

ENTRADA: The Impact of a TTL Change at the TLD Level

Maarten Wullink | DNS-OARC Spring 2016 workshop

March 31st 2016



SIDN

- Domain name registry for the .nl ccTLD of the Netherlands
- 5,6 million domain names
- .nl is the largest DNSSEC signed zone in the world in absolute numbers
- SIDN Labs is the R&D team of SIDN



TTL Change for .nl

Why?

- We changed the zone file update frequency from 2 hours to 1 hour
- Requested by our registrars

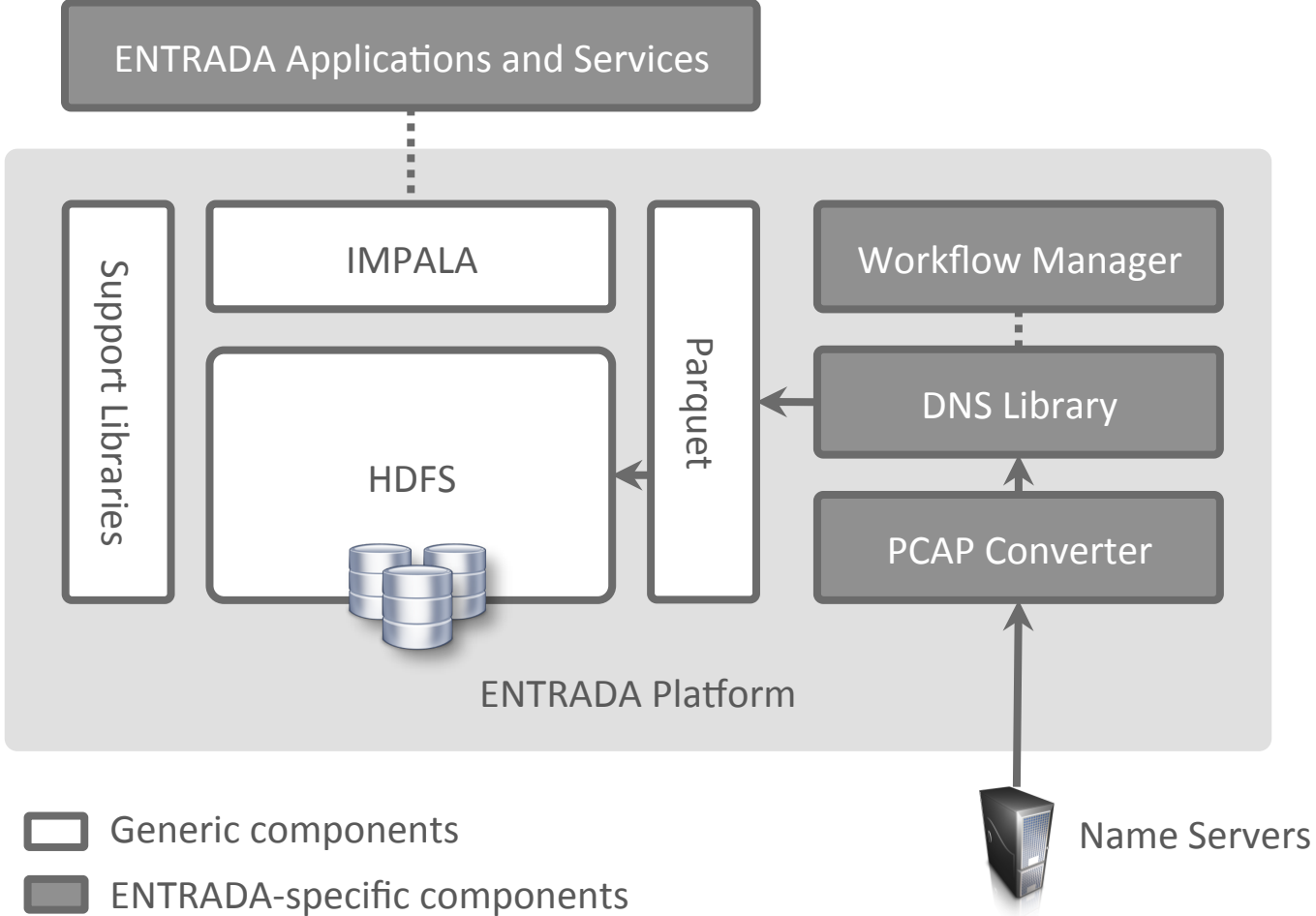
Changes:

- Delegation TTL from 7200 to 3600 seconds
- SOA NXDOMAIN TTL from 900 to 600 seconds

Impact: What effects does this policy change have on DNS traffic?

- We used ENTRADA to measure the effects
- We examined the impact on volume, QTYPE, NXDOMAIN and domainer activity

