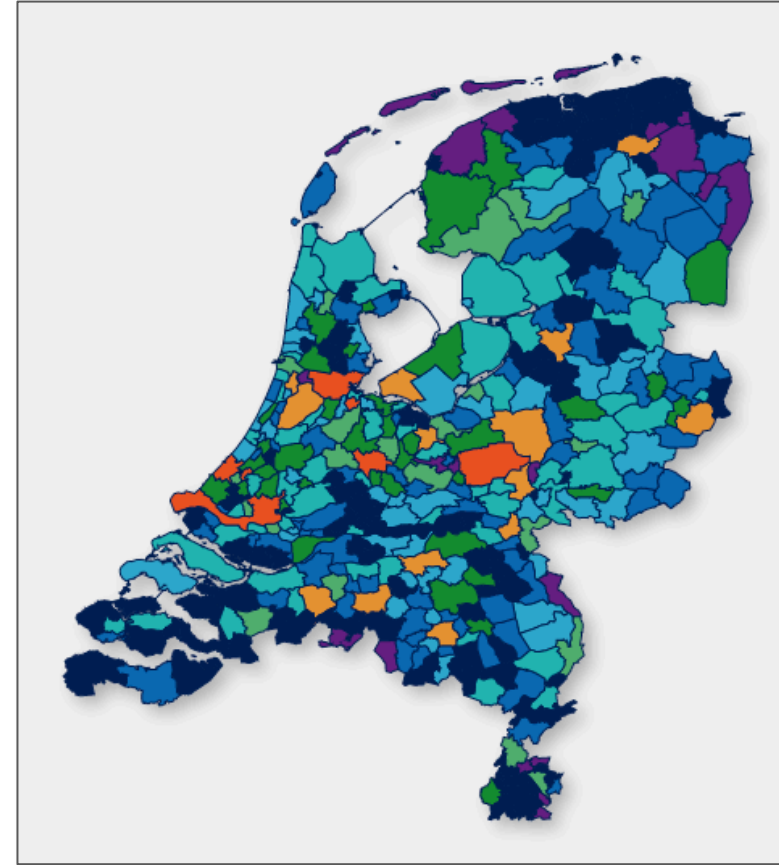
~1 TB RAM





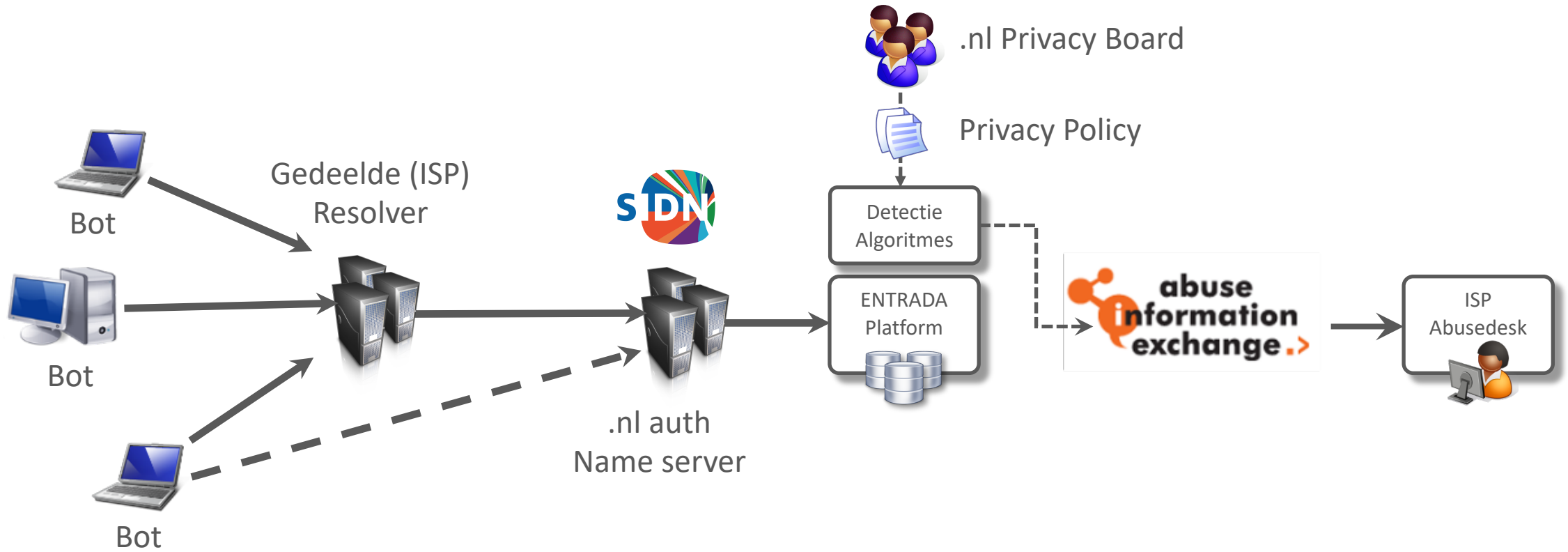
# Voorbeeld Use Cases

- Statistieken (**stats.sidnlabs.nl**)
- Onderzoek
- Inzicht voor DNS beheerders
  - Monitoring
- Detectie van misbruik
  - Botnets
  - Fake webshops

