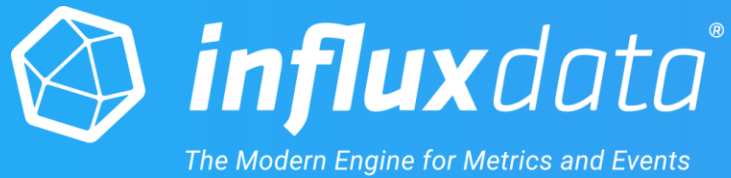
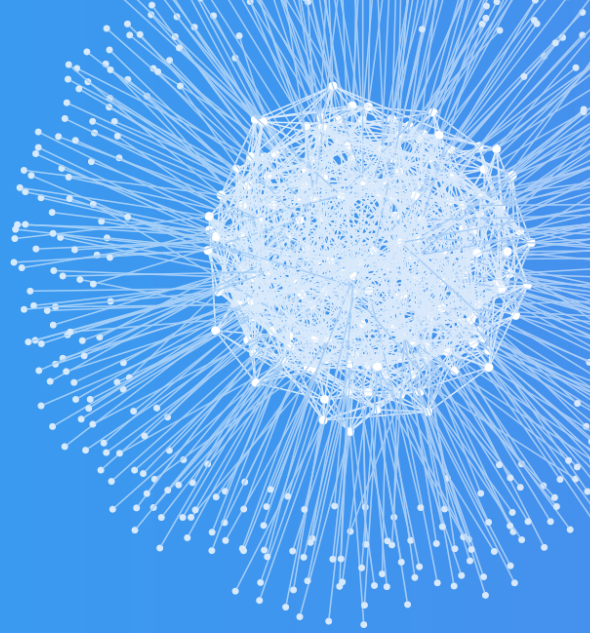
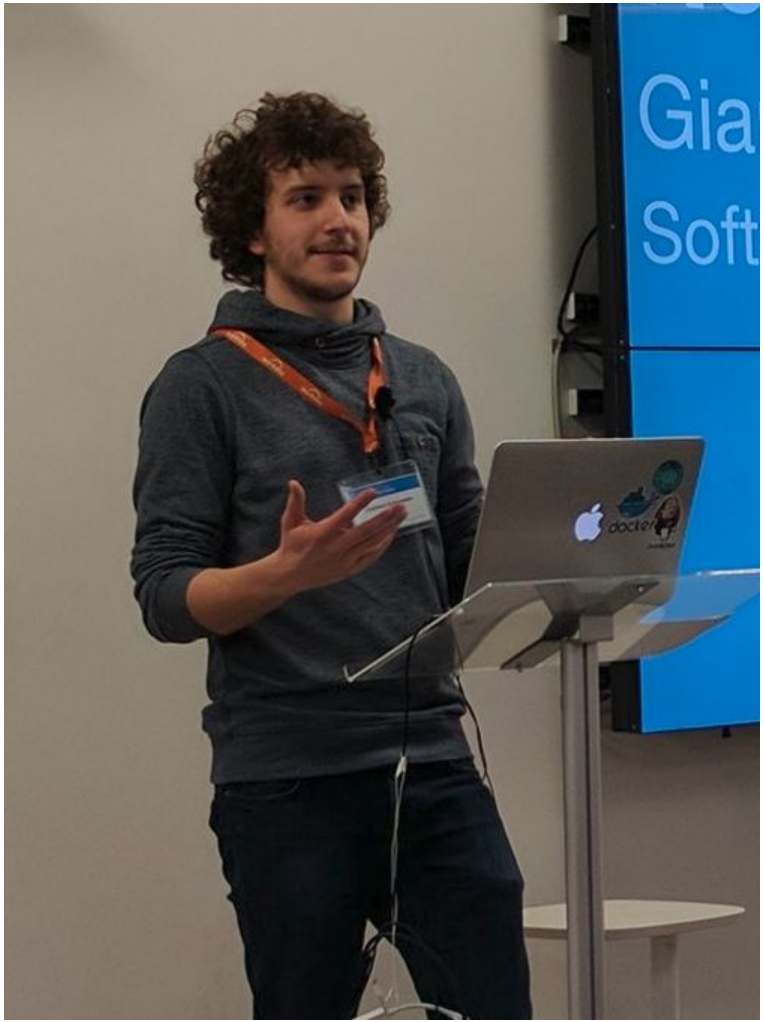