ENTRADA



ENTRADA@SIDN Labs

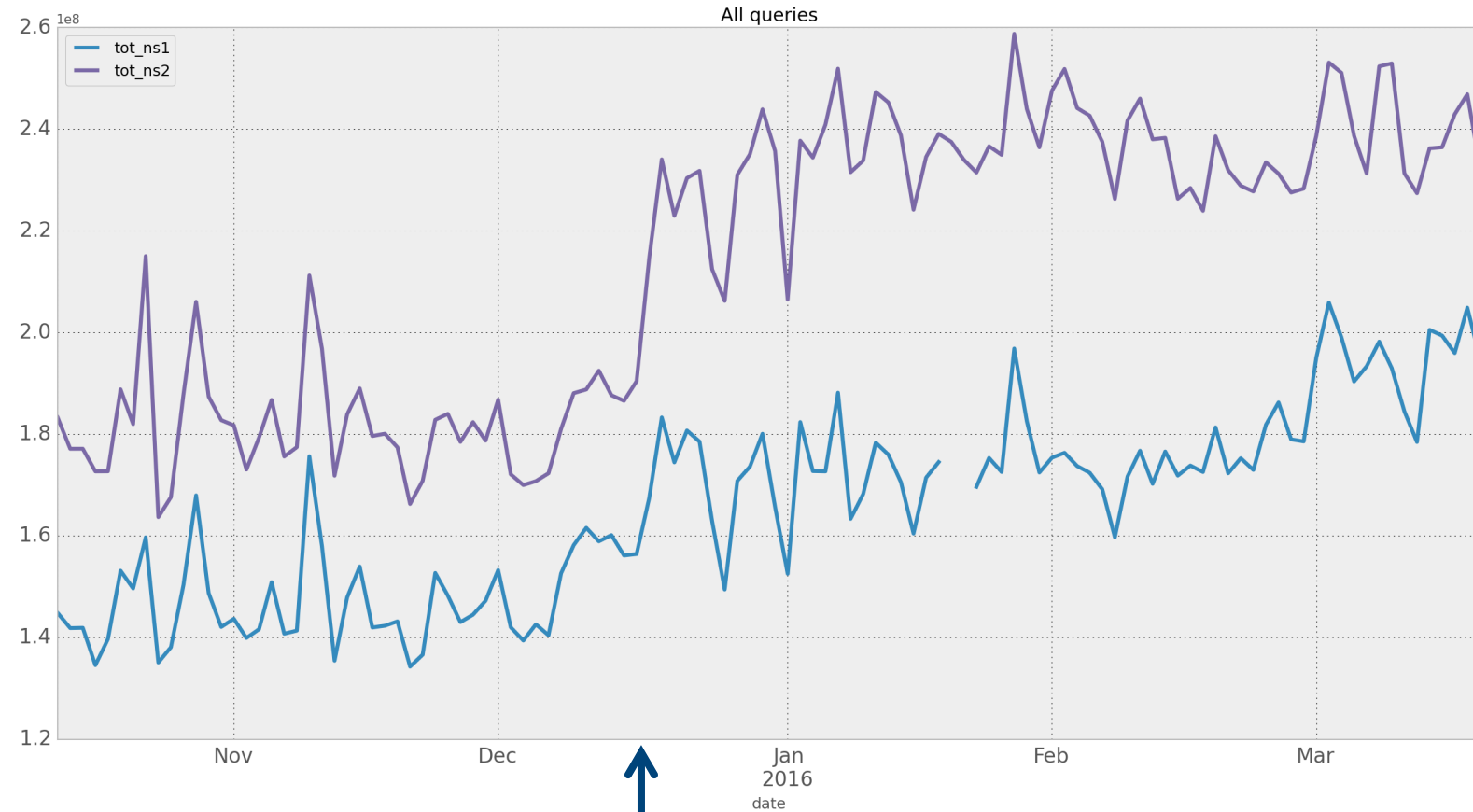
- Operational for 2 years
- Capturing data for 2 .nl name servers
- 130 Billion rows (DNS query+response pairs)
- 17 TB of data

