**Feeding entrada by PCAP files**

The section describes how to feed entrada by pcap files. Since entrada installed in namenode server, the data should be sent to that node to specific location.

**Configuration of the sender:**

* Install ssh server and ssh-clinent .

(yum -y install openssh-server openssh-clients)

* Install sshpass.

(yum install sshpass)

* Install wireshark in the sender node (check capinfos command).

(yum install wireshark\*)

**Configuration of the namenode:**

* Enough storage in the namenode server to handle the big data.
* Install ssh server and ssh client.
* Create folders for each server (e.g. DNS1-PRI, DNS1-SEC, DNS2-PRI, DNS2-SEC) in the captures file in the home of namenode server.

-----------------------------------------------------------------------------------------------------------------

1. The data can be stored in any node in the cluster or any device that can communicate with namenode.
2. Specify the requirements in the bash script
   * username="entrada"
   * server\_ip=192.168.100.1
   * path\_to\_destination="/home/entrada/captures"
   * location=PCAP\_DATA
   * pass="12345"
3. check that all the requirement is installed before running the script.

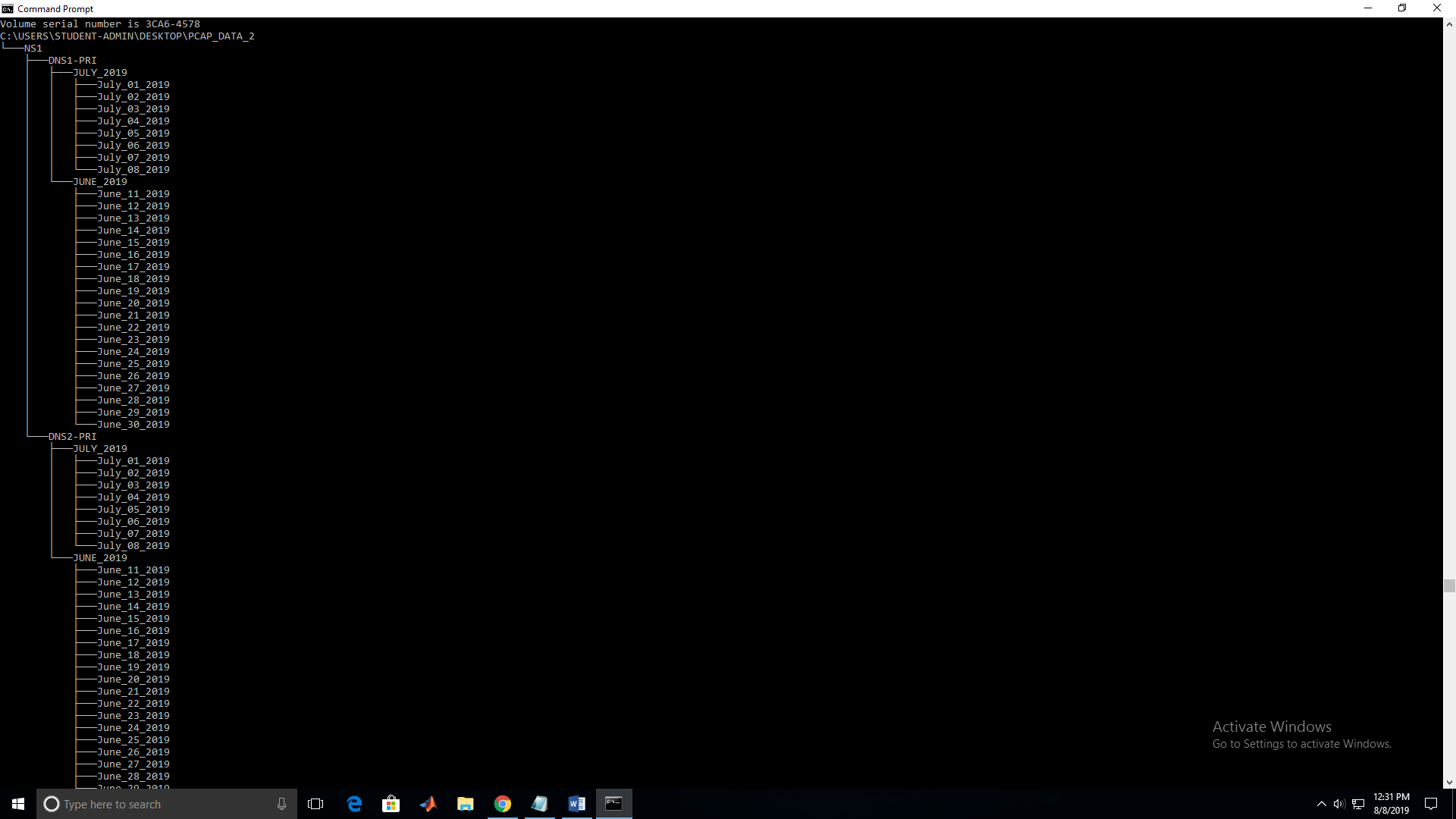
**PCAP\_DATA Directory Tree:**

PCAP\_DATA/NS1/DNS1-PRI/MONTH\_YEAR/month\_day\_year/anyname.pcap

PCAP\_DATA/NS1/DNS2-PRI/MONTH\_YEAR/month\_day\_year/anyname.pcap

PCAP\_DATA/NS2/DNS1-SEC/MONTH\_YEAR/month\_day\_year/anyname.pcap

PCAP\_DATA/NS2/DNS2-SEC/MONTH\_YEAR/month\_day\_year/anyname.pcap



**PCAP Files Script:**

1)Copy the PCAP\_DATA to the home Directory in Namenode4

2) Run the script (shell\_test2.sh ) using “ sudo ./shell\_test2.sh PCAP\_DATA/”

3) switch to Namenode 1 and open Grafana in the browser at [http://192.168.9.102:3000](http://192.168.9.102:3000/)

**Grafana**

Grafana Documentation Page: <https://grafana.com/docs/guides/getting_started/>

1. In Namenode 1, open Grafana in the browser at [http://192.168.9.102:3000](http://192.168.9.102:3000/)
2. Click on the Dashboard Dropdown located in the top left corner of the screen