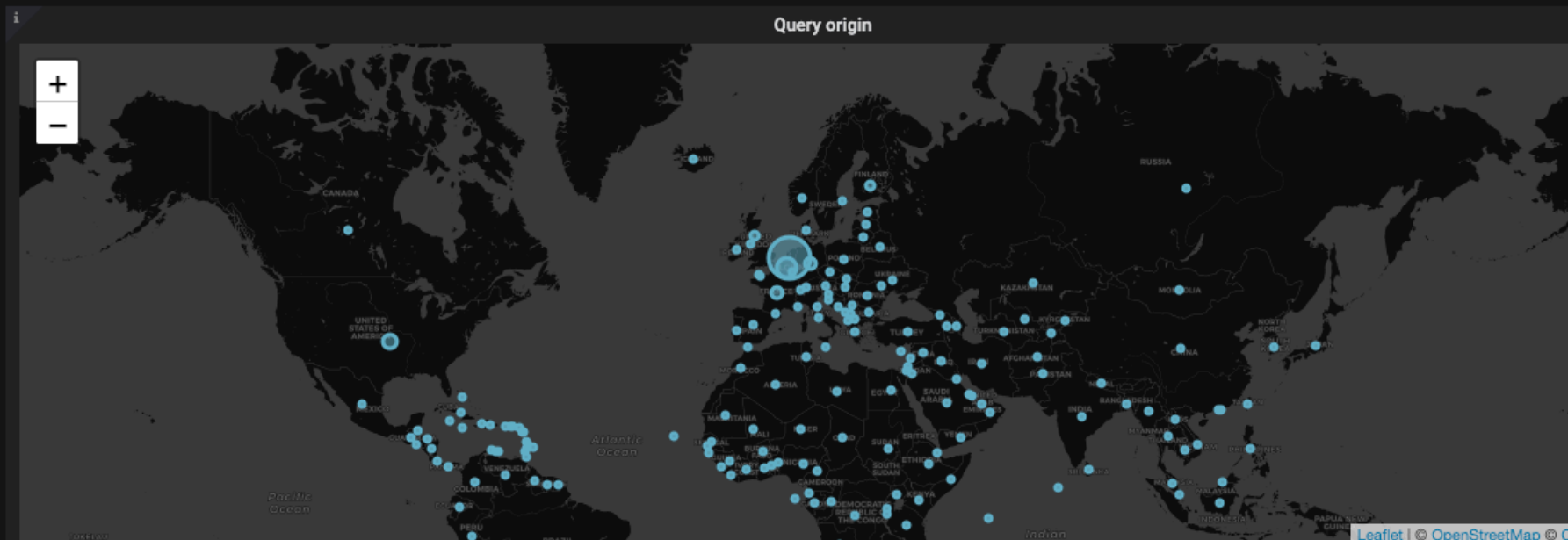
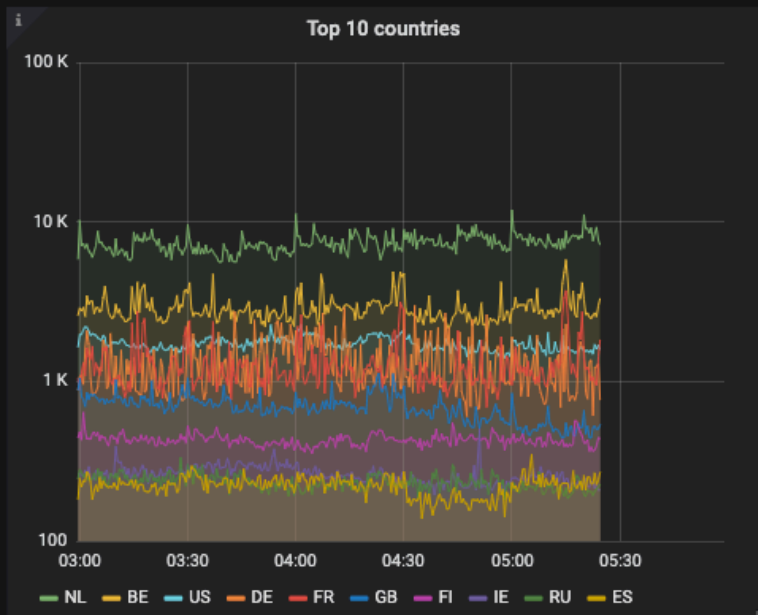
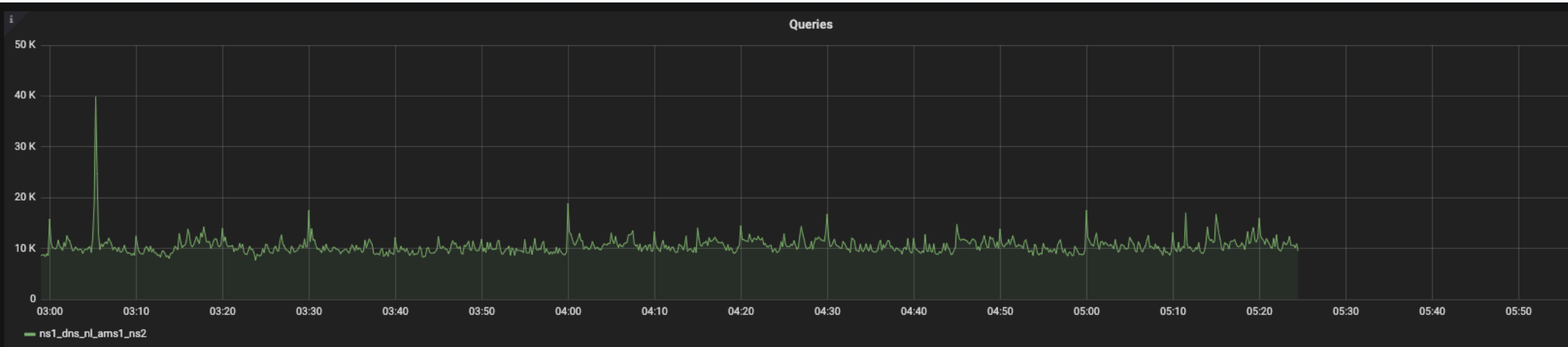


