Sperimentazione ELK X-Pack unificato per servizi Applicativi GARR

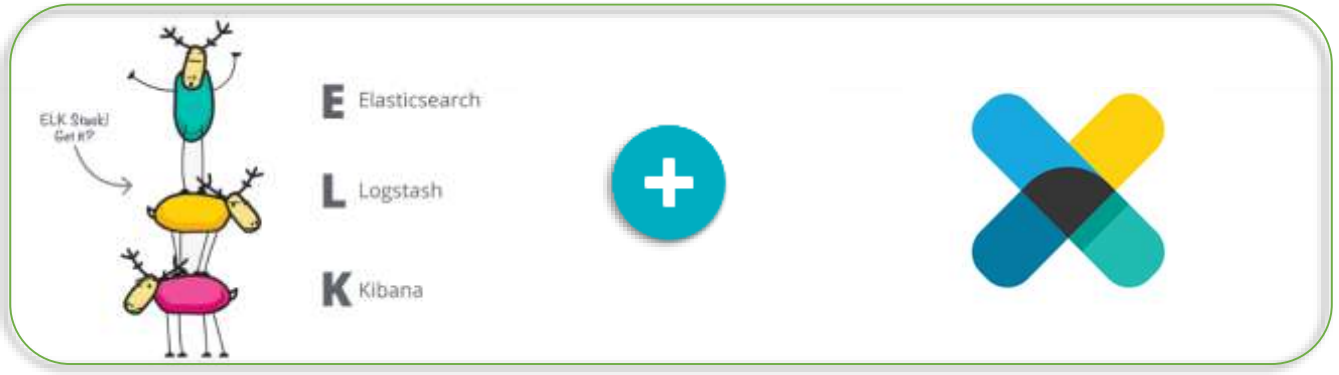
PAOLO VELATI [GRUPPO ELISA] - GARR

Rimini, 12/06/2018
Workshop CCR 2018

Outline

- Motivazioni e Goal
- Tecnologia adottata
- Primi risultati
- Prossimi passi

ELK + X-Pack



Security

Alerting

Monitoring

Reporting

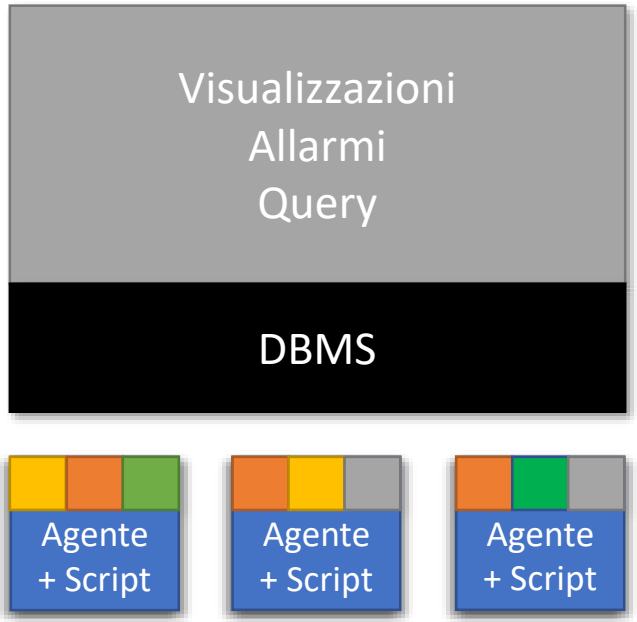
Graph

Machine Learning

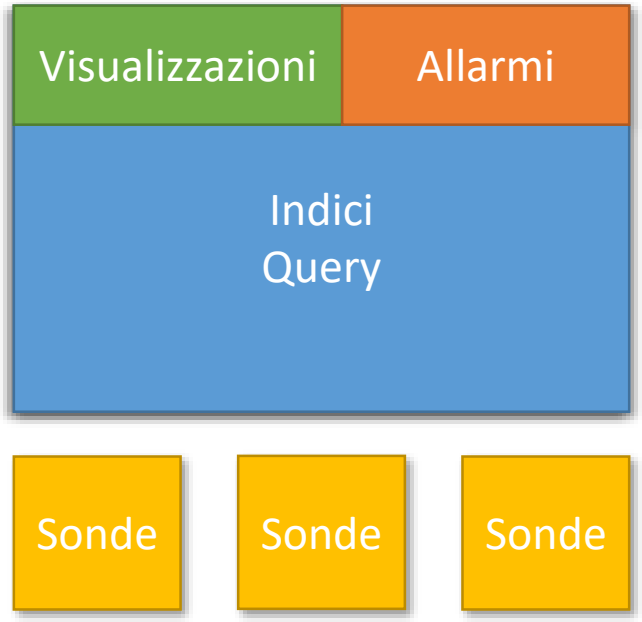
La Motivazione

- Visione olistica stato di sistemi e servizi
- Integrazione con l'esistente
- Armonizzazione dati da fonti eterogenee
- Conoscenza da analisi dei dati

Tradizionale → Moderno



- Sonde App-Aware (pre-filtraggio)
- Reattivo
- Database relazionale / file
- Architettura verticale



- Sonde di dato raw (log, metriche)
- Reattivo + Proattivo
- Inverted Index / Time-series DB
- Scalabilità orizzontale

