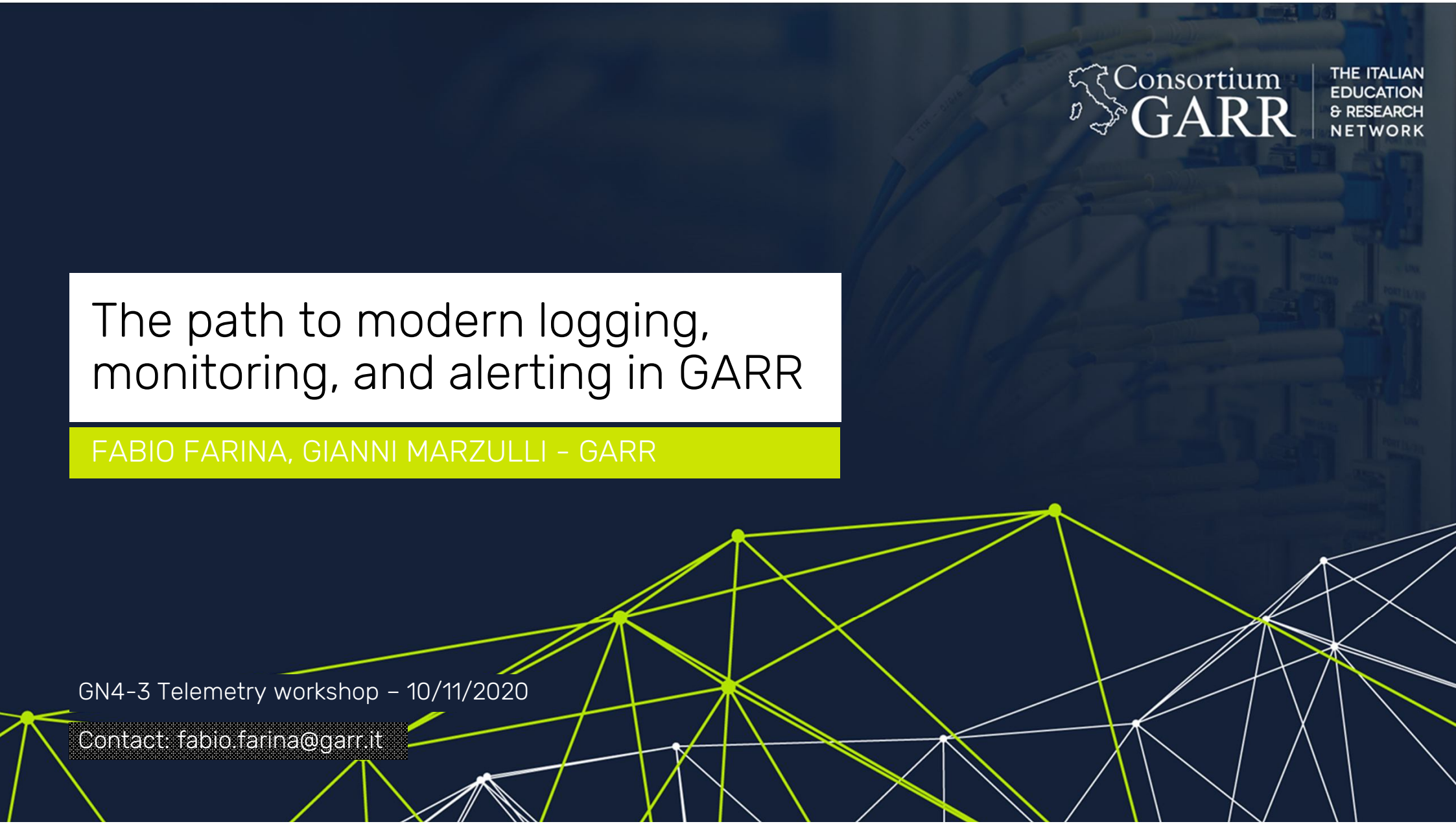


The path to modern logging, monitoring, and alerting in GARR

FABIO FARINA, GIANNI MARZULLI - GARR

GN4-3 Telemetry workshop – 10/11/2020

Contact: fabio.farina@garr.it

Outline

"When you cannot measure it,
your knowledge is of a meagre and unsatisfactory kind"
Lord William Thomson Kelvin