.nl-domeinnamen per postcode

# Botnet Client Detectie

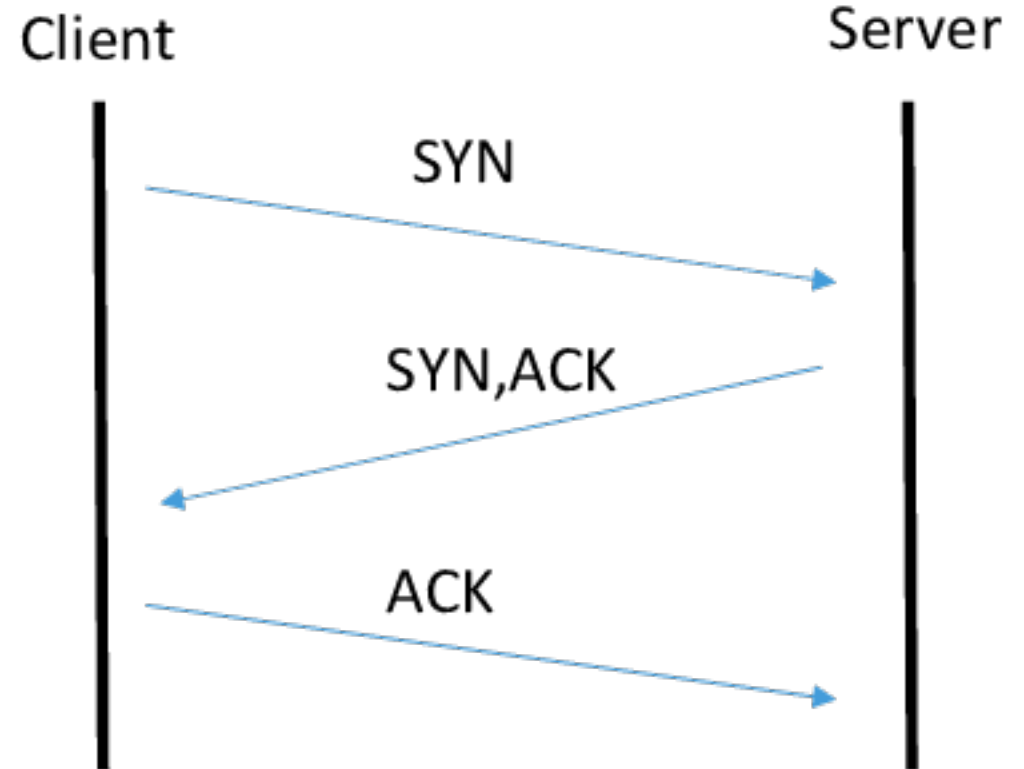


# Monitor verkeer

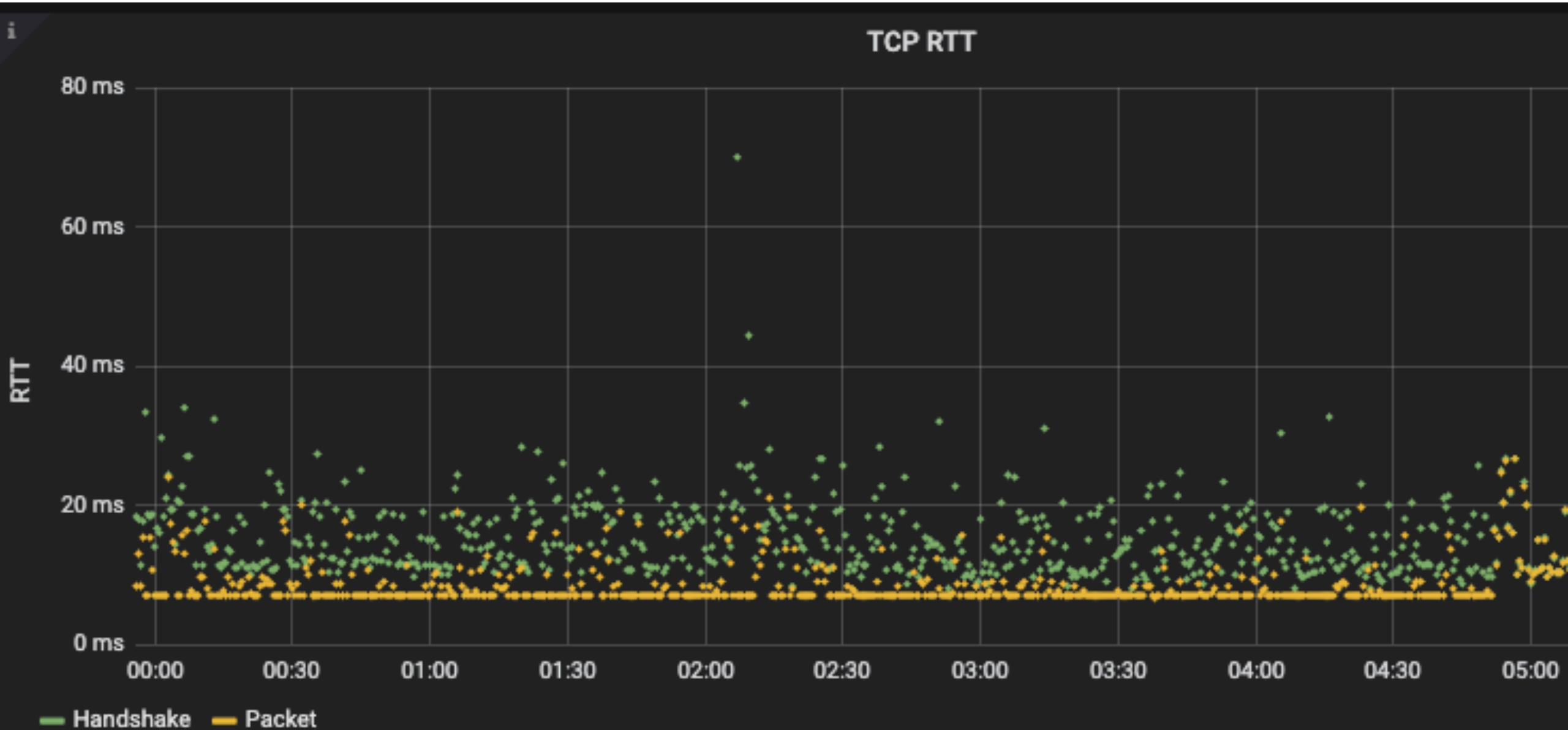


# Quality of service monitor

TCP Round Trip Time



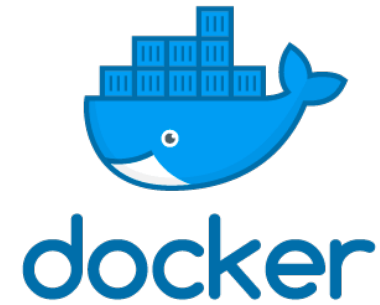
# Quality of service monitor



# Deployment

- Deploy met Docker
- Hadoop, inhouse of in de cloud
- Amazon S3 + Athena
- Config met docker-compose yaml

<https://entrada.sidnlabs.nl>



Amazon Athena



 SIDN.nl

 @SIDN

 SIDN

Q&A

[www.sidnlabs.nl](http://www.sidnlabs.nl) | [stats.sidnlabs.nl](http://stats.sidnlabs.nl)

Bedankt!

