Proyecto GAR

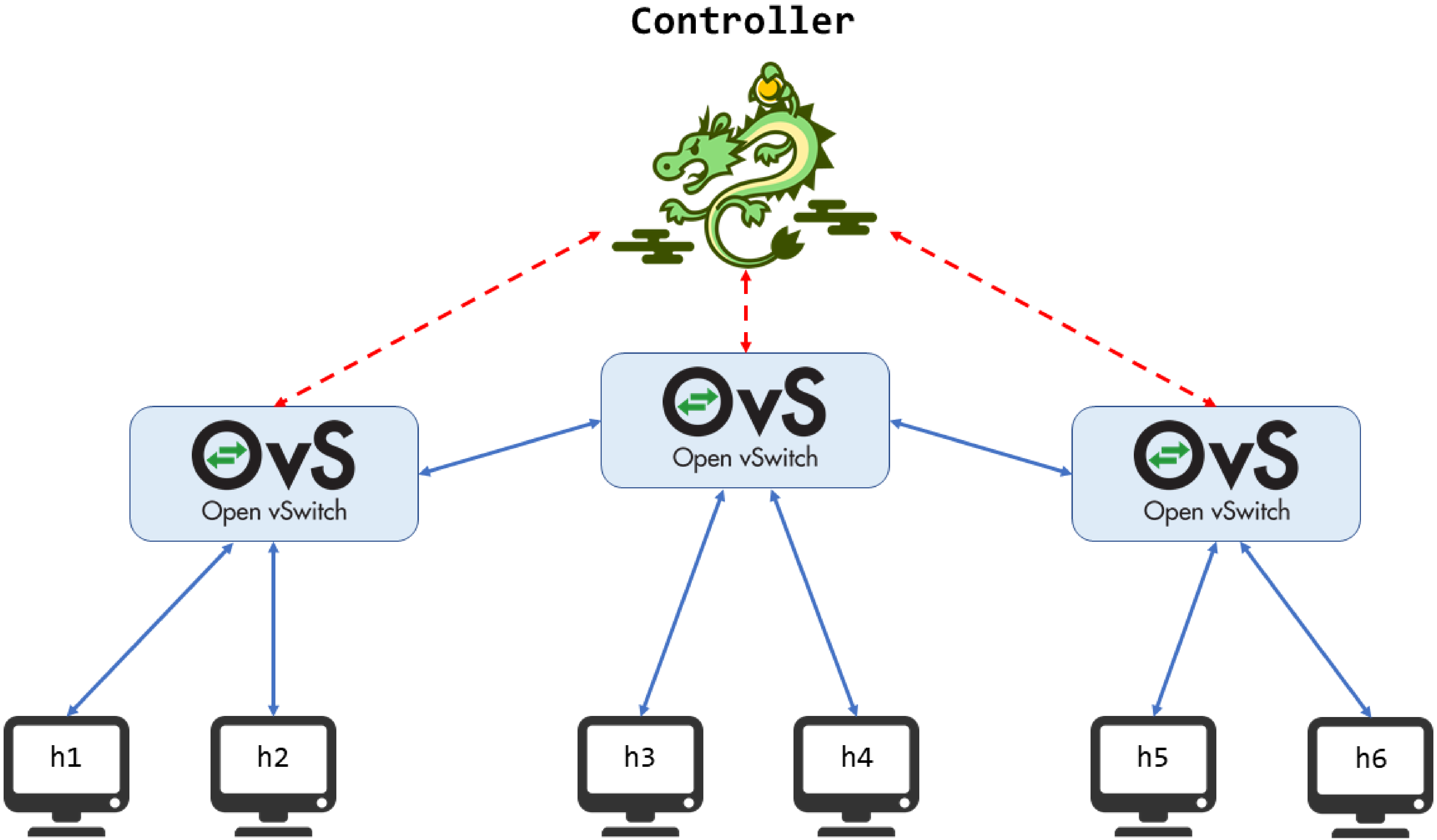
Índice

- **Escenario**
  - Escenario a bajo nivel
- **Herramientas y colectores de datos**
- **Ataque**
- **IA esquema**
  - IA clasificación
- **Grafana**