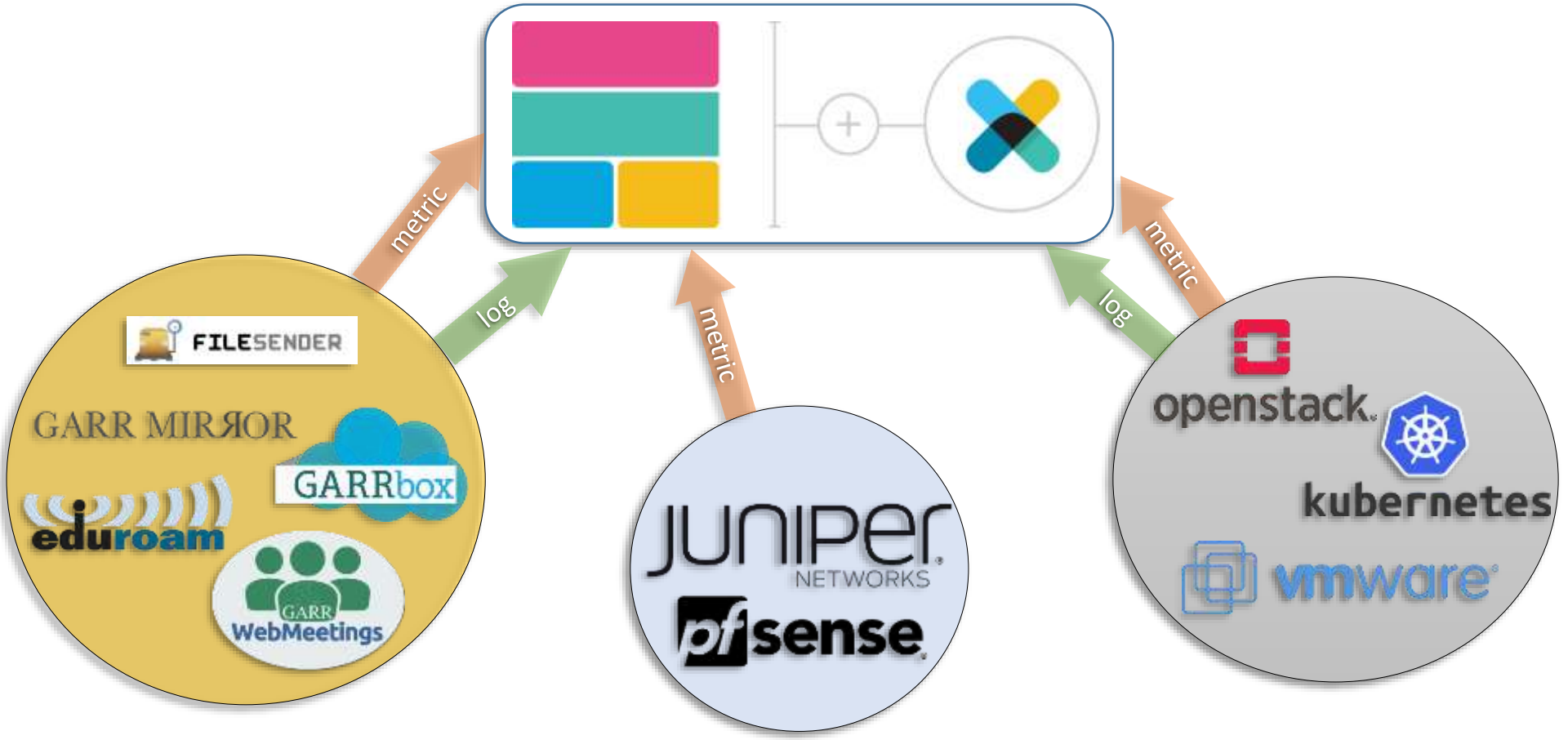
La Sperimentazione

- Definizione di un servizio centralizzato che possa aggregare e