Effect #1: Increase in Number of Queries

NS1: 22%

NS2: 30%

TLD-level TTL is most likely overruled by TTL from authoritatives

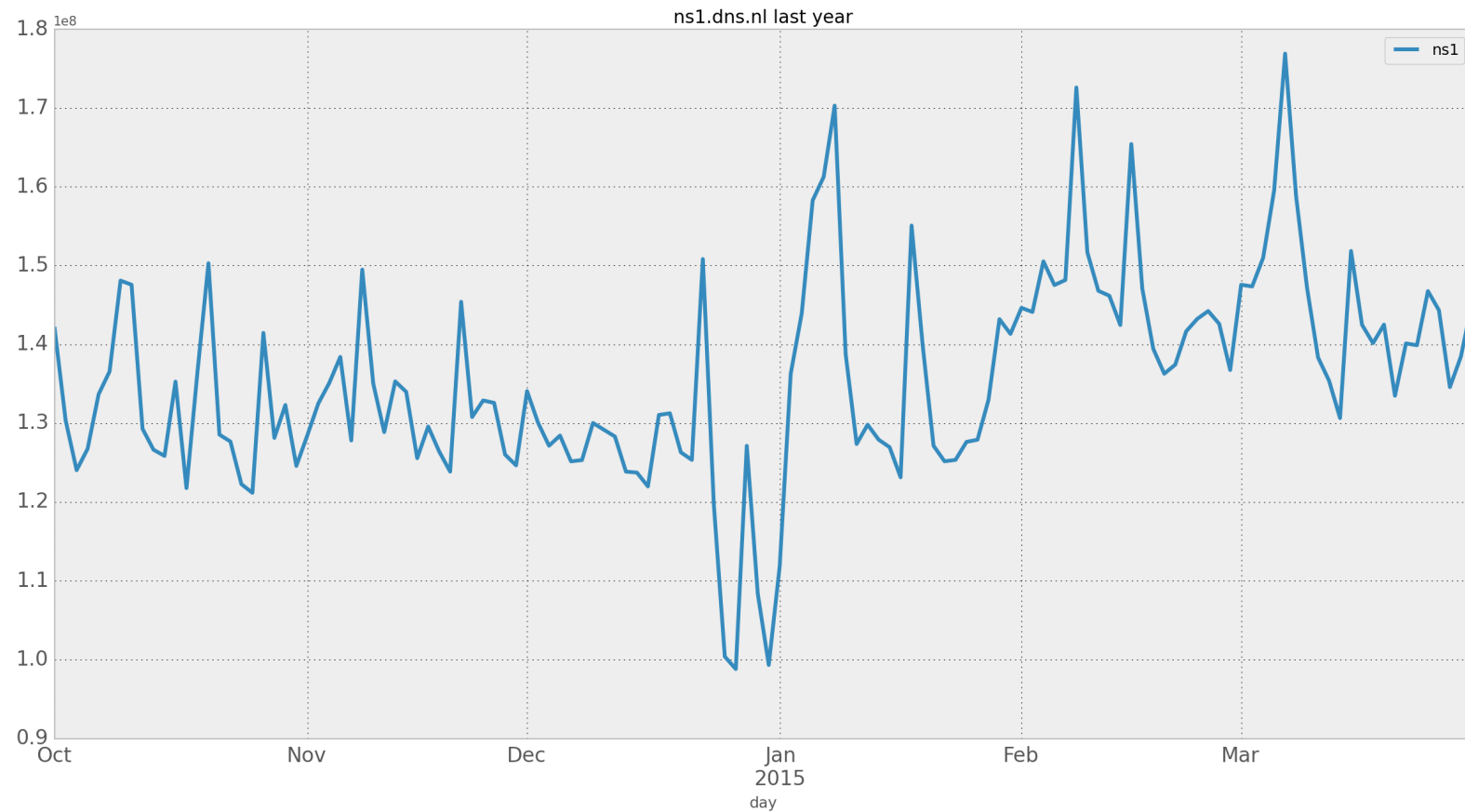


TTL change

Effect #1: Query Increase Last Year

NS1: 7%

Same period last year
we see a smaller increase



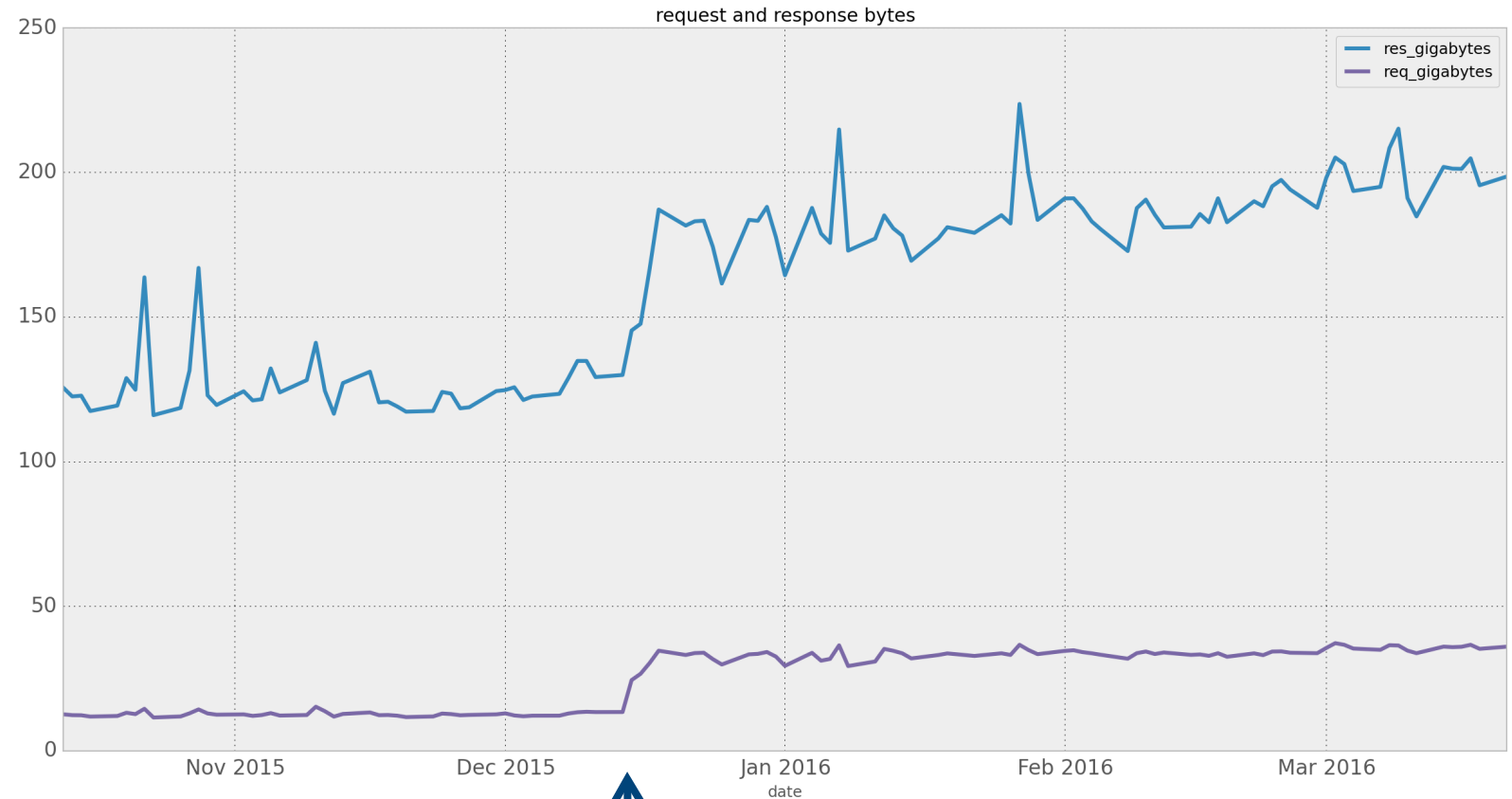
Effect #2: Data Volume

Volume

NS1+NS2

Request: +156%

Response: +47%