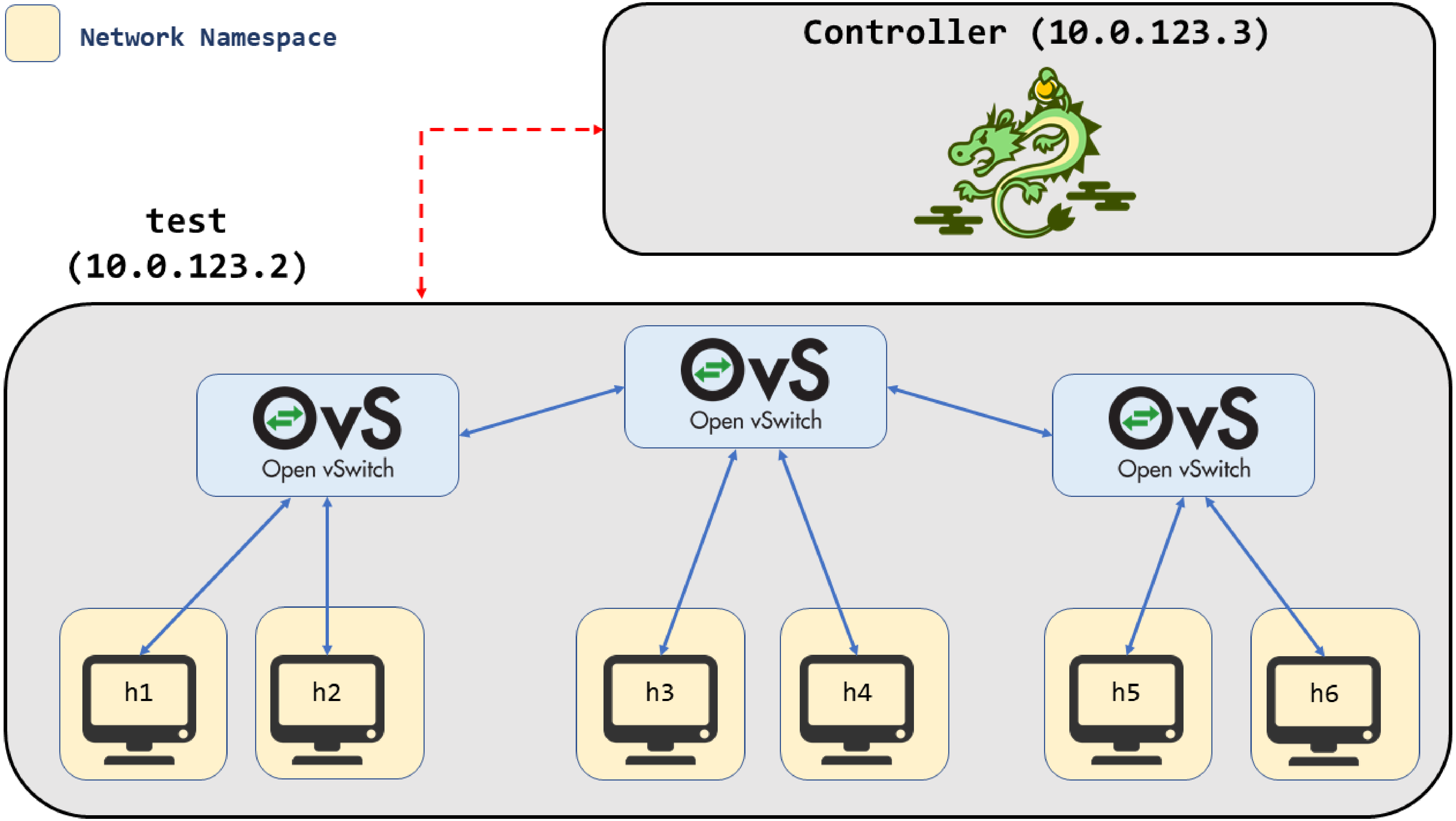
GAR-Project

gar-project.github.io/project

Escenario


Controller
Open vSwitch
Open vSwitch
Open vSwitch
h1
h2
h3
h4
h5
h6

Escenario a bajo nivel



🟨 Network Namespace

Controller (10.0.123.3)

test
(10.0.123.2)