The network is a (great) signal

Gianluca Arbezzano, SRE at InfluxData



Gianluca Arbezzano
Site Reliability Engineer @InfluxData

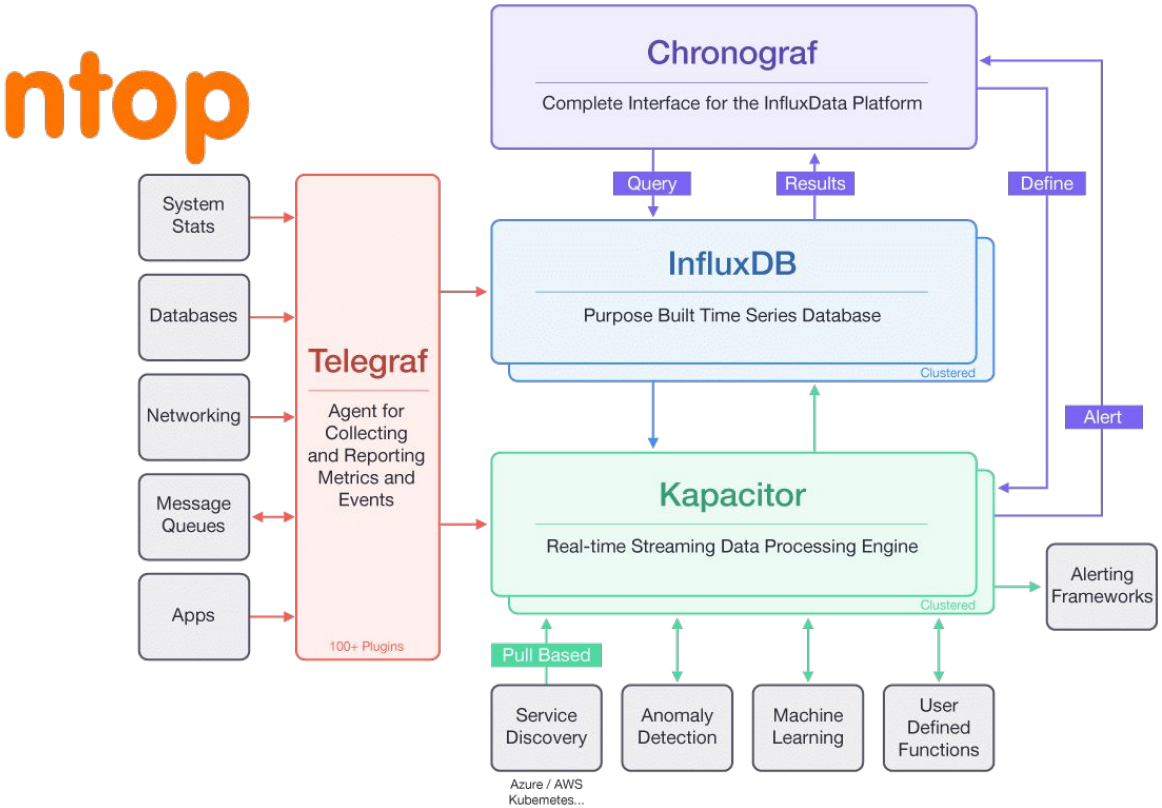
- https://gianarb.it
- @gianarb

What I like:

- I make dirty hacks that look awesome
- I grow my vegetables 🍅🌻🍆
- Travel for fun and work

@gianarb - gianluca@influxdb.com

@gianarb - gianluca@influxdb.com



Ntopng workflow

same network namespace

ntop uses as identifier IPs, in our case the containers IP. But I would like to correlate by hostname and environment as well

telegraf as proxy add those tags for every points.

