ENTRADA

ENTRADA (***ENhanced Top-level domain Resilience through Advanced Data Analysis*** )

Goal

* Provide support for Entrada.
* Install, Configure, and customize plugins for entrada.

What is Entrada?

* Entrada - A tool for DNS big data analytics
* ENTRADA processes DNS data (PCAP-files) from an input location (local, HDFS or S3) and converts and enriches the data to Apache Parquet format, finally sending the results to one of following endpoints:
  + HDFS + Impala (hadoop)
  + S3 + Athena (aws)
  + Local disk (local)

Work done so far

Entrada 0.1.3

* Wrote bash script that splits and renames a hierarchy pf pcap files and send them over with specific time intervals to Entrada.
* Entrada 0.1.3 is designed to process and analyze live feed of pcap file or DNS traffic and show the import time of Queries in the Dashboard Graphana.
* We dove deep into Entrada code and modified it to make Entrada analyze old pcap files instead of live feed.
* Working on Entrada Code to enable World map plugin.

Why Entrada 0.1.3 and not Entrada2.0.3

* Entrada 2.0.3
  + Kind of different and New to Us!
    - This version was deployed very recently, so our work is focused on the previous version.
  + Entrada 2.0.3 have less metrics than Entrada 0.1.3

Tools and apps we used:

IDE: Netbeans, Eclipse

Text Editors: Vi, Nano, Gedit

Development OS: Centos7

Scripting languages: Bash

Programming Languages: Java

Our favorite Command line: SSH