Overview on telemetry usage at GARR

> A brief history

> Current model, tools and strategy

> Future directions

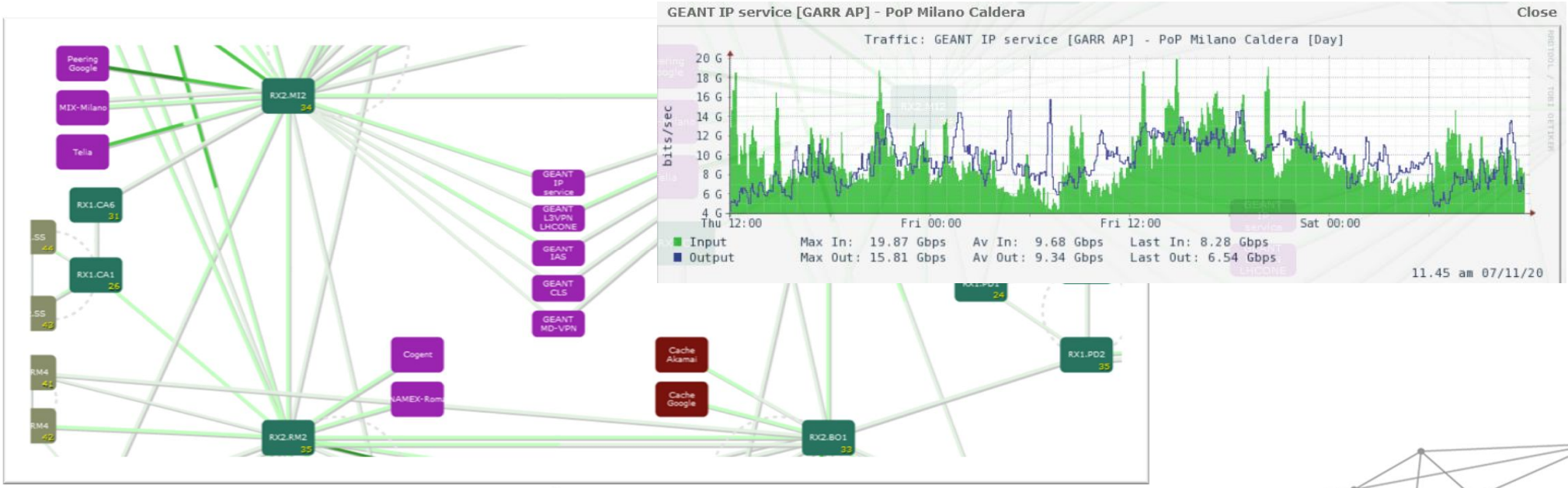
Once upon a time

Since the beginning

> GINS monitoring system

> ad hoc GARR custom development

> weather maps, RRD, SNMP, counters

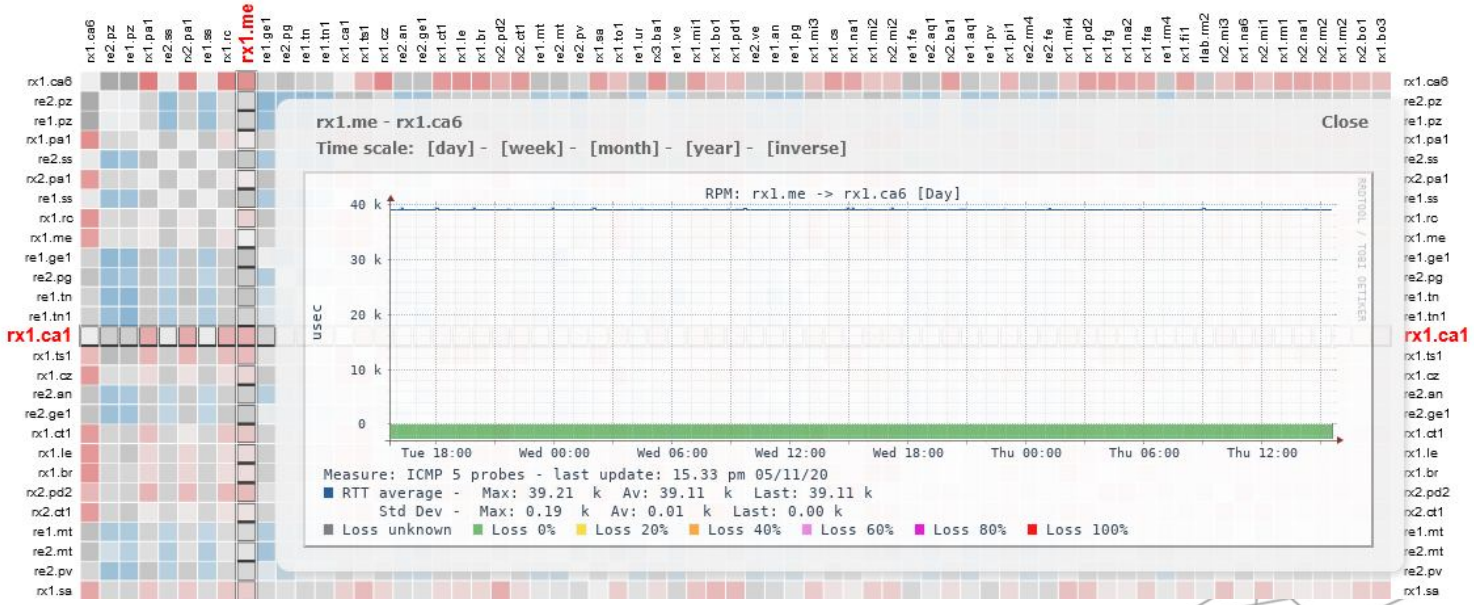