↑
TTL change

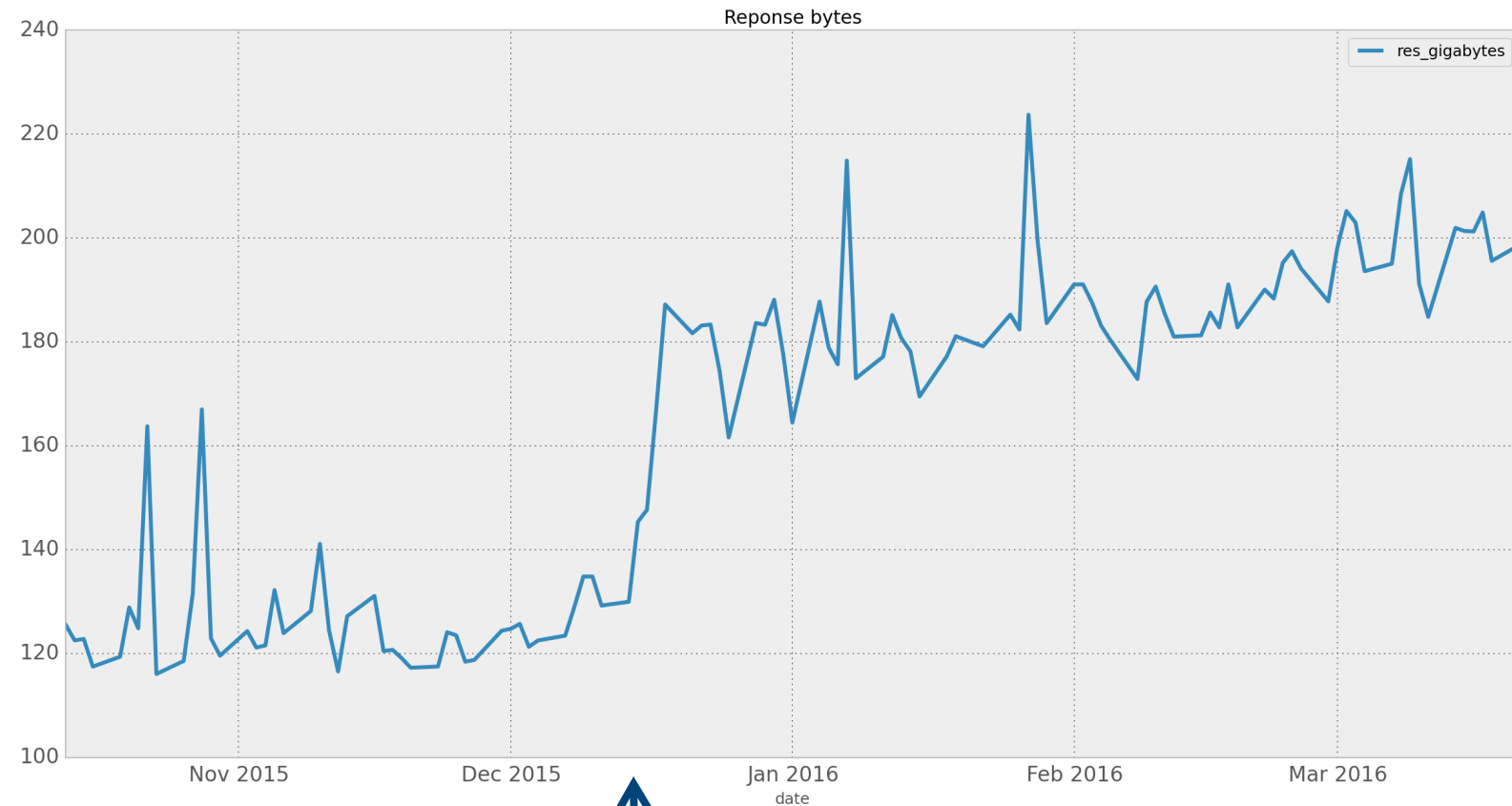


Effect #2: Data Volume

Total volume

NS1+NS2: +59%

Total data volume has
not doubled



TTL change

Effect #3: Qtype Distribution

NS1:

QTYPE Δ

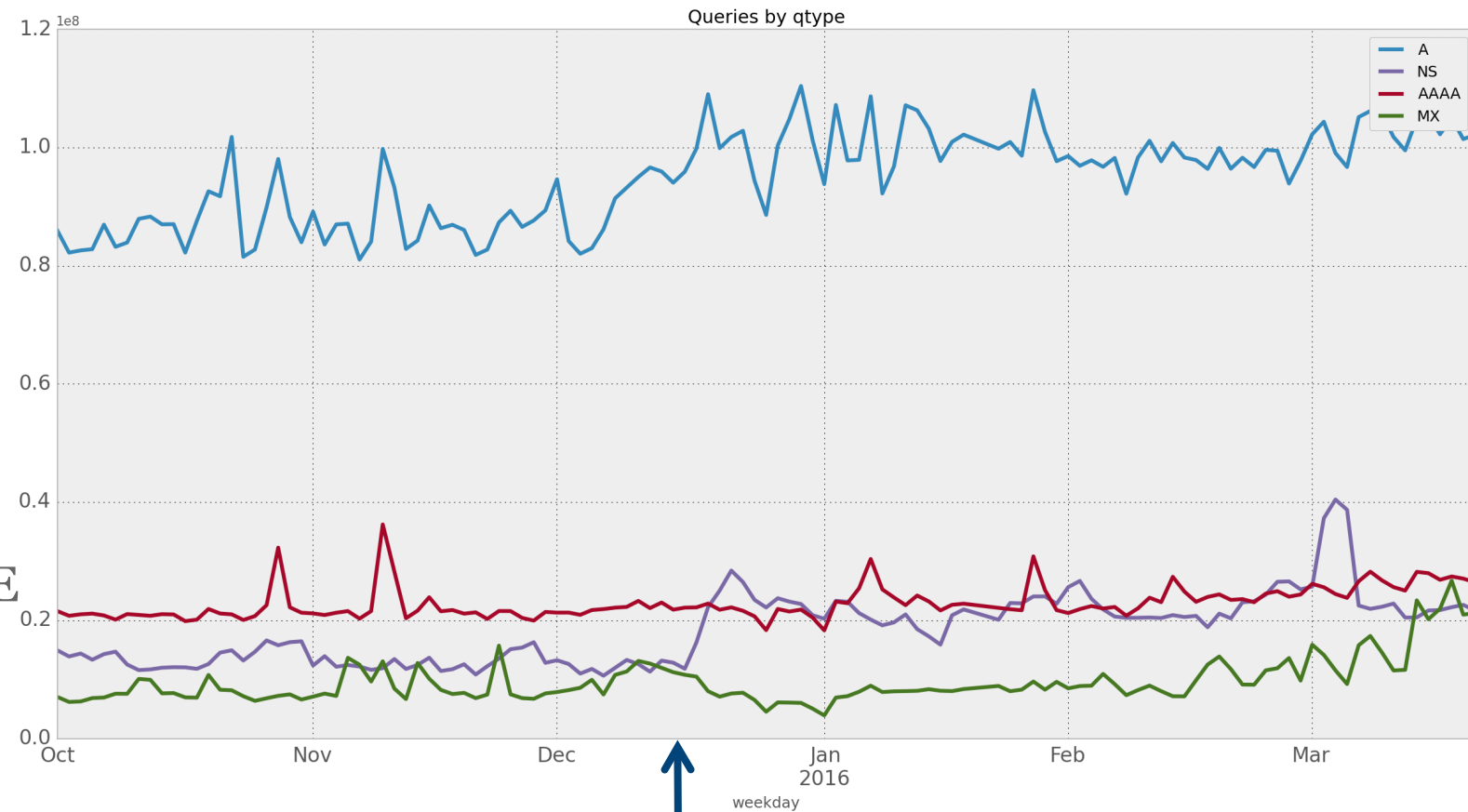
A: +14%

AAAA: +9%

NS: +75%

MX: +19%

As expected the NS QTYPE shows largest increase



TTL change

Effect #3: Qtype Distribution

NS2:

