Serverless DNS Analytics using ENTRADA 2.0

Moritz Müller | SIDN Connect 2019

28 November 2019
Remember ENTRADA?

• Open source tool that handles large amounts of DNS traffic
• It processes, converts and enriches PCAP data
• It stores the data
• It provides interfaces for data analytics
• Deployed by multiple TLDs
What can you do with DNS traffic?

A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries1, Quiçin Scheidle2, Moritz Müller3,5, Willem Tourop4, Ralph Döllner4, Roland van Rijswijk-Deij1,5

1University of Twente, 2TUM, 3SIDN Labs, 4KLU, 5SAN

Abstract. The Domain Name System (DNS) is a critical part of network and internet infrastructure. DNS lookups provide almost any user request. DNS lookups may contain private information about the sites and services a user contacts, which has spurred efforts to protect privacy of users such as transport encryption through DNS over TLS or DNS over HTTPS. In this work, we provide a first look at the recent advances in techniques of minimizing DNS queries in order to provide privacy protection.
What can you do with DNS traffic?
What can you do with DNS traffic?
What can you do with DNS traffic?

Queries
www.rabobank.vervang-service.nl.
Drawbacks of ENTRADA 1.0

ENTRADA 1.0 runs on Hadoop

• Setup and maintenance costs time and money
• Requires knowledge of Hadoop
• Requires hardware or software cluster
This is why we introduce: ENTRADA 2.0

New Features

• Serverless DNS analytics
• Support for multiple SQL query engines
• Quality of Services Monitoring, round-trip time (RTT) analysis
• Easier deployment using Docker
Serverless DNS analytics
Serverless DNS analytics
DNS analytics on the computer of someone else
Serverless DNS analytics
DNS analytics on the computer of someone else

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

ENTRADA will:
• Create database schema
• Convert, upload and optimize data
DNS analytics on the computers of Amazon

Support for Amazon Web Services (AWS)

- S3 storage
- Athena SQL-query engine
- Pricing; $5 per TB of scanned data
Quality of Service Monitoring

- Understanding how clients perceive your DNS service is crucial for measuring reliability, e.g.:
  - are there issues with my uplink?
  - are there issues with my routing/anycast?
  - are there issues with my client?
Quality of Service Monitoring

• External monitoring platforms exist, but:
  • they often cost money
  • they don’t reflect your real clients
  • they don’t provide easy to interpret interfaces
Quality of Service Monitoring with TCP

\[ \text{dif(SYN ACK – ACK)} = \text{RTT} \]
Links

• Introduction: https://www.sidnlabs.nl/nieuws-en-blogs/tijd-voor-entrada-2-0
• Documentation: https://entrada.sidnlabs.nl/
• Source Code: https://github.com/SIDN/entrada

• Contact:
  • Maarten Wullink (marten.wullink.sidn.nl)
  • Moritz Müller (moritz.muller@sidn.nl)