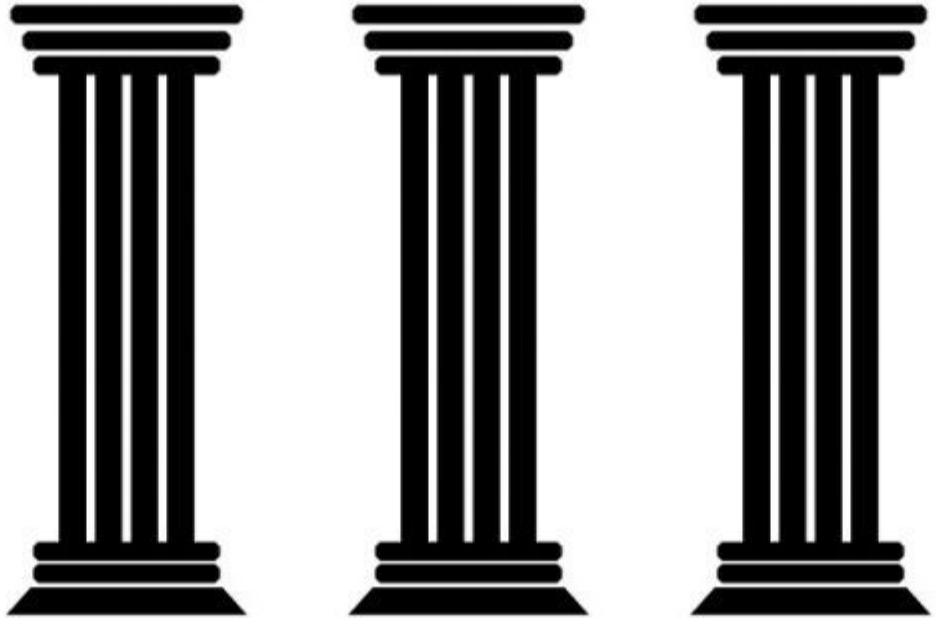
```
[global_tags]
     env = "$ENV"
     hostname = "$HOSTNAME"
```

Zoom

Customers never called me because they experienced too many packet loss.

We need tools that helps us observe a system

Metrics Traces Logs

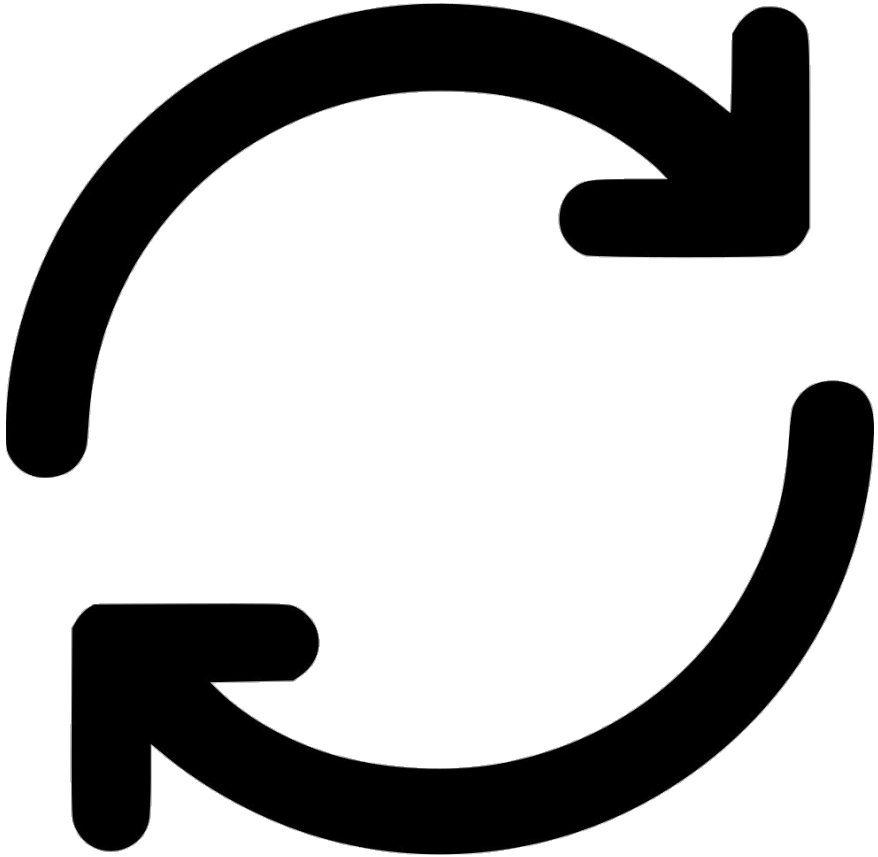


Metric

ntop

Logs

Traces



We need “centralization”

~~Data centralization is not what we need~~

We need to build and enreach a context

Aggregation

Flux Language Elements

```
// get all data from the telegraf db
from(bucket:”telegraf/autogen”)
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

Comments

```
// get all data from the telegraf db
from(bucket:”telegraf/autogen”)
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

Named Arguments

```
// get all data from the telegraf db
from(bucket:”telegraf/autogen”)
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

String Literals

```
// get all data from the telegraf db
from(bucket:”telegraf/autogen”)
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

Buckets, not DBs

```
// get all data from the telegraf db
from(bucket:”telegraf/autogen”)
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