Open vSwitch

Open vSwitch

Open vSwitch

h1

h2

h3

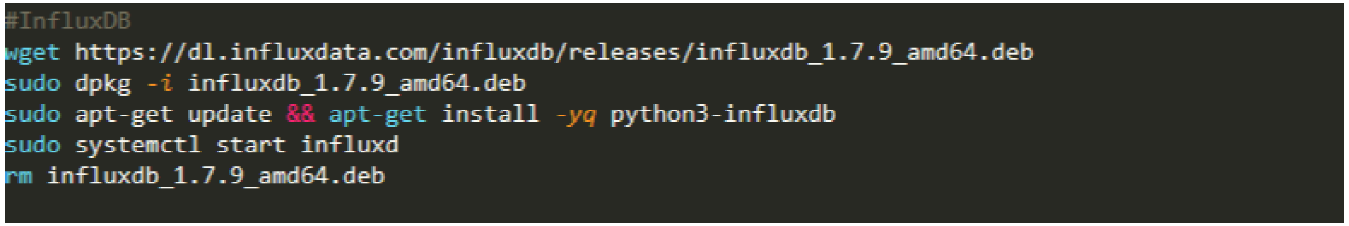
h4

h5

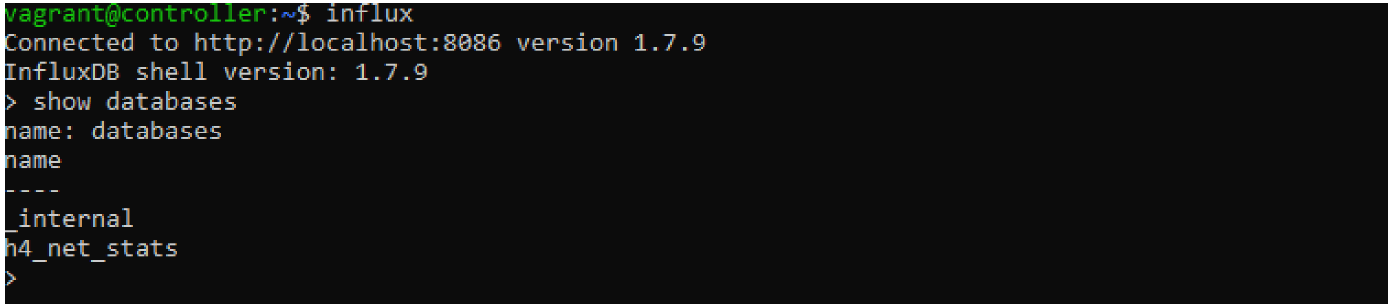
h6

Tools and Data colllector

influxdb

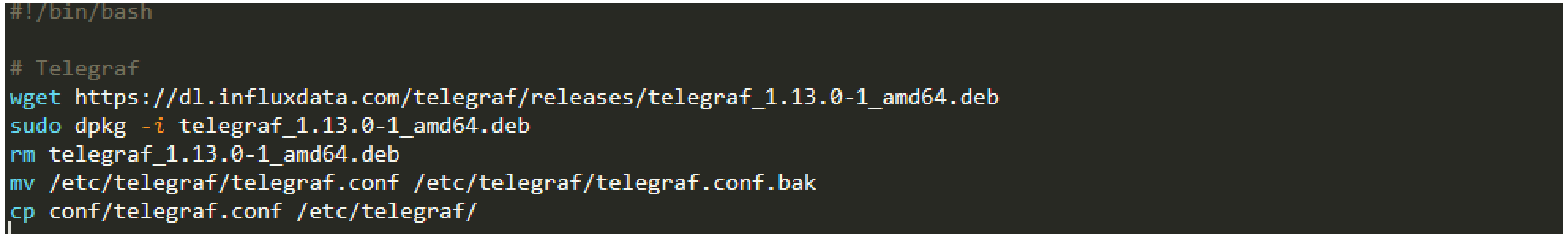


```
#InfluxDB
wget https://dl.influxdata.com/influxdb/releases/influxdb_1.7.9_amd64.deb
sudo dpkg -i influxdb_1.7.9_amd64.deb
sudo apt-get update && apt-get install -yq python3-influxdb
sudo systemctl start influxd
rm influxdb_1.7.9_amd64.deb
```



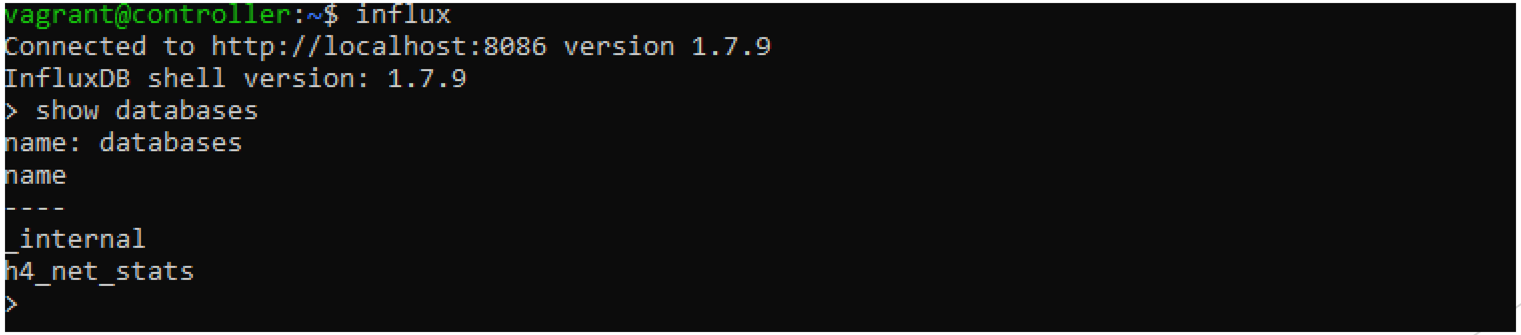
```
vagrant@controller:~$ influx
Connected to http://localhost:8086 version 1.7.9
InfluxDB shell version: 1.7.9
> show databases
name: databases
name
----
_internal
h4_net_stats
>
```