armonizzare i sistemi di monitoraggio distribuiti

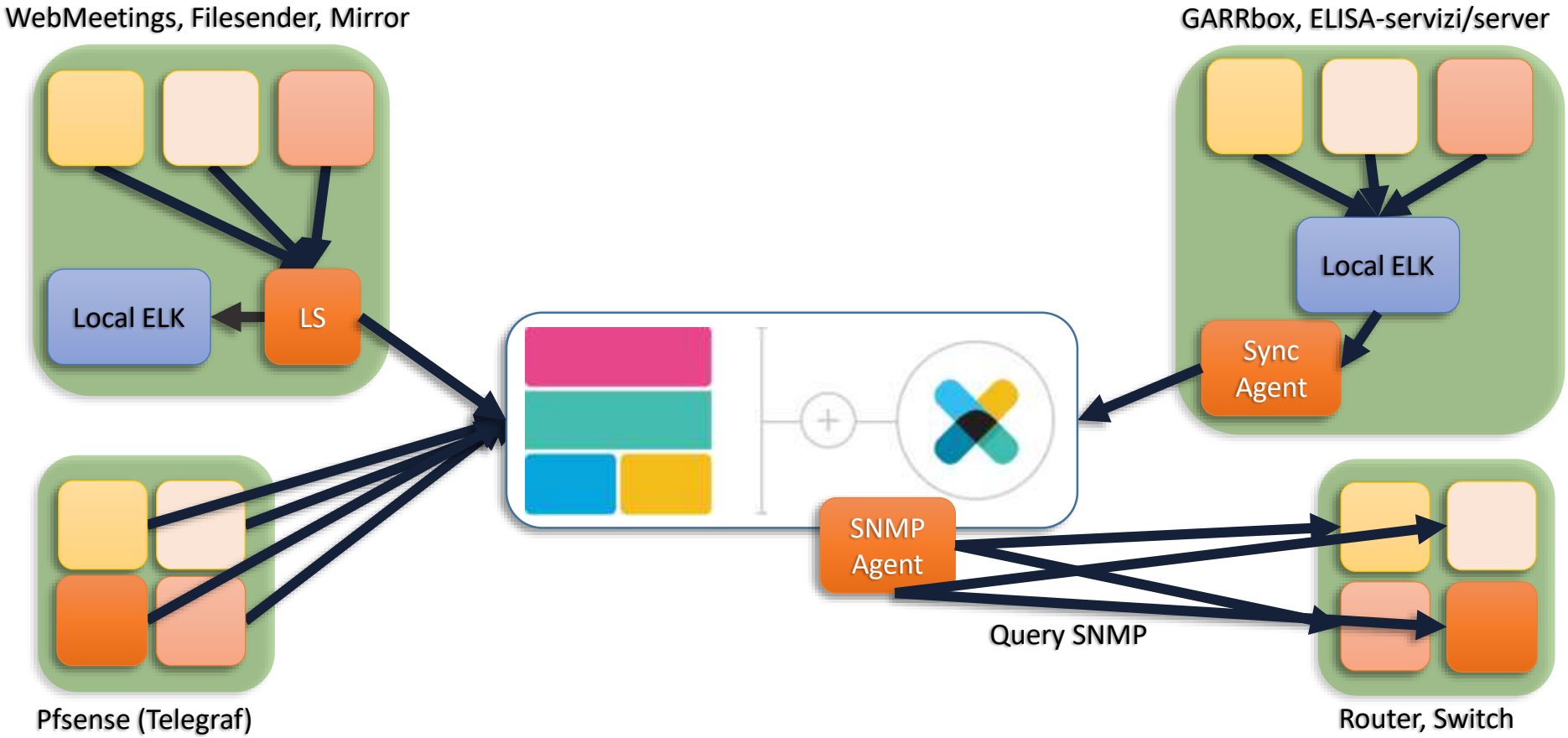
maggiore conoscenza → maggiore controllo