Once upon a time

~2017 – Early days

> Juniper RPM for RTT monitoring

> InfluxDB & custom visualization



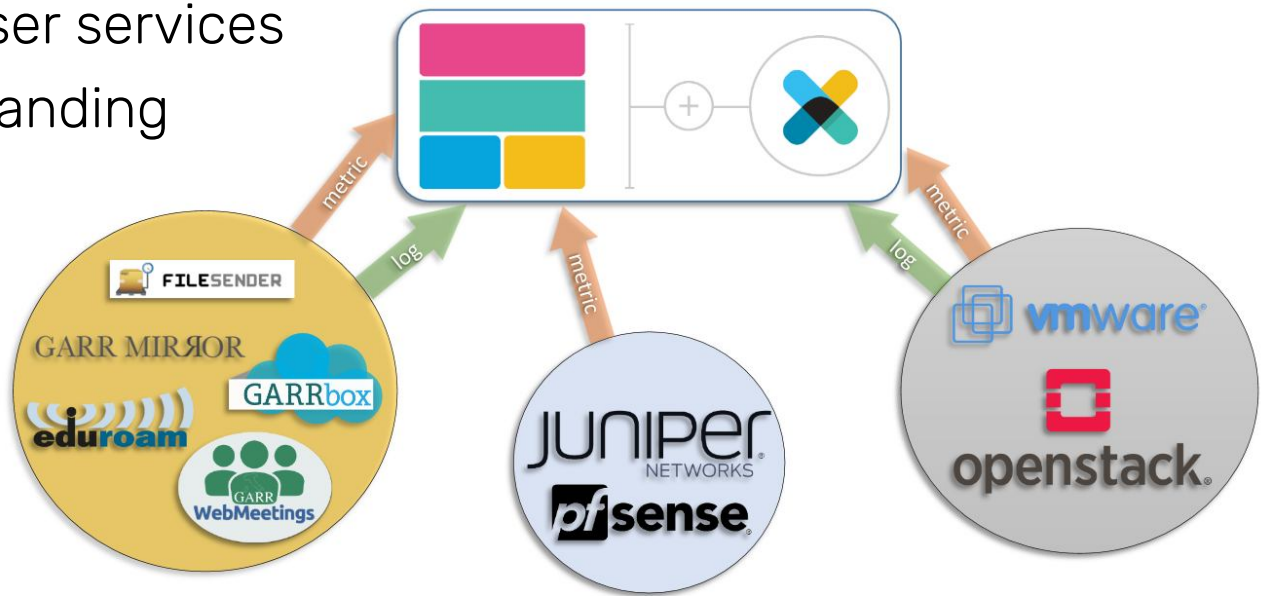
Time goes by

2018 – Elastic.com PoC

> Log centralization exercise

> DC, network & end-user services

> Learning and understanding



Till more recent time