telegraf™



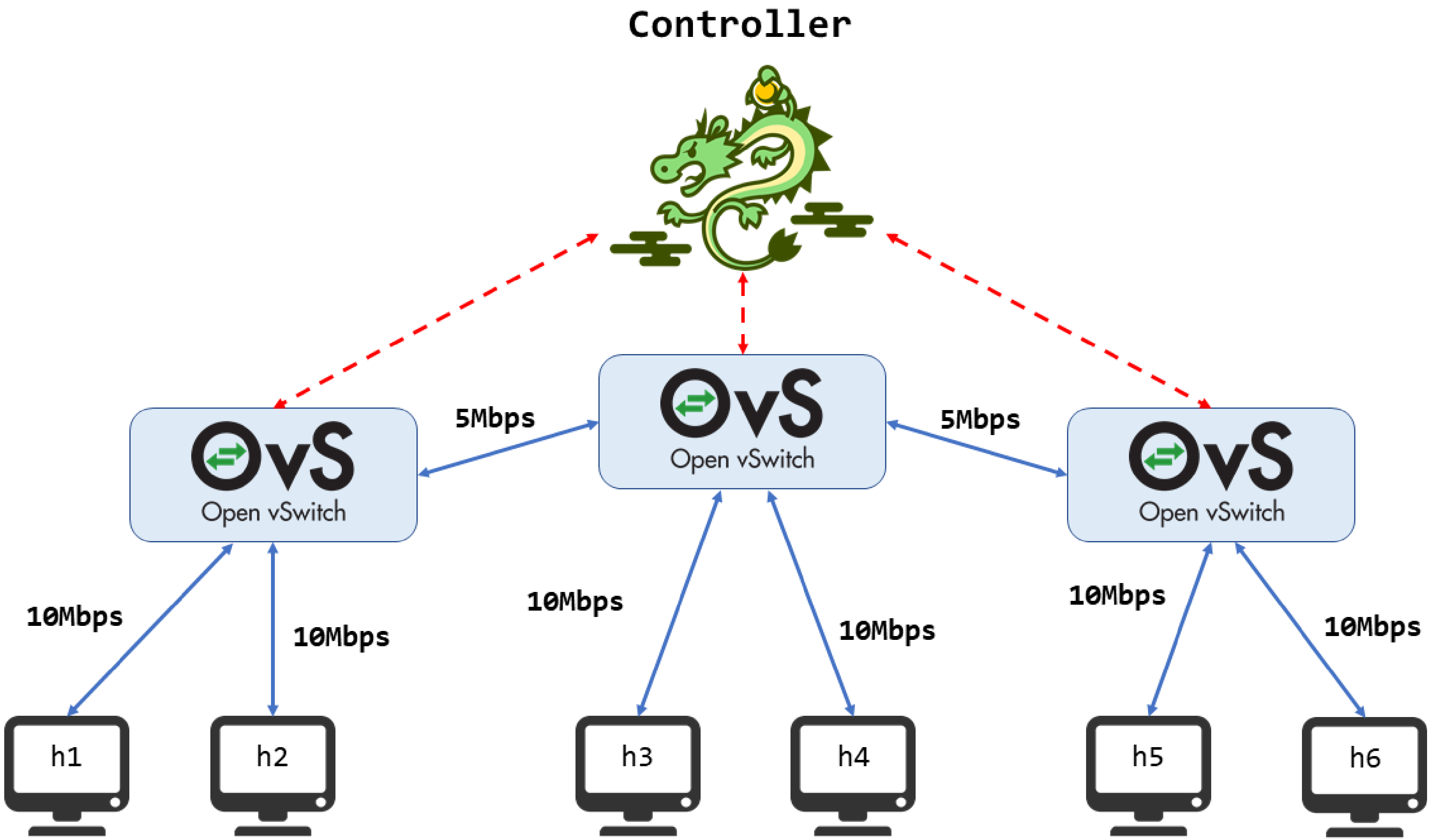
```
#!/bin/bash

# Telegraf
wget https://dl.influxdata.com/telegraf/releases/telegraf_1.13.0-1_amd64.deb
sudo dpkg -i telegraf_1.13.0-1_amd64.deb
rm telegraf_1.13.0-1_amd64.deb
mv /etc/telegraf/telegraf.conf /etc/telegraf/telegraf.conf.bak
cp conf/telegraf.conf /etc/telegraf/
```



```
vagrant@controller:~$ influx
Connected to http://localhost:8086 version 1.7.9
InfluxDB shell version: 1.7.9
> show databases
name: databases
name
----
_internal
h4_net_stats
>
```