```
// get all data from the telegraf db
from(bucket:"telegraf/autogen")
  // filter that by the last hour
  |> range(start: -1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

Duration Literal

```
// get all data from the telegraf db
from(bucket:"telegraf/autogen")
  // filter that by the last hour
  |> range(start: 2018-11-07T00:00:00Z)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

Time Literal

```
// get all data from the telegraf db
from(bucket:"telegraf/autogen")
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

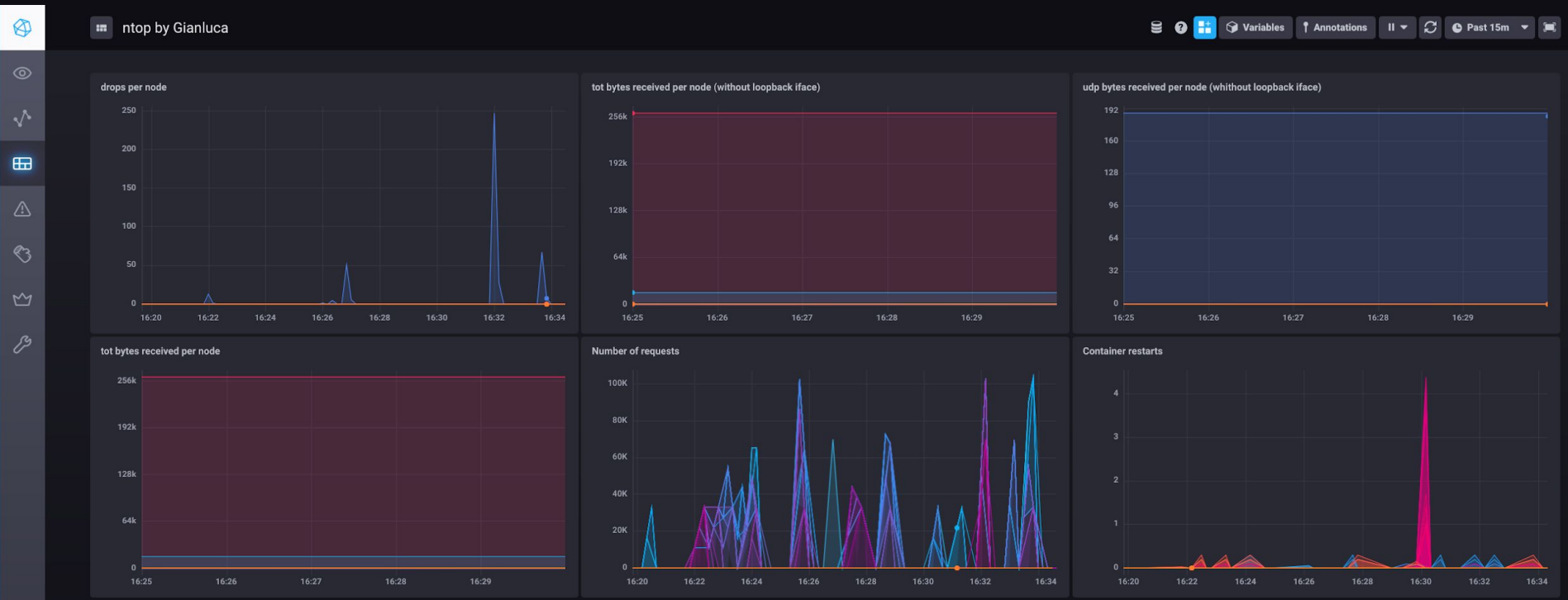
Pipe forward operator

```
// get all data from the telegraf db
from(bucket:"telegraf/autogen")
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => r._measurement == "cpu" and r._field == "usage_system")
```

Anonymous Function

```
// get all data from the telegraf db
from(bucket:"telegraf/autogen")
  // filter that by the last hour
  |> range(start:-1h)
  // filter further by series with a specific measurement and field
  |> filter(fn: (r) => (r._measurement == "cpu" or r._measurement == "cpu")
                  and r.host == "serverA")
```

Predicate Function



Network is a solid concept

Network is made by the same principles. There are IPs and flows. But the perception about how it works is way different if look at:

- Bare metal in your own datacenter
- Cloud Computing
- Containers and Kubernetes

Tools needs to give us the ability to understand the network of where we are and vice versa.

Community is the unique solution.

Share your experience
Learn from somebody else

Any question?

Reach out:
@gianarb
gianluca@influxdb.com
https://gianarb.it