- Gruppo Evoluzione Rete (ELISA) + System Support x 1 mese di lavoro
- Servizi Top-of-Network + Elementi infrastrutturali lab Evoluzione Rete
- Collaborazione in corso con Elastic.co

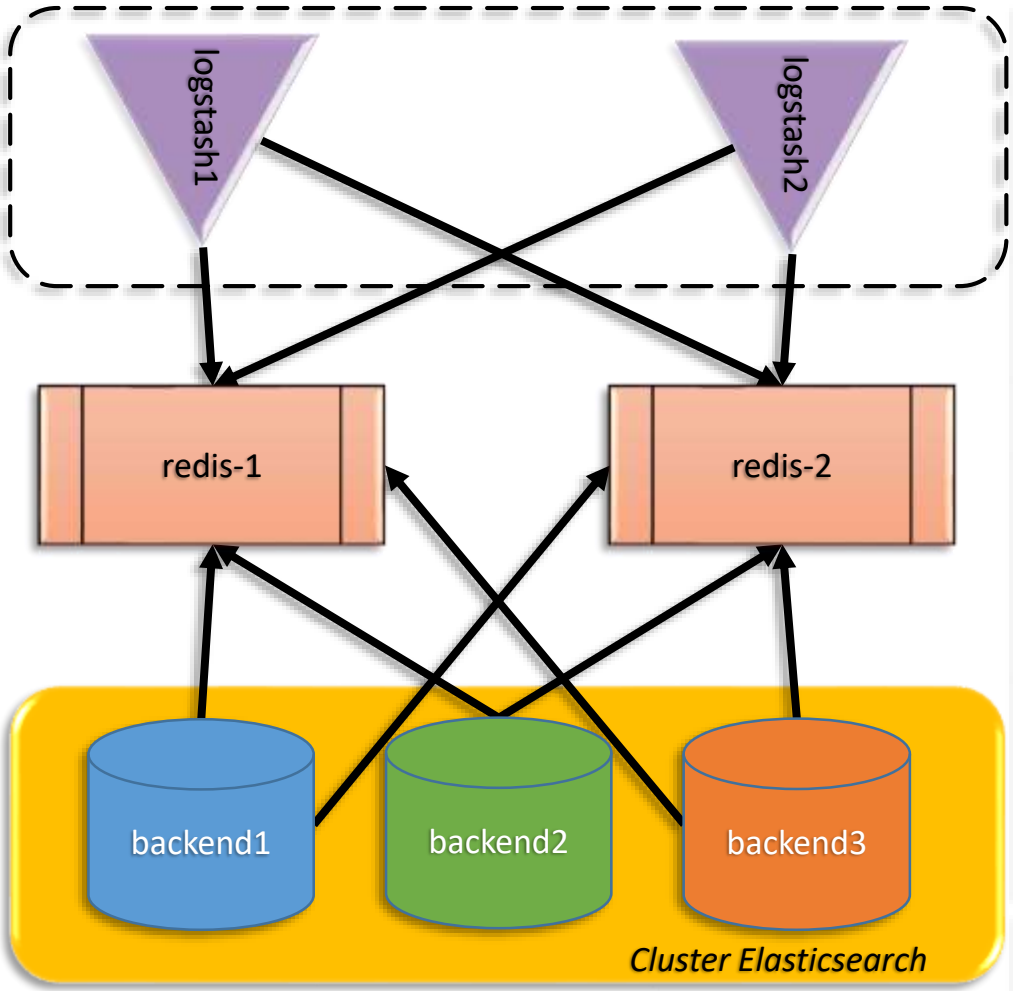
Servizi, sistemi e dispositivi connessi



Architettura alto livello