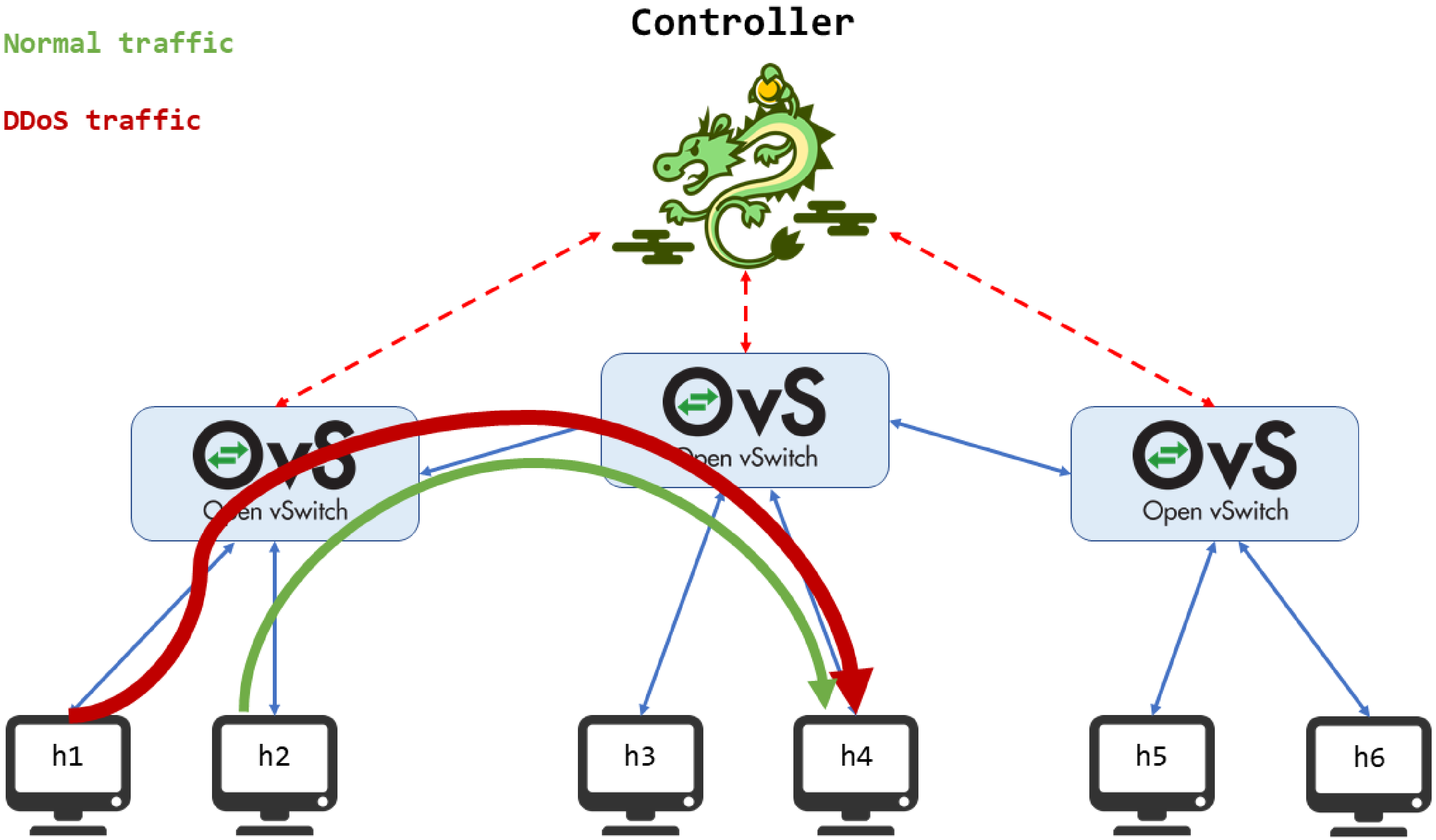
Ataque


Controller
Open vSwitch
Open vSwitch
Open vSwitch
5Mbps
5Mbps
10Mbps
10Mbps
10Mbps
10Mbps
10Mbps
10Mbps
h1
h2
h3
h4
h5
h6