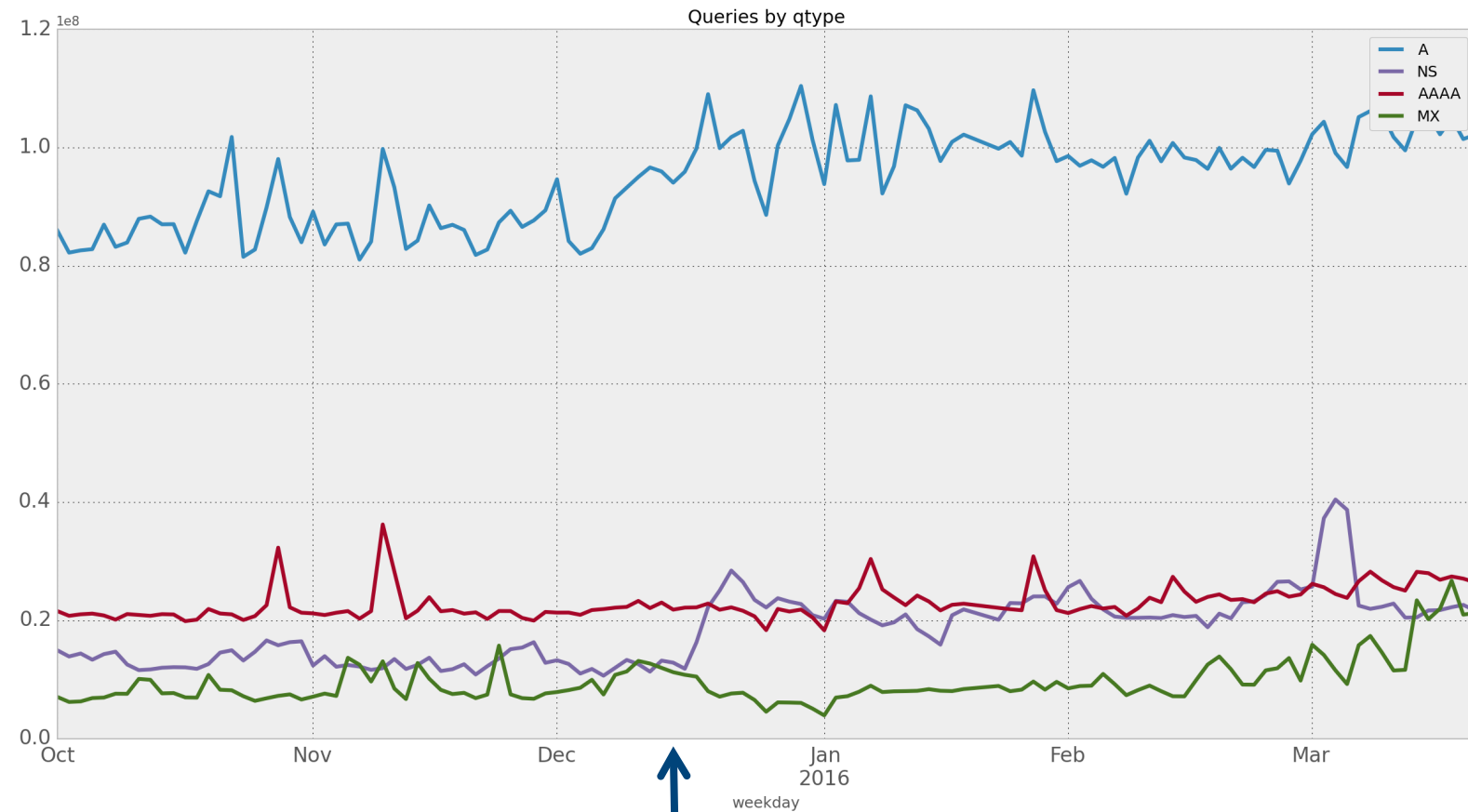
QTYPE Δ

A: +23%

AAAA: +6%

NS: +85%%

MX: +13%

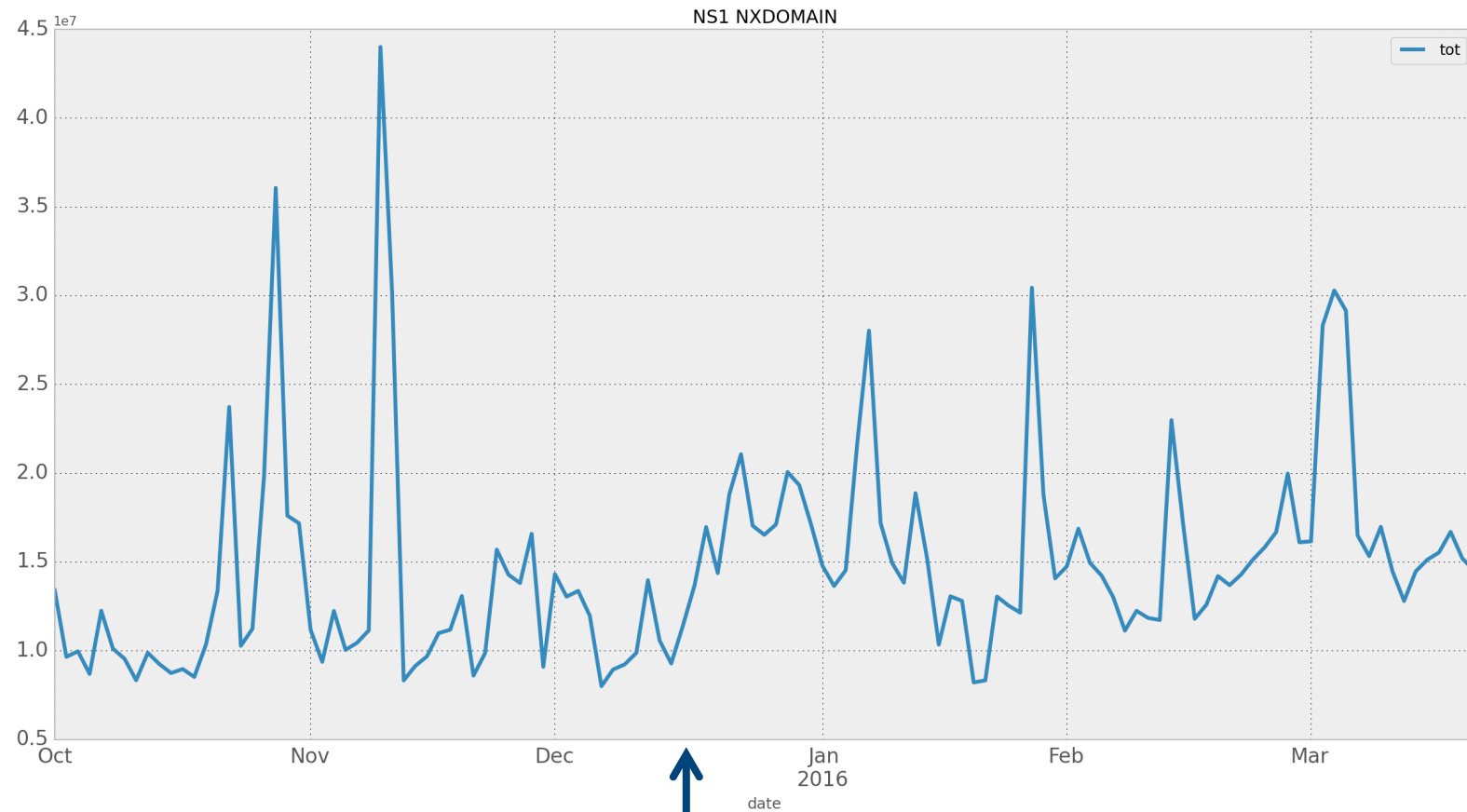


TTL change

Effect #4: Increase in NXDOMAIN Responses

NS1: ~ +30%

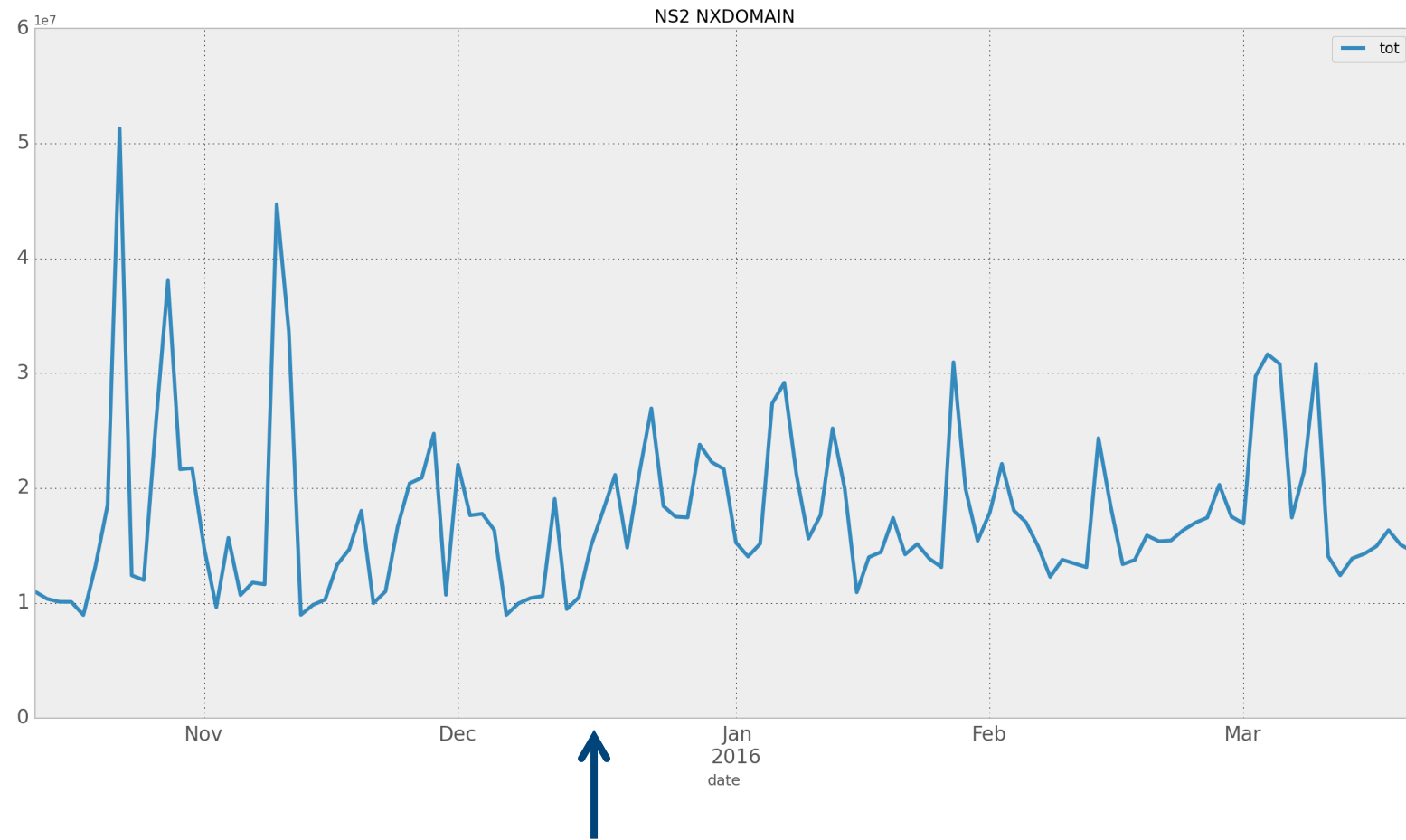
Relatively small increase
in NXDOMAINS



TTL change

Effect #4: Increase in NXDOMAIN Responses

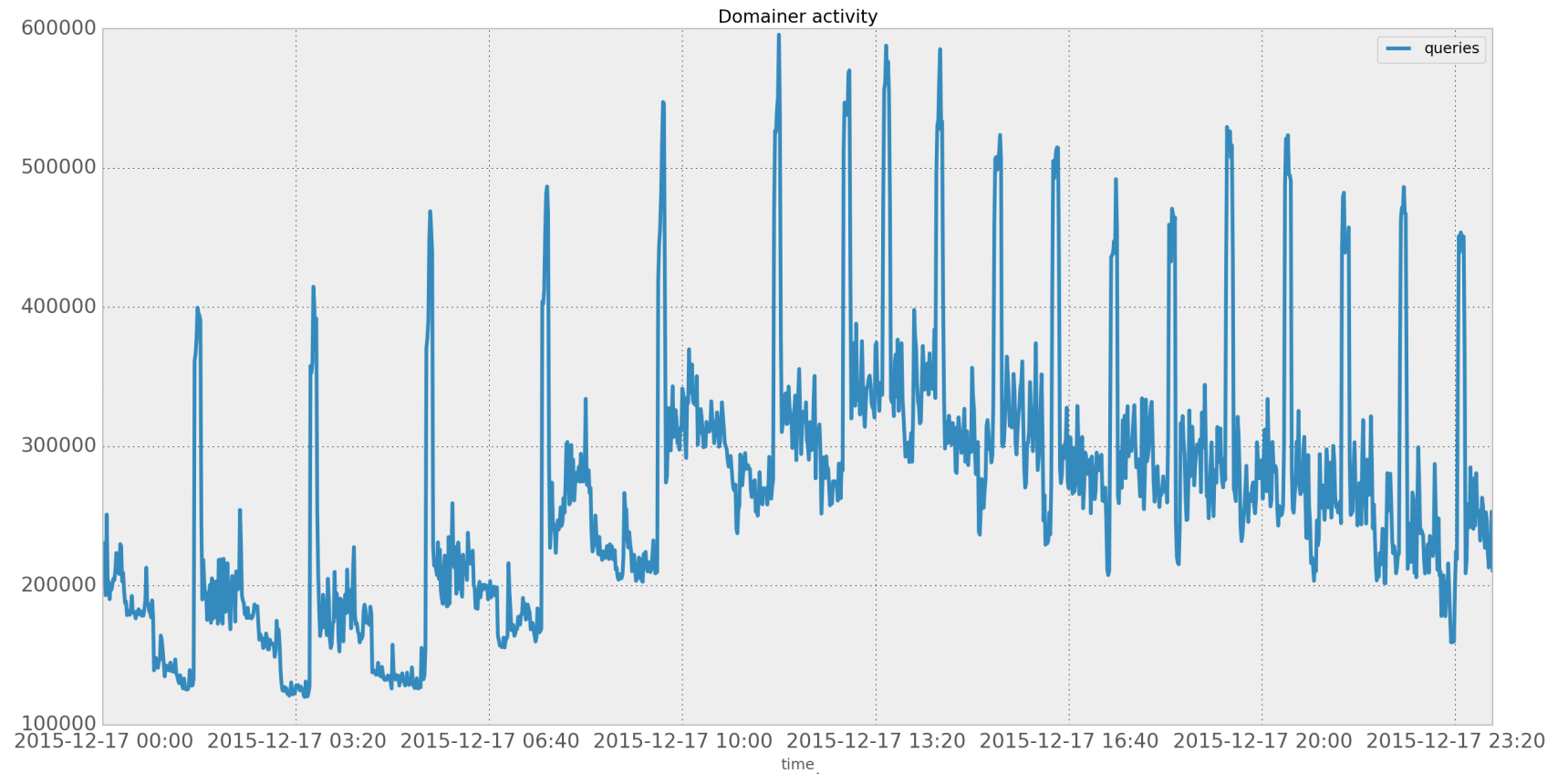
NS2: ~ +24%



TTL change

Effect #5: Domainer Activity

Domainers cause
more traffic peaks



TTL change

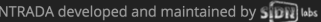
Conclusions and Discussion

- No significant impact on the operational DNS infrastructure
 - TLD-level TTL is most likely overruled by TTL from authoritatives
 - Total data volume has not doubled
 - NS QTYPE shows largest increase
 - Small NXDOMAIN increase
 - Doubled domainer query peaks
- ENTRADA proved to be very useful for measuring the effect of DNS policy changes
- We are interested in the experiences of other DNS operators and registries

Now Available as Open Source!



The screenshot shows the homepage of the ENTRADA project. At the top, there is a dark navigation bar with links for Home, ABOUT, DOCUMENTATION, COMMUNITY, GITHUB, and RESEARCH PAPER. The main header is a dark blue section with the title 'ENTRADA' and the subtitle 'An open source platform for network data analytics'. A 'Get Started' button is centered below the subtitle. The main content area is light gray and features eight feature cards arranged in a 2x4 grid. Each card has an icon, a title, and a brief description. At the bottom left, there is a copyright notice for 2016 SIDN Labs.