Late 2018 – Set mid-term goals

> Transition to production

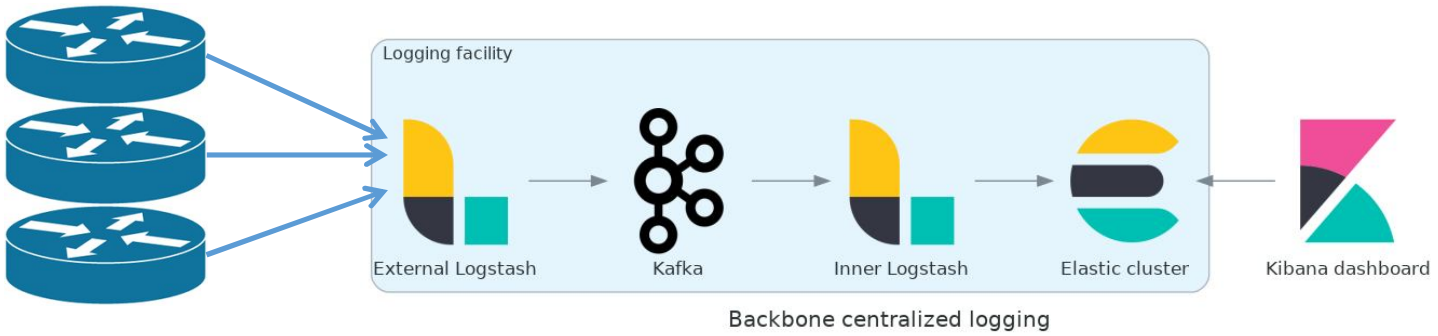
> Standardize monitoring tools and processes

> Harmonize with GARR automation methodology

2019 – Backbone central logging facility

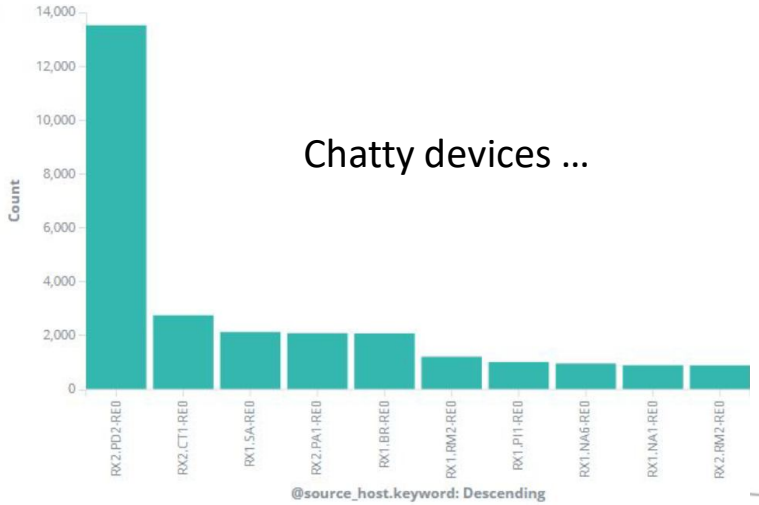
2020 – Telemetry model and tools consolidation