3. Choose “DNS Analysis” or any other dashboard you want to show.

Grafana Variables:

Query : entrada.\*

Regex: DNS[1-2].\*

**Cleaning old data for a fresh start: (Create a script)**

1. In Namenode, remove all files in /opt/graphite/storage/whisper/entrada using the command “ sudo rm –rf /opt/graphite/storage/whisper/entrada/\* “
2. Remove all the files in the locations :

* /home/captures/
* /home/pcap/incoming/
* /home/pcap/processing/
* /home/pcap/prossesed/archive

1. Remove the files :

* /home/entrada-latest/tmp/DNS1-PRI-pcap-process.hist
* /home/ entrada-latest /tmp/DNS2-PRI-pcap-process.hist
* /home/ entrada-latest /tmp/DNS1-SEC-pcap-process.hist
* /home/ entrada-latest /tmp/DNS2-SEC-pcap-process.hist

1. Remove the data form impala
   * Open **Hue** <http://192.168.9.102:8889> (user=admin)(pass=admin)
   * Then write in sql engine (truncate <name of table>)

#! /bin/bash

//Script to Clean files for a fresh start

sudo rm –rf /opt/graphite/storage/whisper/entrada/\*

rm /home/captures/\*

rm /home/pcap/incoming/\*

rm /home/pcap/processing/\*

rm /home/pcap/incoming/\*

rm /home/entrada-latest/tmp/DNS1-PRI-pcap-process.hist

rm /home/entrada-latest/tmp/DNS2-PRI-pcap-process.hist

rm /home/entrada-latest/tmp/DNS1-SEC-pcap-process.hist

rm /home/entrada-latest/tmp/DNS2-SEC-pcap-process.hist

**Entrada and Hue ( SQL Queries )**

“The ENTRADA data model support many types of SQL queries which can be used to a extract interesting information from the captured network data. You might be interested in resolver behavior, domain name usage or the use of certain types of DNS attributes. Here we display some example queries, below each query, we show its (fictional) result.”

1. Open [http://192.168.9.102:8889](http://192.168.9.102:8889/) in the browser
2. Enter a SQL query and click the execute button or CTRL+ENTER

For Example: to show all data for the first 50 rows enter

“ SELECT \* FROM queries LIMIT 100; ”

1. Some examples can be found in <https://entrada.sidnlabs.nl/query_examples/>

**Entrada version 2.0.3 installation**

This version use docker container.