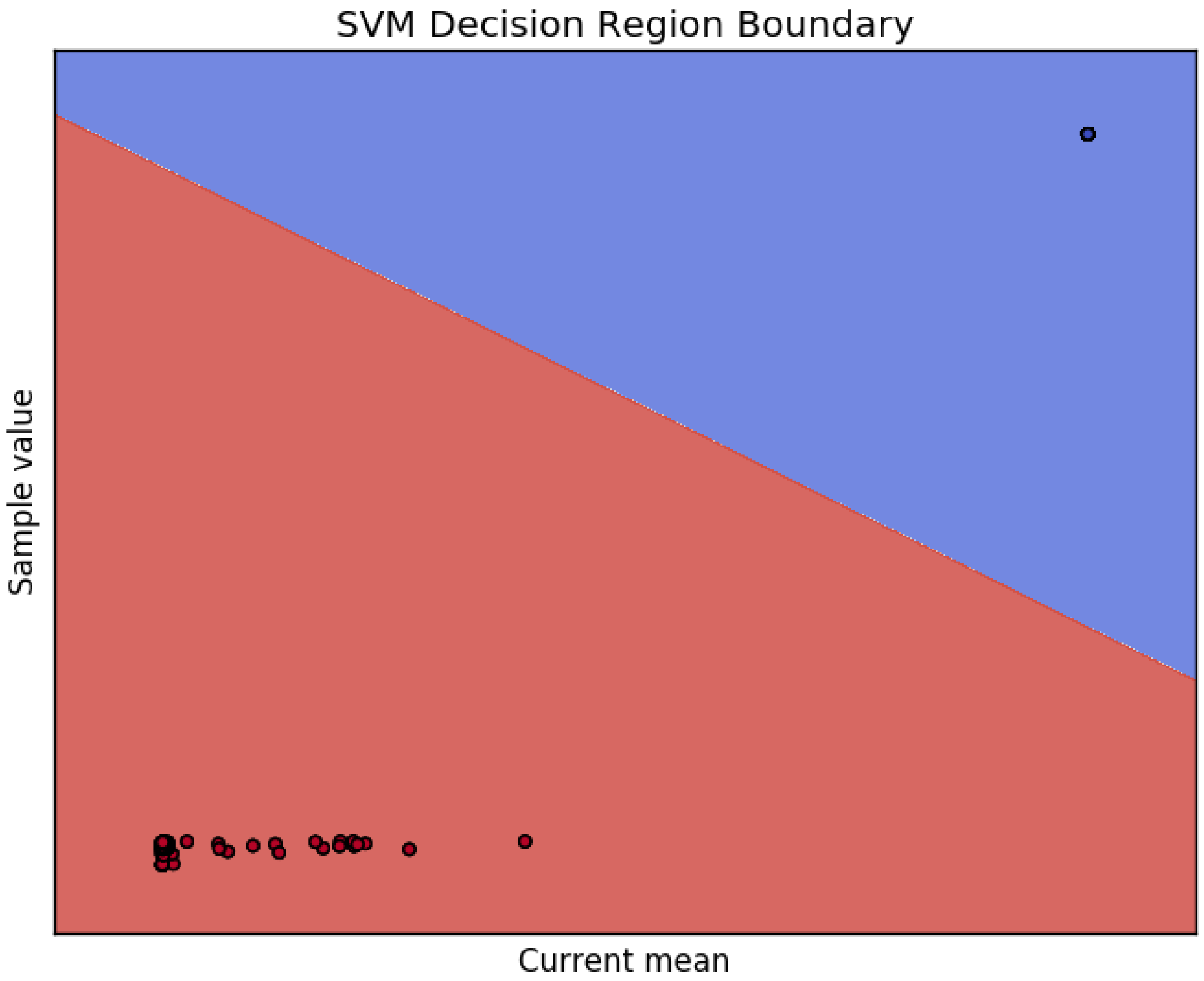
Ataque (II)