Backbone routers logging facility

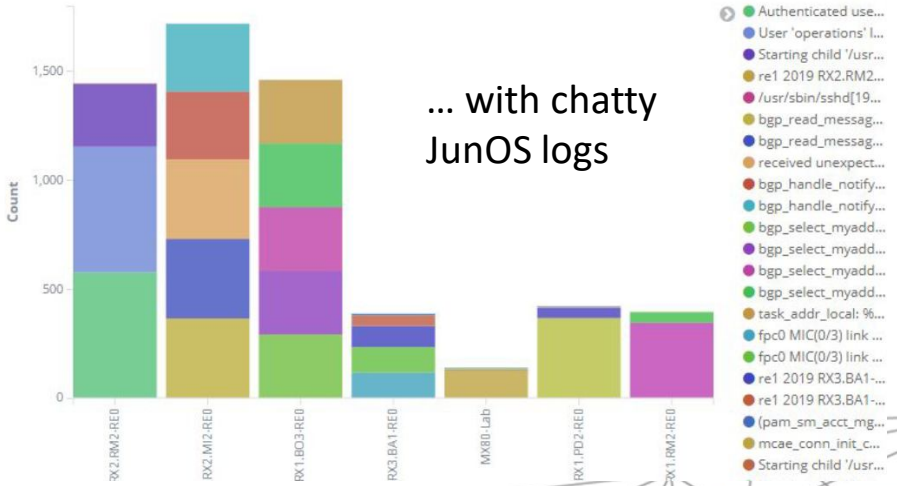


«No garbage in!»

4 hours to setup the platform, 2 weeks to clean up the data (mid July 2019)



Chatty devices …



… with chatty JunOS logs

Backbone logging

Whole network daily index size after data pipeline optimization

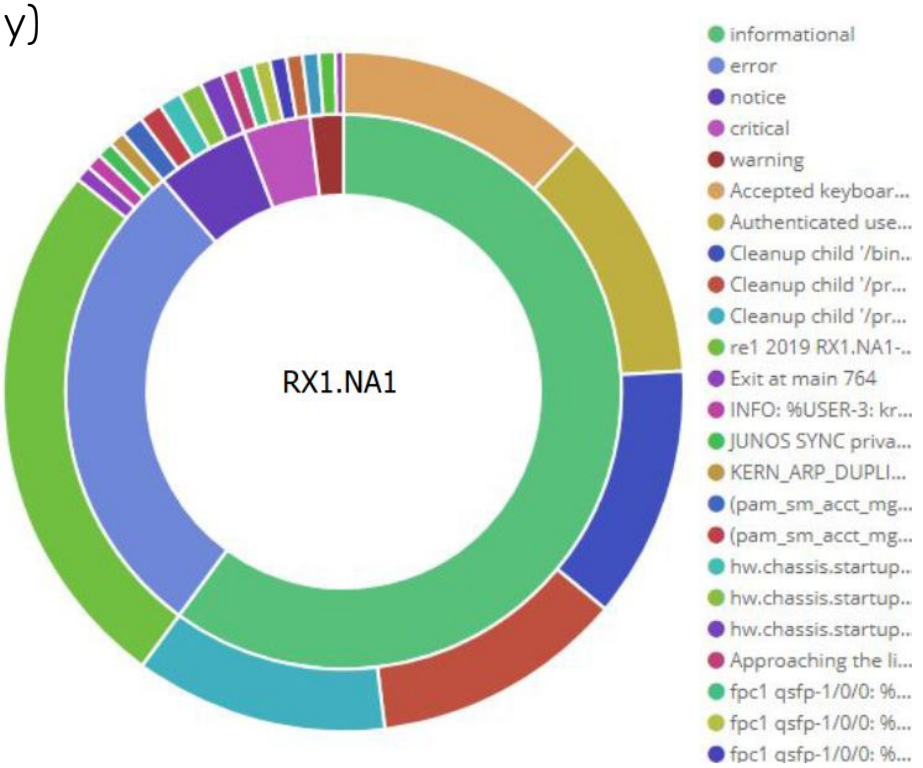
> from 200 MB/day to 60 MB/day (80 kEvents/day)