**Requirement :**

* install docker
  + sudo yum install docker
  + sudo systemctl enable docker.service
  + sudo systemctl start docker.service
* install docker-compose
  + sudo curl -L "https://github.com/docker/compose/releases/download/1.24.1/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
  + sudo chmod +x /usr/local/bin/docker-compose
  + sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
  + check if docker-compose is working (docker-compose --version)

you should get docker-compose version 1.24.1, build 1110ad01

* install postgresql database
  + try to install the postgresql in different device
  + you can use the postgresql of cloudera but make sure its version > 9.2
  + create database call it entrada
  + create new account for example (user=entrada, pass=toor)
  + enable the connection to the postgresql from the device that have entrada
  + #edit pg\_hba.conf by adding

#host all all <ip\_of\_device>/32 trust

host all all 192.168.100.1/32 trust

**Installation :**

1. copy the file .../entrada/docker-compose/docker-compose-postgresql-hadoop.yml to another folder like ~/Desctop/docker-entrada/docker-compose-postgresql-hadoop.yml and change the name to docker-compose.yml .
2. Create these folders inside **docker-entrada**
   * input
   * output
   * archive
   * log
   * work
   * conf
3. copy core-site.xml and hdfs-site.xml to the conf dir , these are the configurations of cloudera

* cp /etc/hadoop/conf/hdfs-site.xml like ~/Desctop/docker-entrada/conf/hdfs-site.xml
* cp /etc/hadoop/conf/core-site.xml like ~/Desctop/docker-entrada/conf/core-site.xml

1. you need to change the configuration to be met for the system

**!!use IPes only, don’t use names like namenode.entrada.om because it will not work!!**

**Important configuration**

* ENTRADA\_NAMESERVERS=DNS1-PRI,DNS1-SEC,DNS2-PRI,DNS2-SEC
* SPRING\_DATASOURCE\_USERNAME=<user of postgresql: you can use **postgres**>
* SPRING\_DATASOURCE\_PASSWORD=<password of postgres>
* SPRING\_DATASOURCE\_URL=postgresql://<host\_or\_ip>:5432/entrada
* HDFS\_NAMESERVICE\_HOST=<ip of HDFS>
* IMPALA\_DAEMON\_HOST=<ip of impala>
* ENTRADA\_LOCATION\_OUTPUT=hdfs://<ip of HDFS >:8020/user/entrada/database

also you need to enable graphite because it is disabled by default

* MANAGEMENT\_METRICS\_EXPORT\_GRAPHITE\_ENABLED=true
* MANAGEMENT\_METRICS\_EXPORT\_GRAPHITE\_HOST=<graphite host>

for more configurations detail see <https://entrada.sidnlabs.nl/about/configuration/>

**Start Entrada:**

1. go to the directory where docker-compose.yml is located and run the following command

* sudo docker-compose up

1. solve the problems if any
2. start feeding entrada
   * create folder for each server in input directory
     + DNS1-PRI,DNS2-PRI,….
   * Send pcap files to these folders with this name format to avoid any problem

SERVER\_year-month-day\_hour:min.pcap (DNS1-PRI\_2019-5-10\_20:55.pcap )

**Graphite docker:**

* There is graphite docker image, you can install docker image instead of local graphite

sudo docker run -d\

--name graphite\

--restart=always\

-p 8080:80\

-p 2003-2004:2003-2004\

-p 2023-2024:2023-2024\

-p 8125:8125/udp\

-p 8126:8126\

-v "/opt/graphite/conf:/opt/graphite/conf"\

-v "/opt/graphite/storage:/opt/graphite/storage"\

graphiteapp/graphite-statsd

* To restart graphite
  + sudo docker start -a graphite

**Grafana docker:**

* There is grafana docker image, you can install docker image instead of local Grafana