🟩 Normal traffic

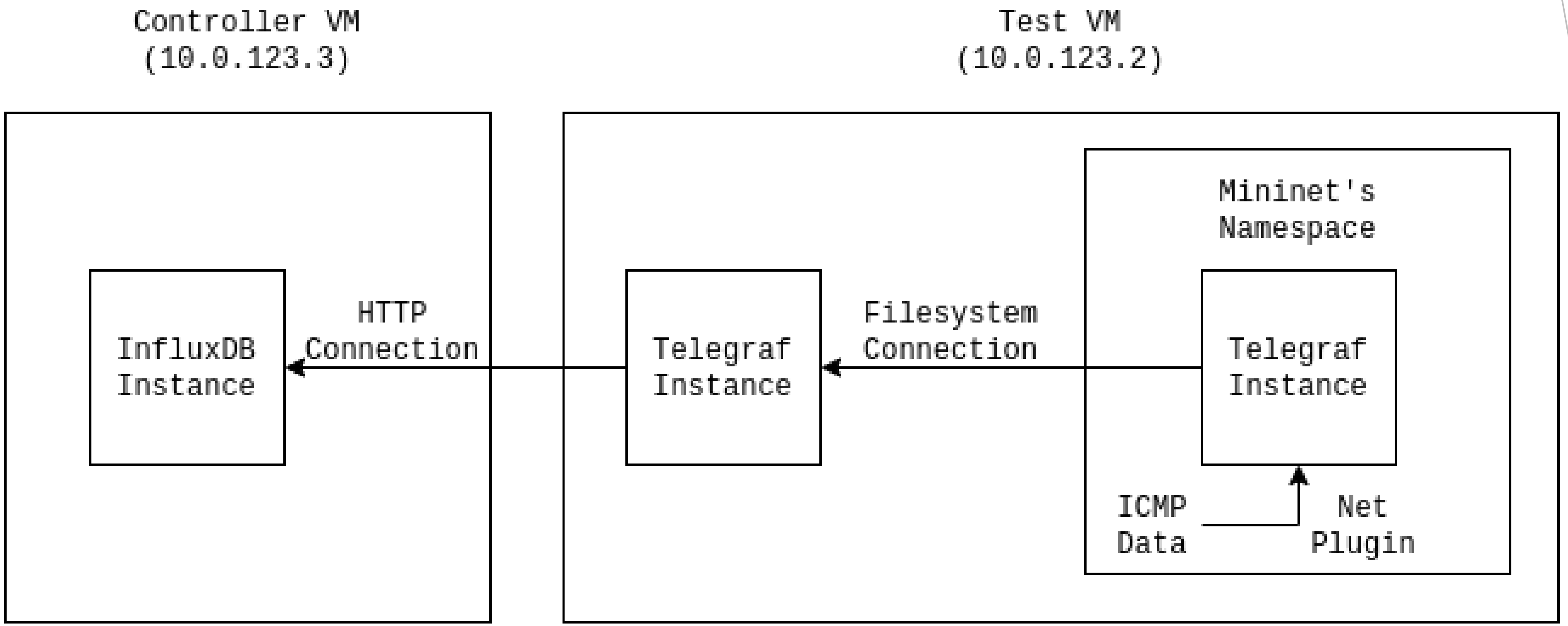
🟥 DDoS traffic



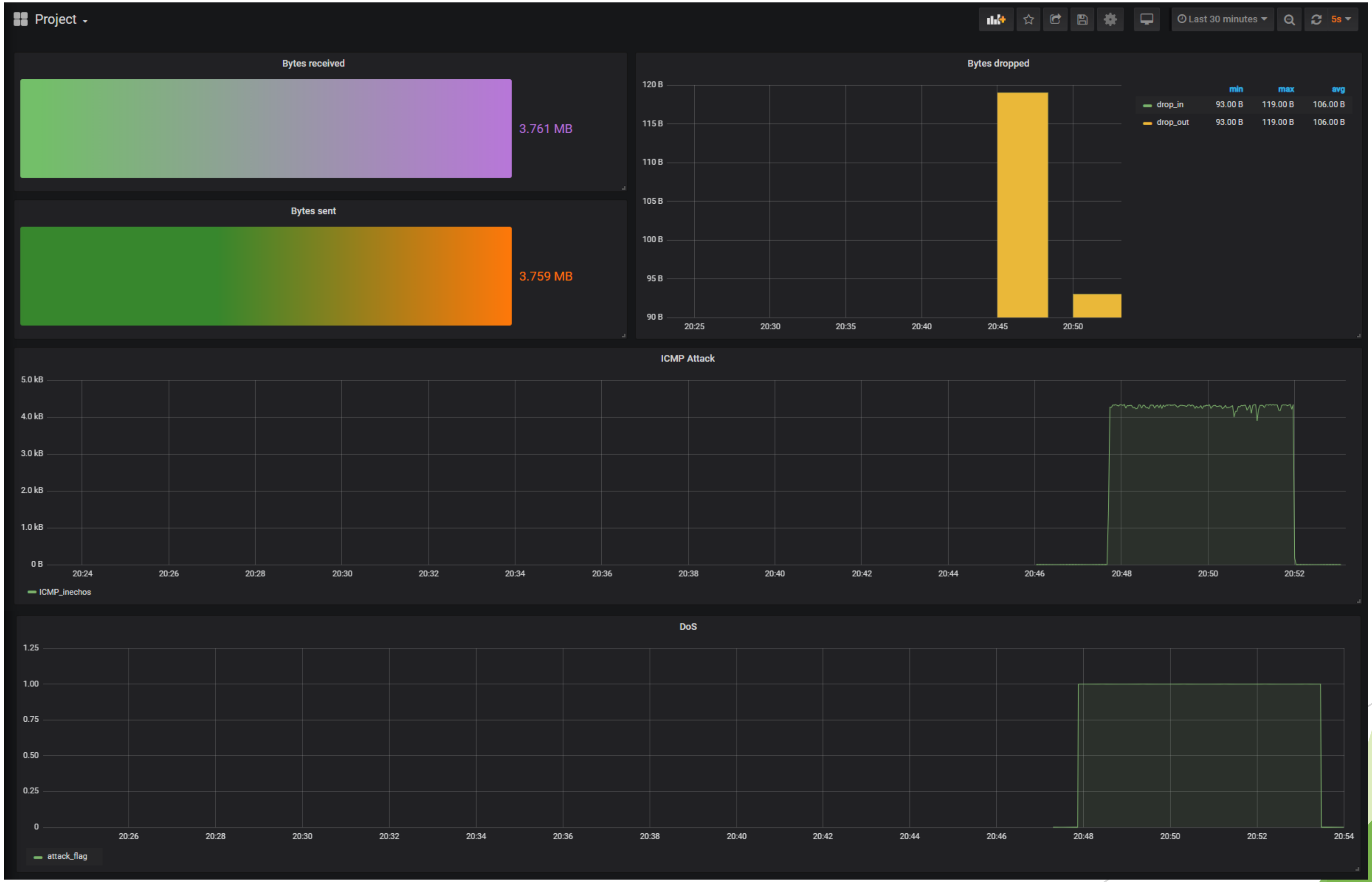
Pinceladas de las SVMs



¡A por esos datos!