Usage from the network operations

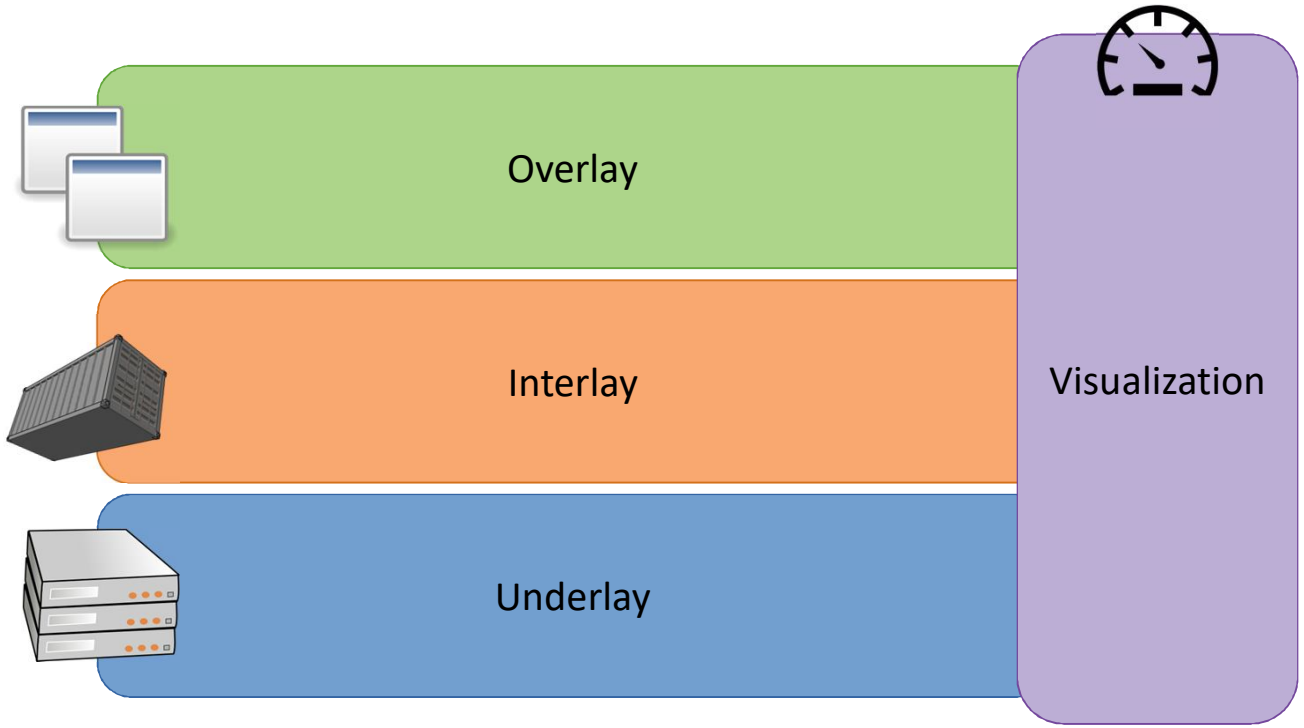
> check faults and misbehavior
> track BGP sessions changes
> check CLI/SSH access on the routers
> simpler log exchange with Juniper support
> events clustering by severity / by roles

More recent changes

> Cisco CPEs log collection
> Alerting (more later…)