sudo docker run \

-d \

-p 3000:3000 \

--name=grafana \

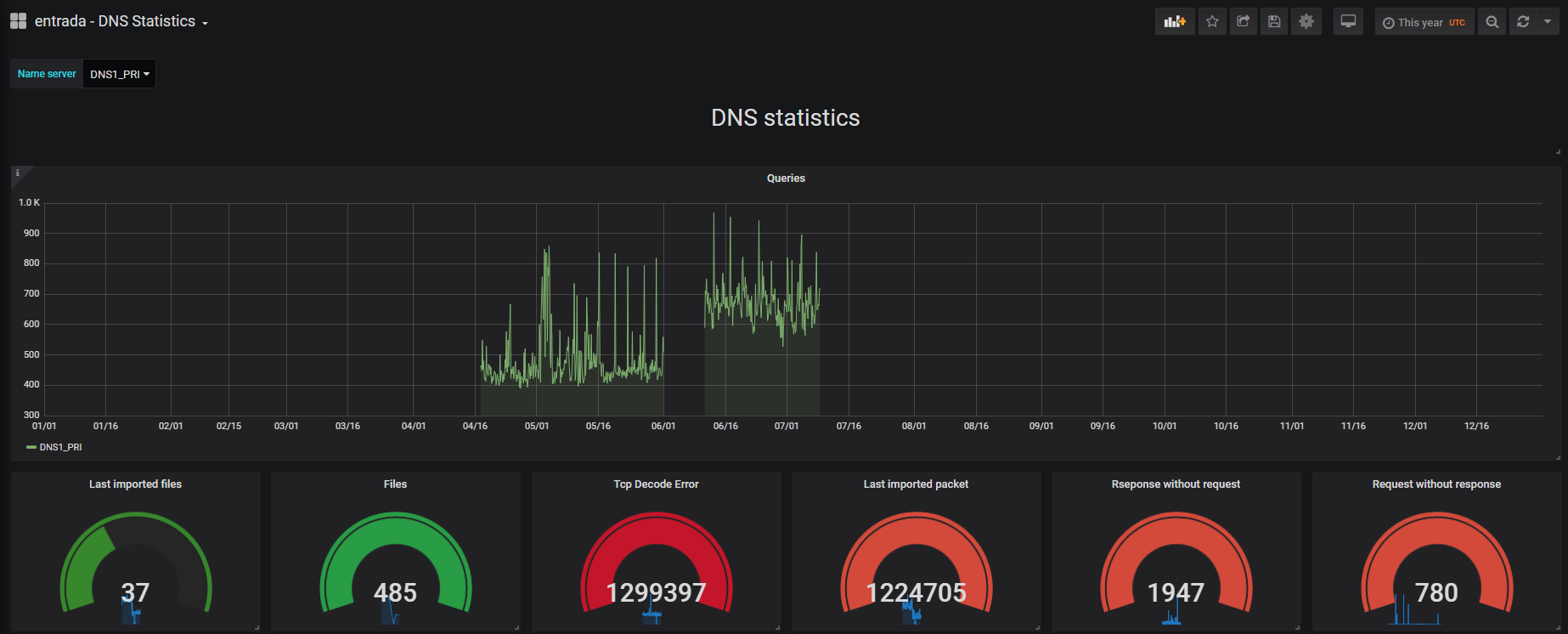
--restart=always\

-e "GF\_INSTALL\_PLUGINS=grafana-clock-panel,grafana-simple-json-datasource,grafana-worldmap-panel" \

grafana/Grafana

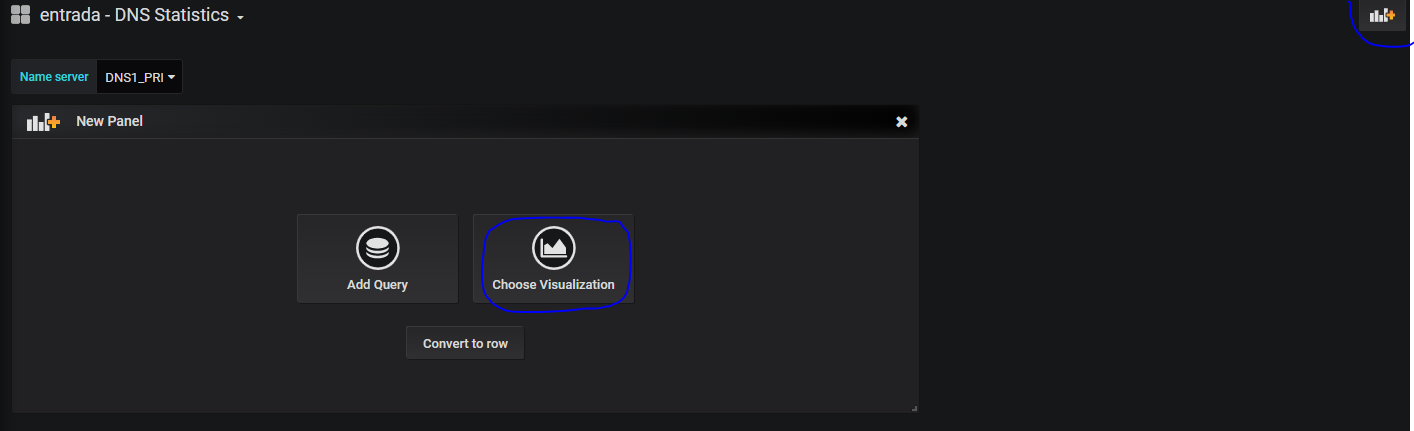
* To restart Grafana
  + docker start -a grafana