Home ENTRADA developed and maintained by  ABOUT DOCUMENTATION COMMUNITY GITHUB RESEARCH PAPER

ENTRADA

An open source platform for network data analytics

[Get Started](#)

- Performance**
Analyze the Parquet data equivalent of about 50 terabytes of pcap data in under 3.5 minutes with a small 4 data-node cluster. Read the performance evaluation in our [research paper](#).
- Analytics**
Use an efficient columnar data format with a massively parallel SQL query engine for low latency and high concurrency analytic queries.
- Query Language**
Query your data using the SQL-92 standard and standardized interfaces for Java and Python, which makes it easy for anyone to start analyzing network data
- Data model**
Using a data model designed for DNS/IP/TCP/UDP/ICMP network data enabling fast analytics with precomputing, enrichment and pre-joining of request and response packets.
- Monitoring**
View real-time process and network data metrics with Graphite and Grafana dashboards. Visualizing ENTRADA processes and ingested network data.
- Storage**
Automatic conversion to a columnar data format with efficient compression and encoding schemes is used to optimize the data volume and query performance.
- Workflow**
Automating all the steps required to insert captured network data into the ENTRADA database. Spend 100% of your time on data analysis.
- Support**
Availability of multiple support channels for users and developers. Contact us for any questions about [support](#).

Copyright (C) 2016 

entrada.sidnlabs.nl



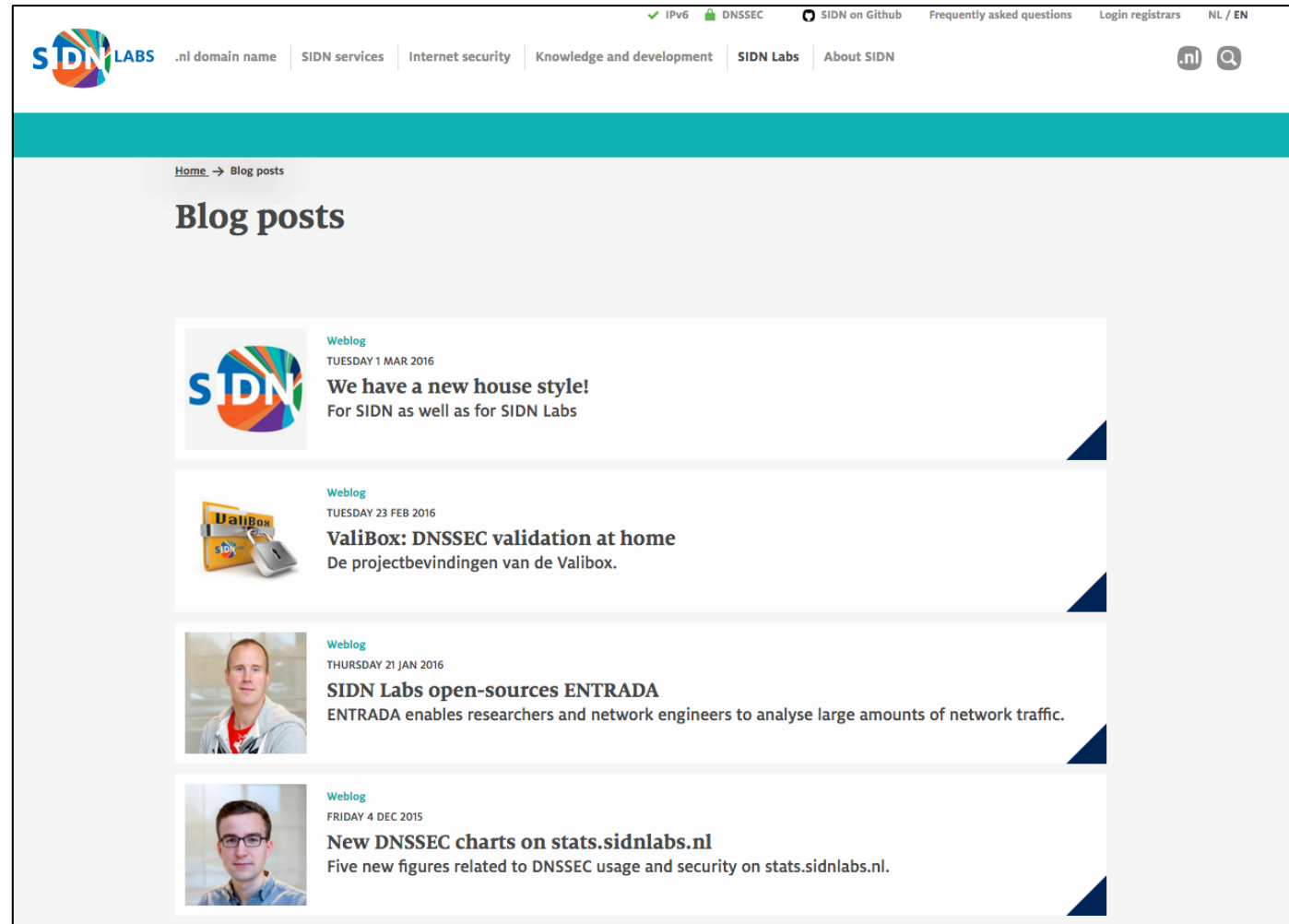
Questions?

Maarten Wullink
Research Engineer

maarten.wullink@sidn.nl

 @wulliak


www.sidnlabs.nl





The screenshot shows the SIDN Labs website with a teal header. The navigation menu includes: SIDN LABS, .nl domain name, SIDN services, Internet security, Knowledge and development, SIDN Labs, and About SIDN. Utility links include: IPv6, DNSSEC, SIDN on Github, Frequently asked questions, Login registrars, and NL / EN. A search icon and ".nl" domain icon are also present.


Breadcrumbs: Home → Blog posts

Blog posts

- 

Weblog
TUESDAY 1 MAR 2016
We have a new house style!
For SIDN as well as for SIDN Labs
- 

Weblog
TUESDAY 23 FEB 2016
ValiBox: DNSSEC validation at home
De projectbevindingen van de Valibox.
- 

Weblog
THURSDAY 21 JAN 2016
SIDN Labs open-sources ENTRADA
ENTRADA enables researchers and network engineers to analyse large amounts of network traffic.
- 

Weblog
FRIDAY 4 DEC 2015
New DNSSEC charts on stats.sidnlabs.nl
Five new figures related to DNSSEC usage and security on stats.sidnlabs.nl.