Data collection and presentation



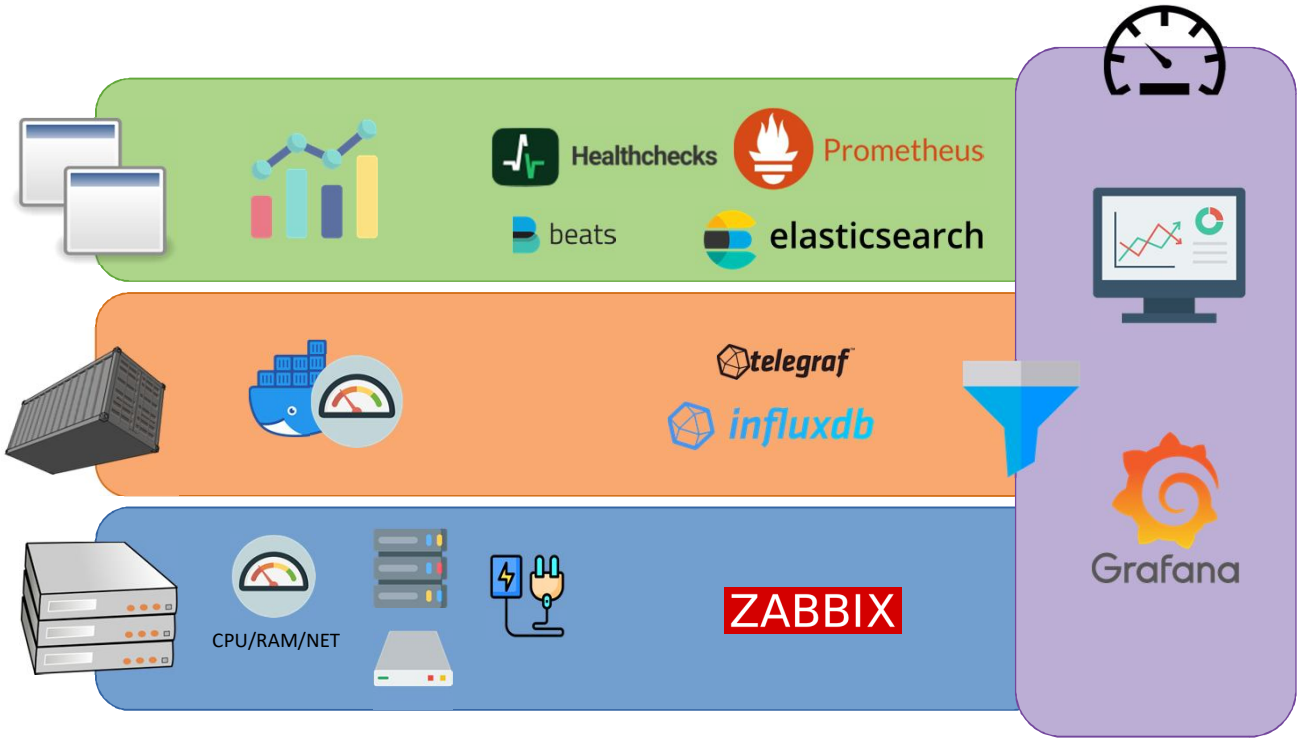
Collection layered model

« You cannot measure blood pressure with a thermometer »