**Grafana**



Example: How to add new plot in Grafana

This explains how to add new widget in Grafana in steps;



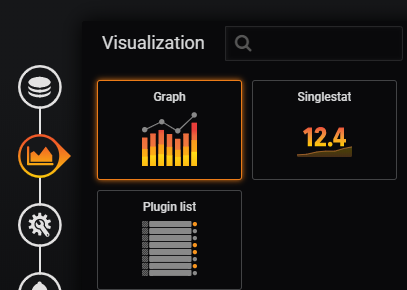
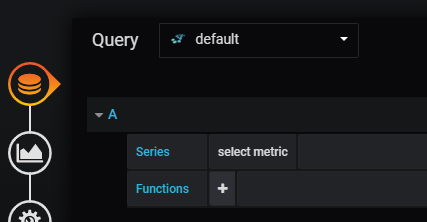


Figure 1:Add Query for DNS1\_PRI

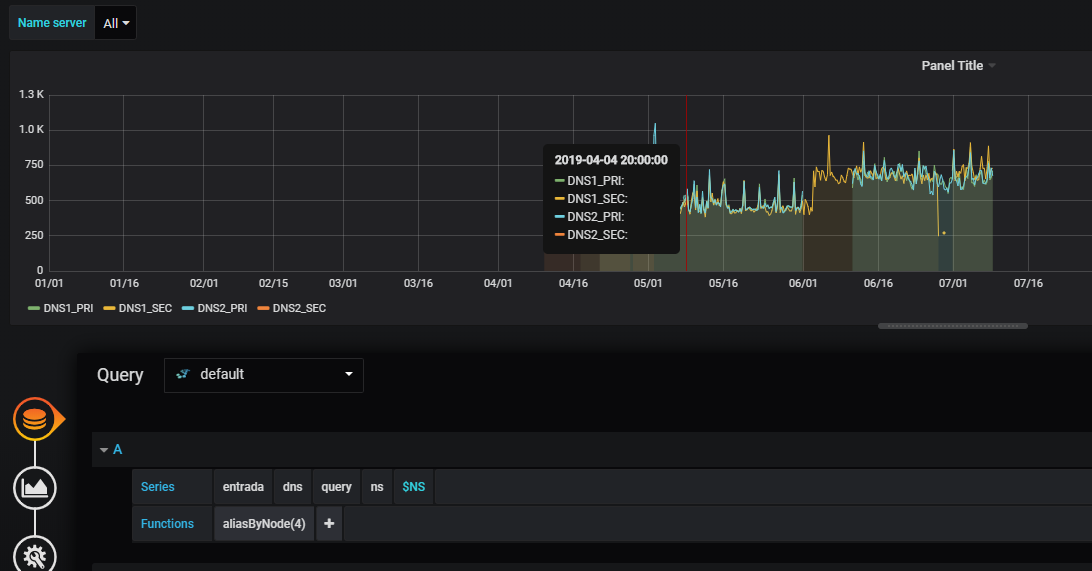
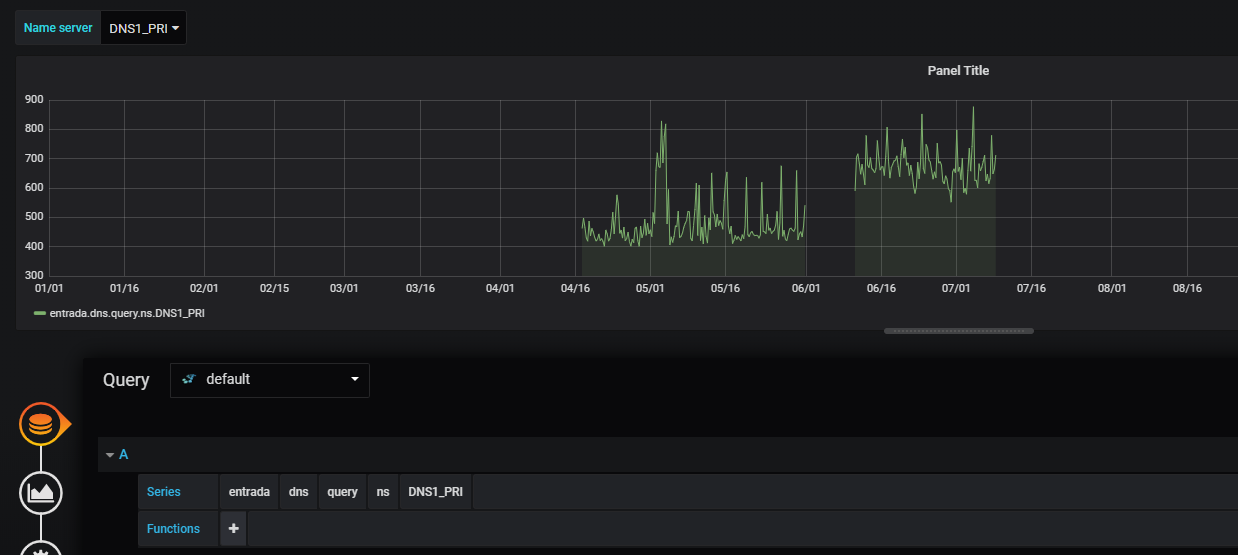
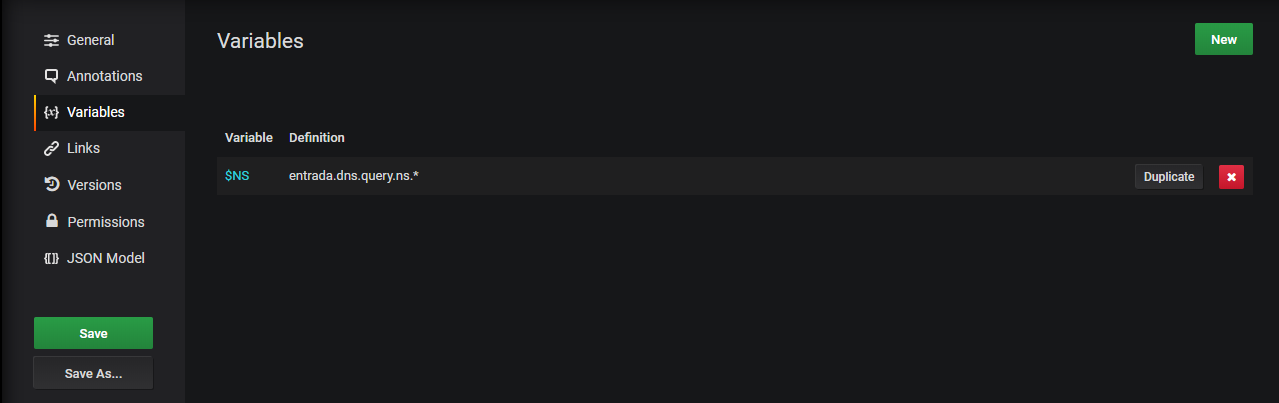
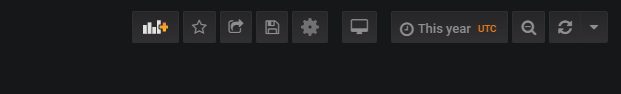
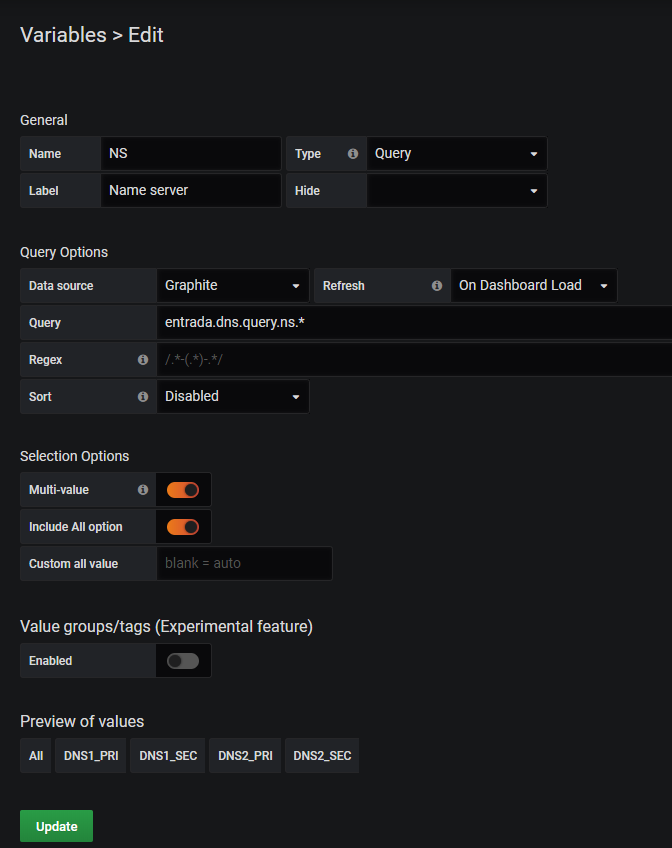
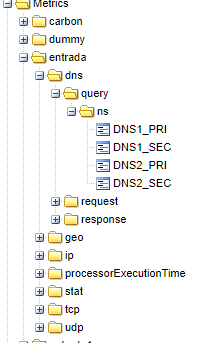