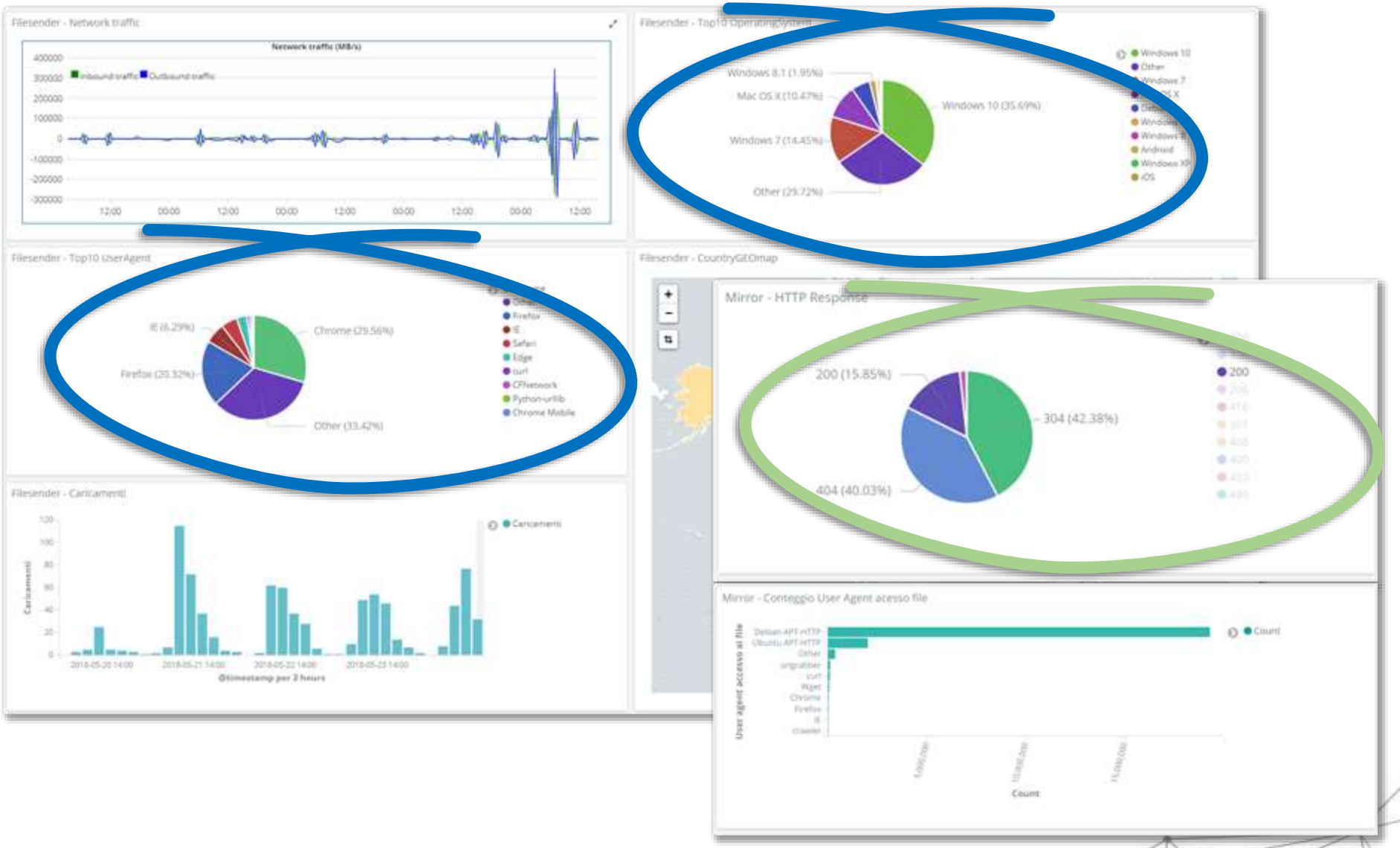
Architettura nel dettaglio



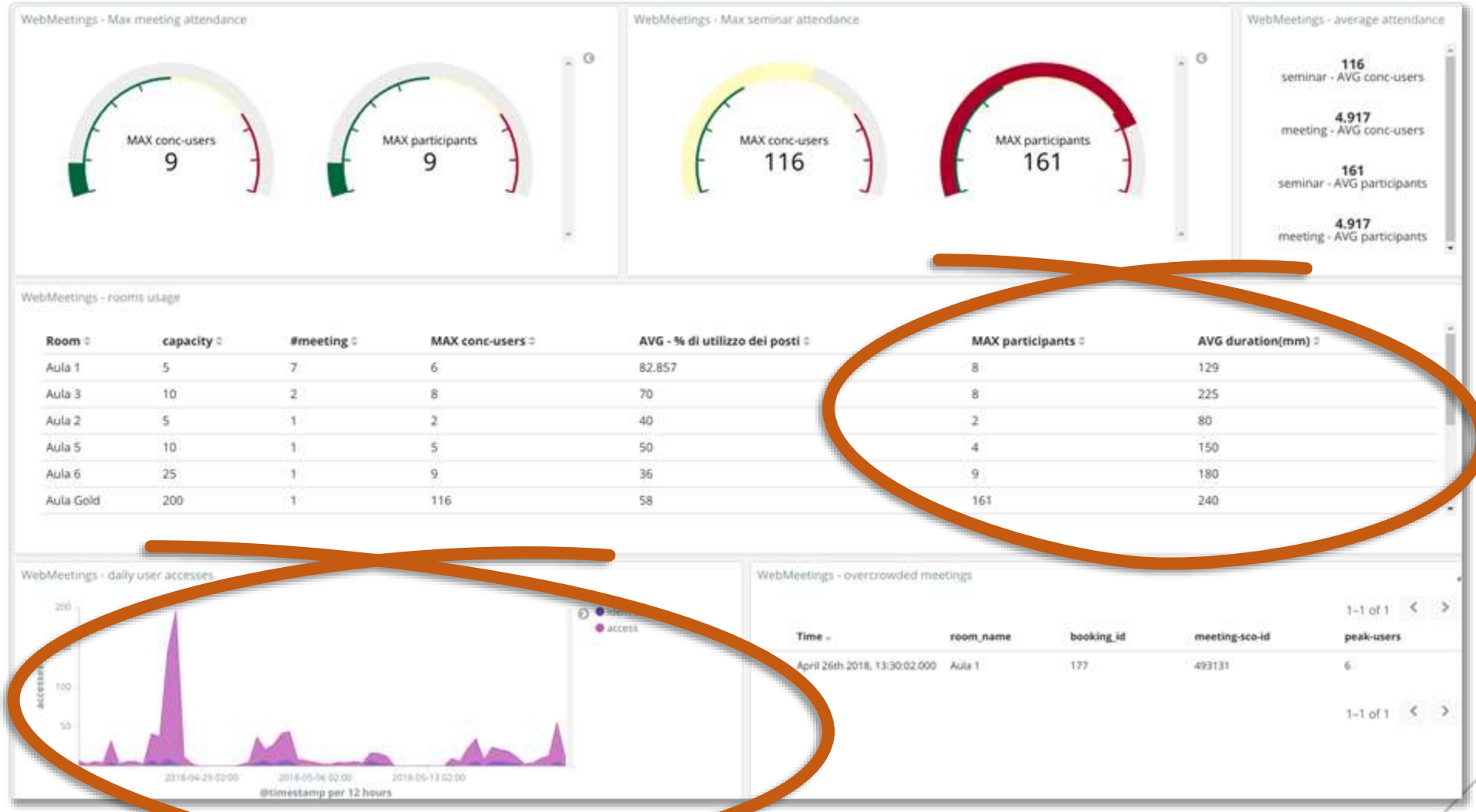
Elemento	Componenti
3 nodi di backend	• elasticsearch • logstash • kibana
2 nodi tampone/coda (queue)	• redis-server
2 nodi di frontend	• logstash
1 nodo proxy (non presente nello schema)	• reverse proxy e load balancer (nginx) verso i servizi kibana
1 nodo di storage per backup (non presente nello schema)	• nfs server montato sui nodi di backend (daily backup)

Risorse: 32vCPU, 64G RAM, 460G Storage OpenStack, ambiente di sviluppo c/o Milano-Bicocca