Holistic view

Many services and many projections through a single pane of glass

Toolset: data lakes and probes



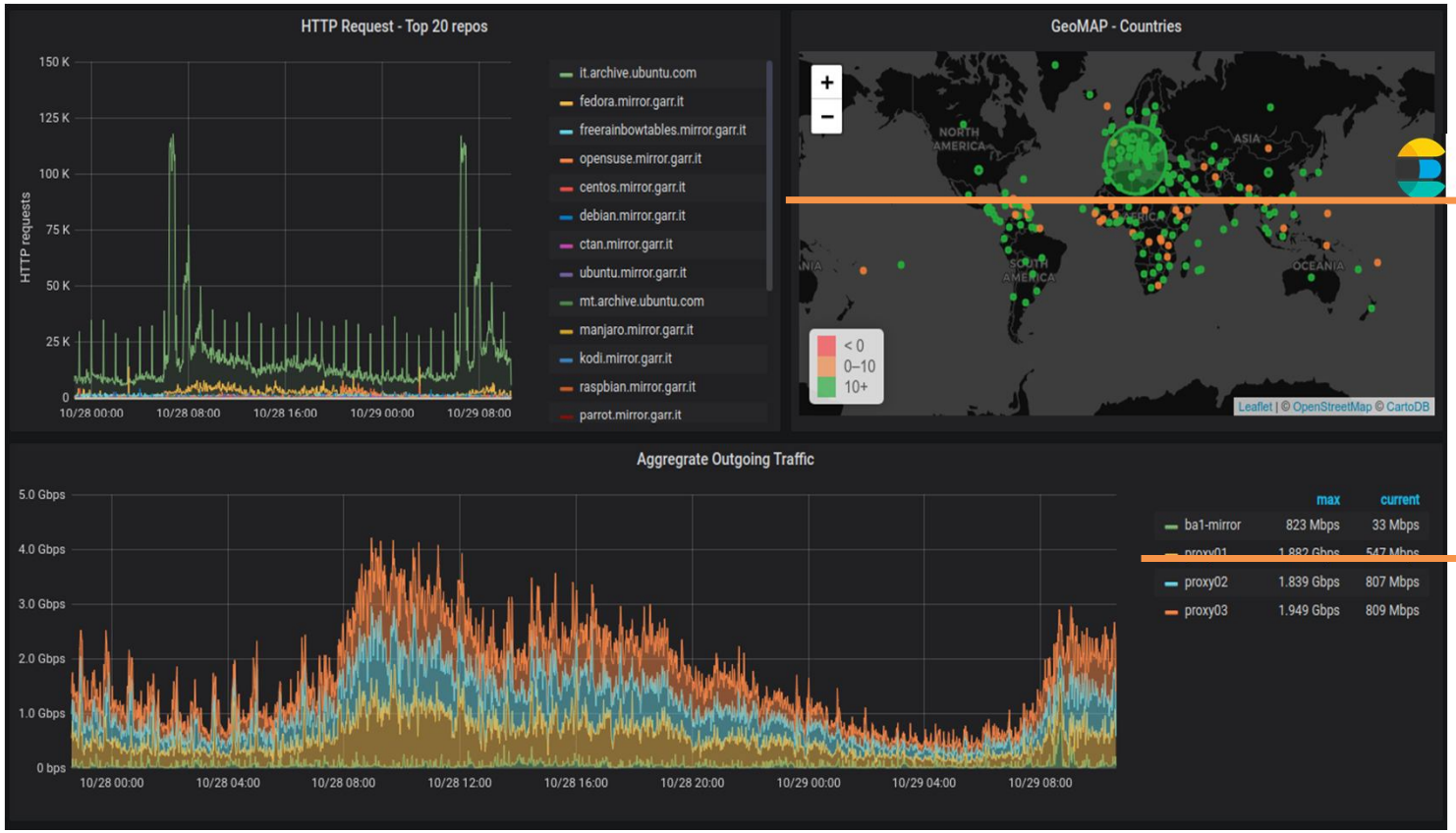
Automation tools

> Data lakes
Kubernetes
Helm packages

> Probes
Ansible roles
Docker containers

A vertical view - GARR Mirror

Service Operation perspective



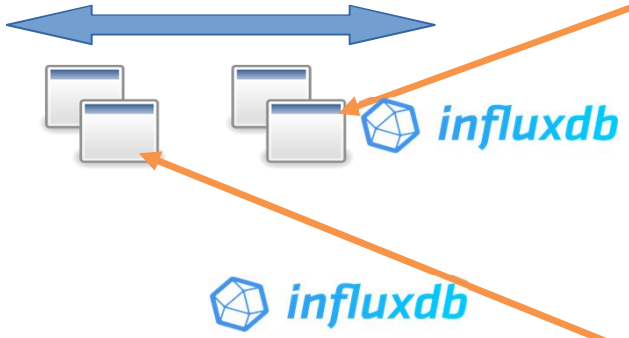
elasticsearch

Vertical view

ZABBIX

A horizontal view – Videoconference services

Horizontal view

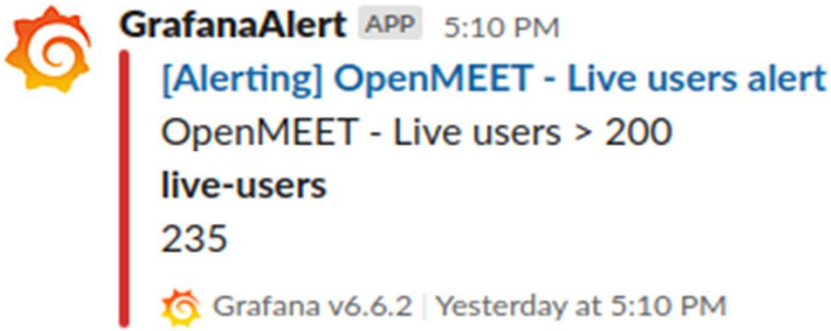


Service Planning perspective

Alerting and notification

- Operation paradigm shift
  - Hardware and software fault detection
  - Relevant service events as alerts

- Multi-cannel notification
  - Minimal signal/noise ratio
  - Selective sending to the expert
  - Integration with collaboration tools (Slack channels, email)



Conclusions

Long journey

> standardized telemetry approach

> methods and decisions first, then tools – but automation is a must-have

> alerting, notification pave the path for the evolution

Next steps

> application services log analysis (Kubernetes support, data filtering)

> telemetry & log analysis convergence

> smarter thresholds, richer analytics if/where needed

> nudge the operations teams to Site Resilience Engineering

images by https://www.flaticon.com