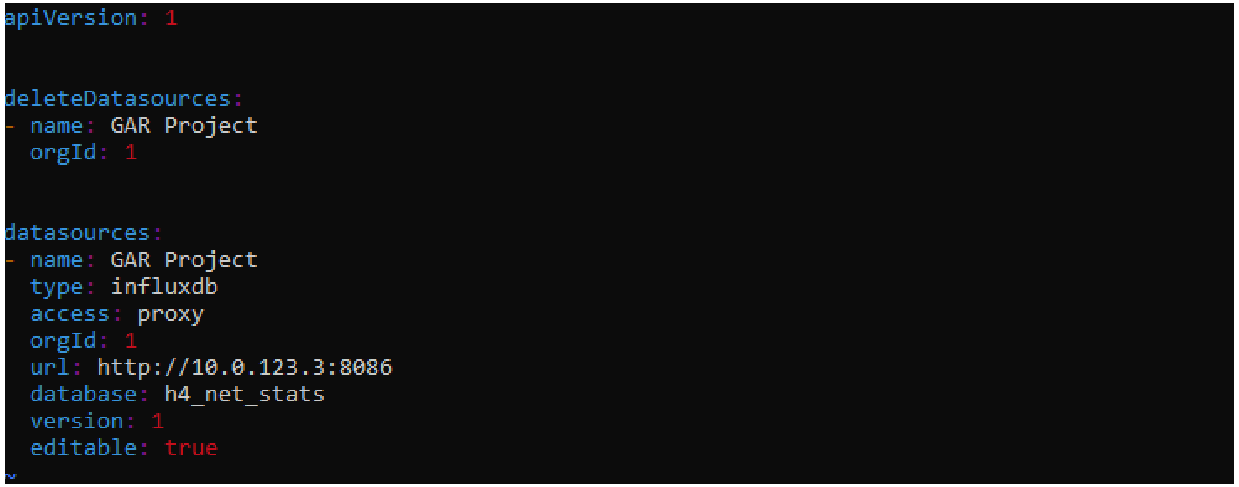


Grafana



	min	max	avg
🟩 drop_in	93.00 B	119.00 B	106.00 B
🟨 drop_out	93.00 B	119.00 B	106.00 B

Datasource

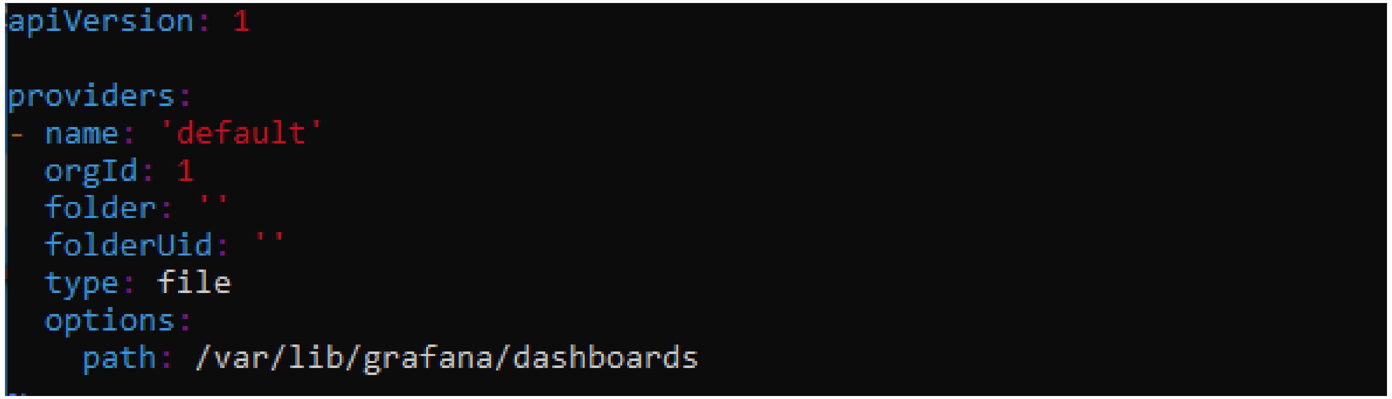


```
apiVersion: 1


deleteDatasources:
- name: GAR Project
  orgId: 1


datasources:
- name: GAR Project
  type: influxdb
  access: proxy
  orgId: 1
  url: http://10.0.123.3:8086
  database: h4_net_stats
  version: 1
  editable: true
~
```

Dashboard



```
apiVersion: 1

providers:
- name: 'default'
  orgId: 1
  folder: ''
  folderUid: ''
  type: file
  options:
    path: /var/lib/grafana/dashboards
```