Dashboard: FileSender / Mirror

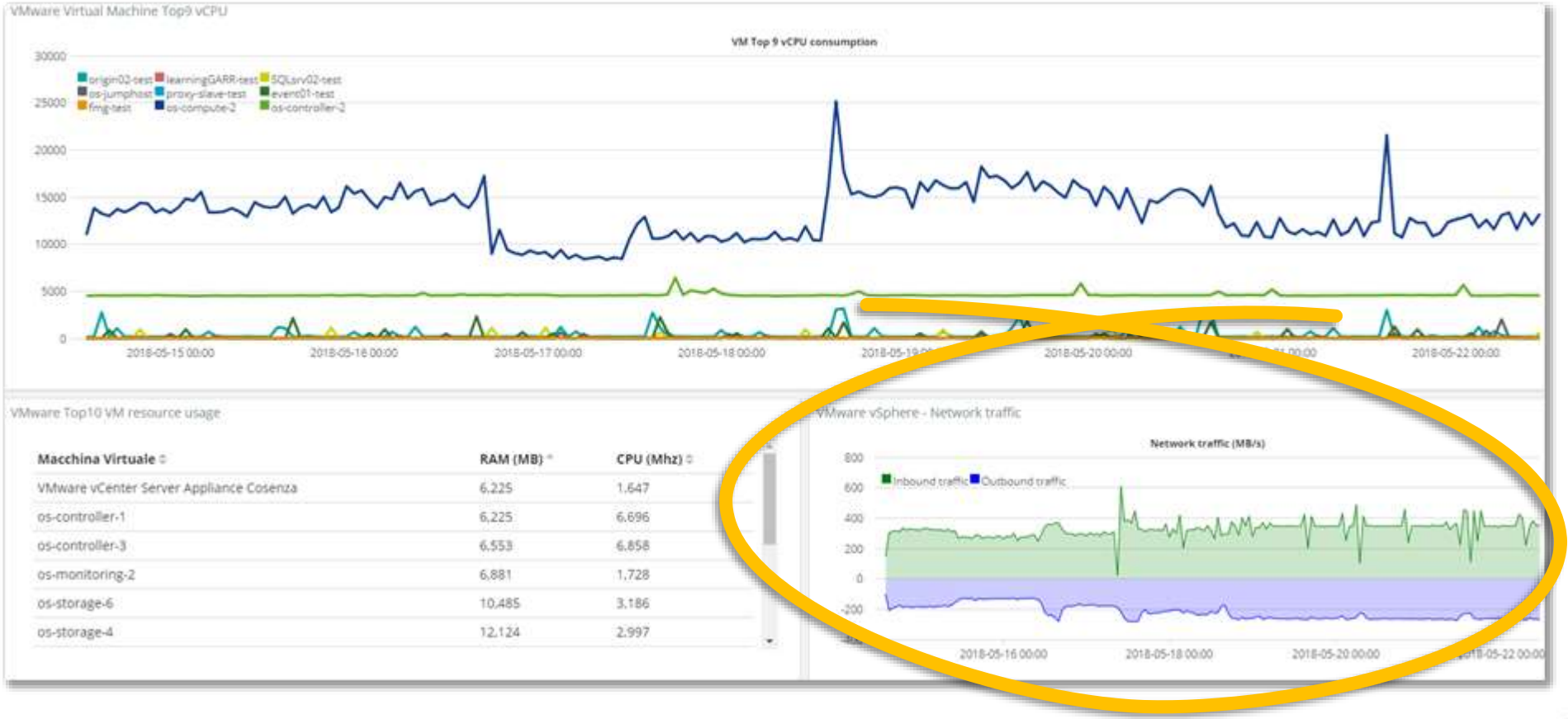


Dashboard: WebMeetings



Dashboard: GARRbox

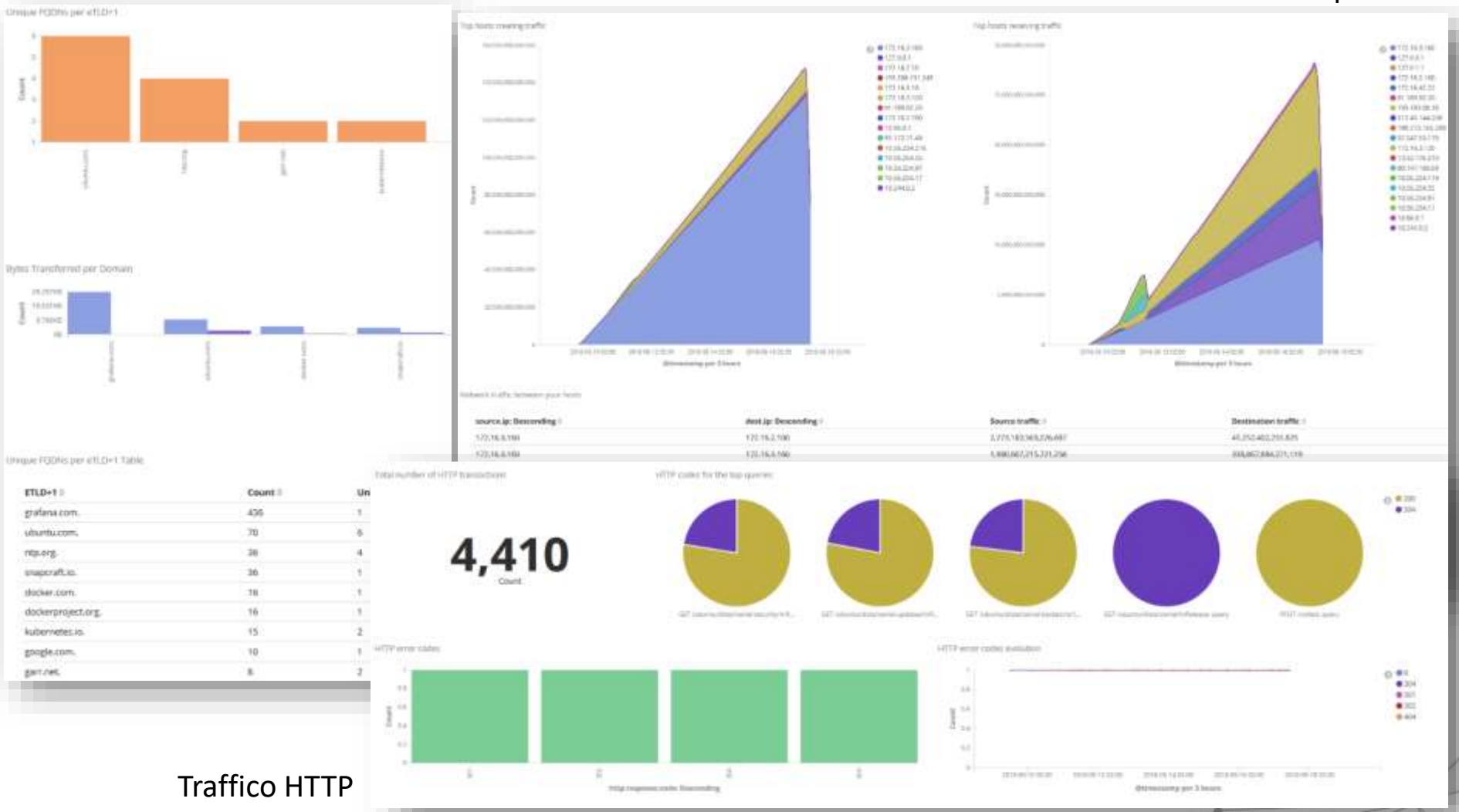
Dashboard: VMware



Dashboard: vRouter e infrastruttura ELISA

Traffico DNS

Flussi e Top-talker



Traffico HTTP

Dashboard: Multi-servizio / Multi-vista

Dashboard: Multi-servizio / Multi-vista

Prime osservazioni inattese

Anomaly detection

Primi risultati…

- Molti risultati in poco tempo e poco sforzo

(Docker + Ansible + OpenStack) + Agile == 

- Opt-in dei servizi in breve tempo
  - Sia da zero sia in integrazione con monitoraggio esistente

- Creazione di viste e analisi dati
  - Curva di apprendimento bassa

...e criticità riscontrate

- Dimensionamento risorse
- Filtraggio dei log inviati
- Rallentamenti interfaccia
- Ritardo nella visualizzazione dei log
- Limitazioni hardware per ambiente di test
  - Disk 100% busy, ~140 iops
  - ~50-100 event/s

Prossimi passi

- La sperimentazione continua…
  - Aggiunta di ulteriori servizi top of the net e visualizzazioni
  - Maggiore confidenza con lo strumento
  - Servizi e elementi di rete: analisi dei flussi e DNS/NTP

- Collaborazione con Elastic.co
  - Transizione a servizio