Figure 2: Add Query by adding Variable for Name server

Example: How to add variable in Grafana as shown in previous example..





Name: here add the name of the variable

Label: here add the label of variable that shown in the top left of the page.

Query: you can write any query that have the names of servers in graphite.

**Code**

version: '3.7'

services:

entrada:

image: sidnlabs/entrada:ali # **ali** is the tag of modified version

restart: always

ports:

- 8083:8080

environment:

# ENTRADA options

- ENTRADA\_NAMESERVERS=DNS1-PRI,DNS1-SEC,DNS2-PRI,DNS2-SEC

# PostgreSQL config options, make sure the the database is created before

# starting the container

# replace <host\_or\_ip> with the actual host of ip, do not use localhost

- SPRING\_DATASOURCE\_URL=jdbc:postgresql://192.168.100.3:5432/entrada

- SPRING\_DATASOURCE\_DRIVER\_CLASS\_NAME=org.postgresql.Driver

- SPRING\_DATASOURCE\_USERNAME=entrada

- SPRING\_DATASOURCE\_PASSWORD=toor

- SPRING\_JPA\_DATABASE\_PLATFORM=org.hibernate.dialect.PostgreSQLDialect

# Hadoop ( copy core-site.xml and hdfs-site.xml to the conf dir)

- HDFS\_NAMESERVICE\_HOST=192.168.100.1

- IMPALA\_DAEMON\_HOST=192.168.100.5

- ENTRADA\_LOCATION\_OUTPUT=hdfs://192.168.100.1:8020/user/entrada/database

- HDFS\_USERNAME=hdfs

# grphite

- MANAGEMENT\_METRICS\_EXPORT\_GRAPHITE\_ENABLED=true

- MANAGEMENT\_METRICS\_EXPORT\_GRAPHITE\_HOST=192.168.100.1

- MANAGEMENT\_METRICS\_EXPORT\_GRAPHITE\_PORT=2003

- MANAGEMENT\_METRICS\_EXPORT\_GRAPHITE\_PREFIX=entrada

# The following options do NOT need to be changed

# change the volume mappings below, in the "volumes:" section

- ENTRADA\_ENGINE=hadoop

- JAVA\_OPTS=-Xmx4g -Xms4g

# Map internal container path to a path on the host

# format <host-path>:<container:path>

# ENTRADA will write to /entrada/... in the container

volumes:

- ./:/entrada/data/

dns:

- 8.8.8.8

#Limit container logging

logging:

options:

max-size: "10m"

max-file: "3"

note: this version is modified from version **entrada 2.0.10** to display some statistics ,This version is called **ali ,** if you change the version to newer one , you will not be able to get the statistics.