Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Sperimentazione ELK X-Pack unificato per servizi Applicativi GARR

PAOLO VELATI [GRUPPO ELISA] - GARR

Roma, 30/05/2018

Workshop GARR 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

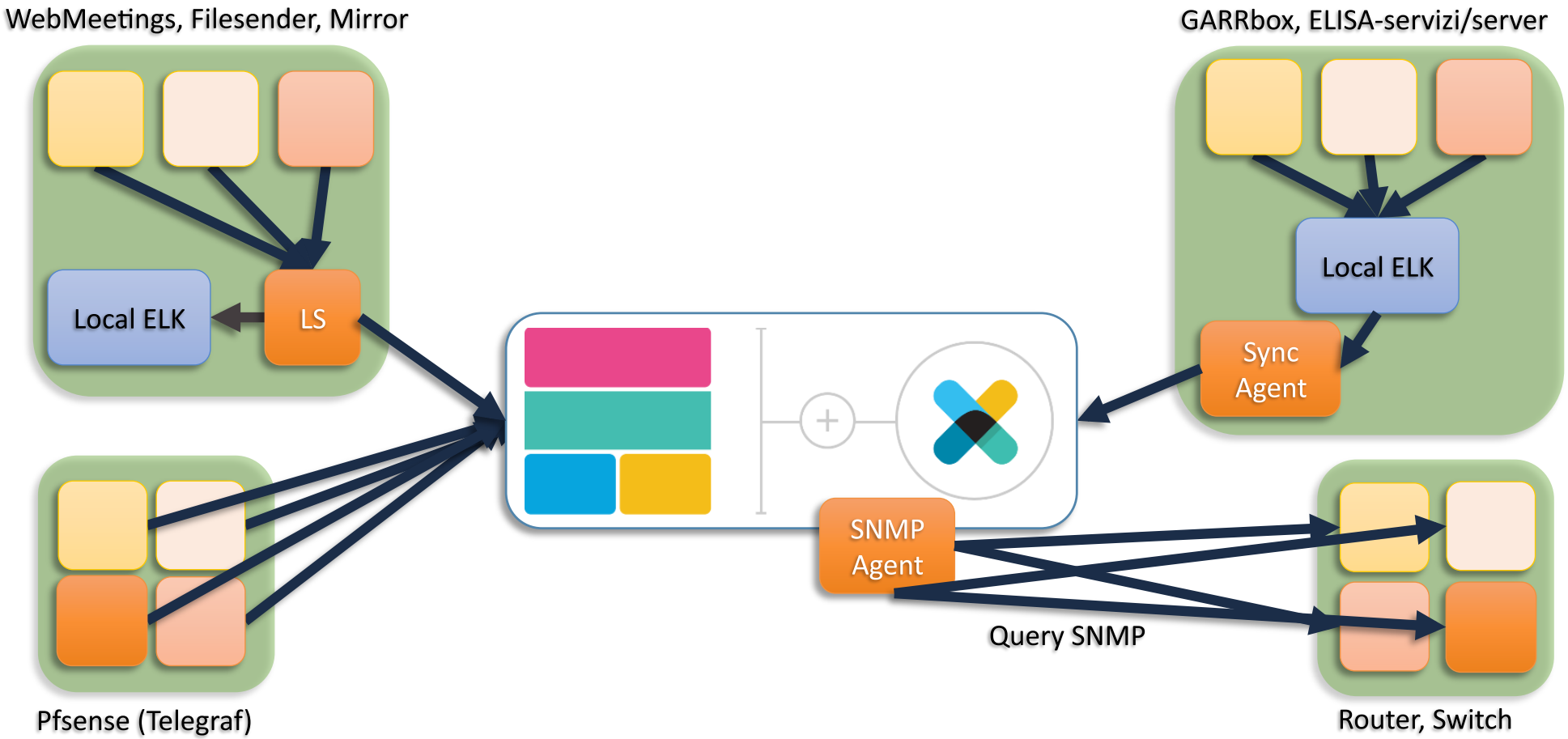
La Sperimentazione

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

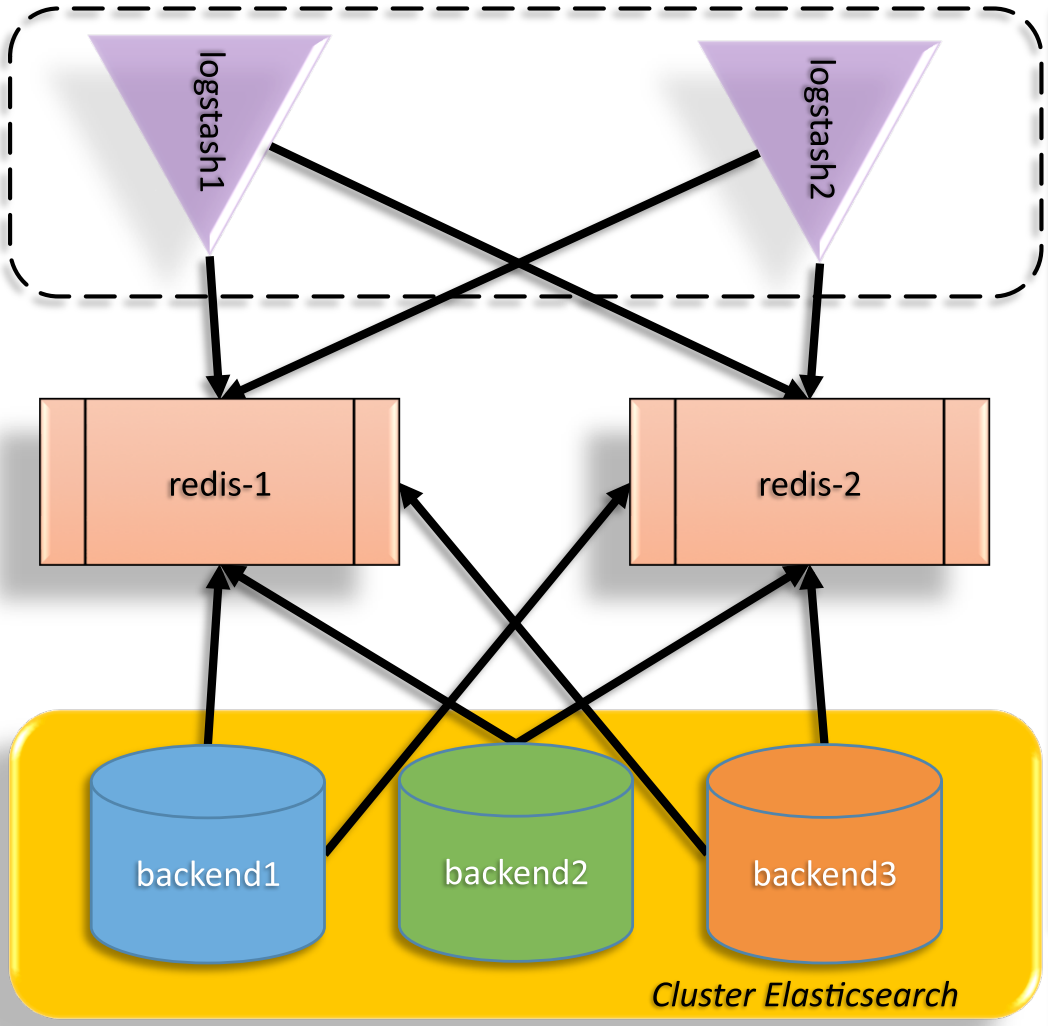
maggiore conoscenza → maggiore controllo

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

Architettura alto livello



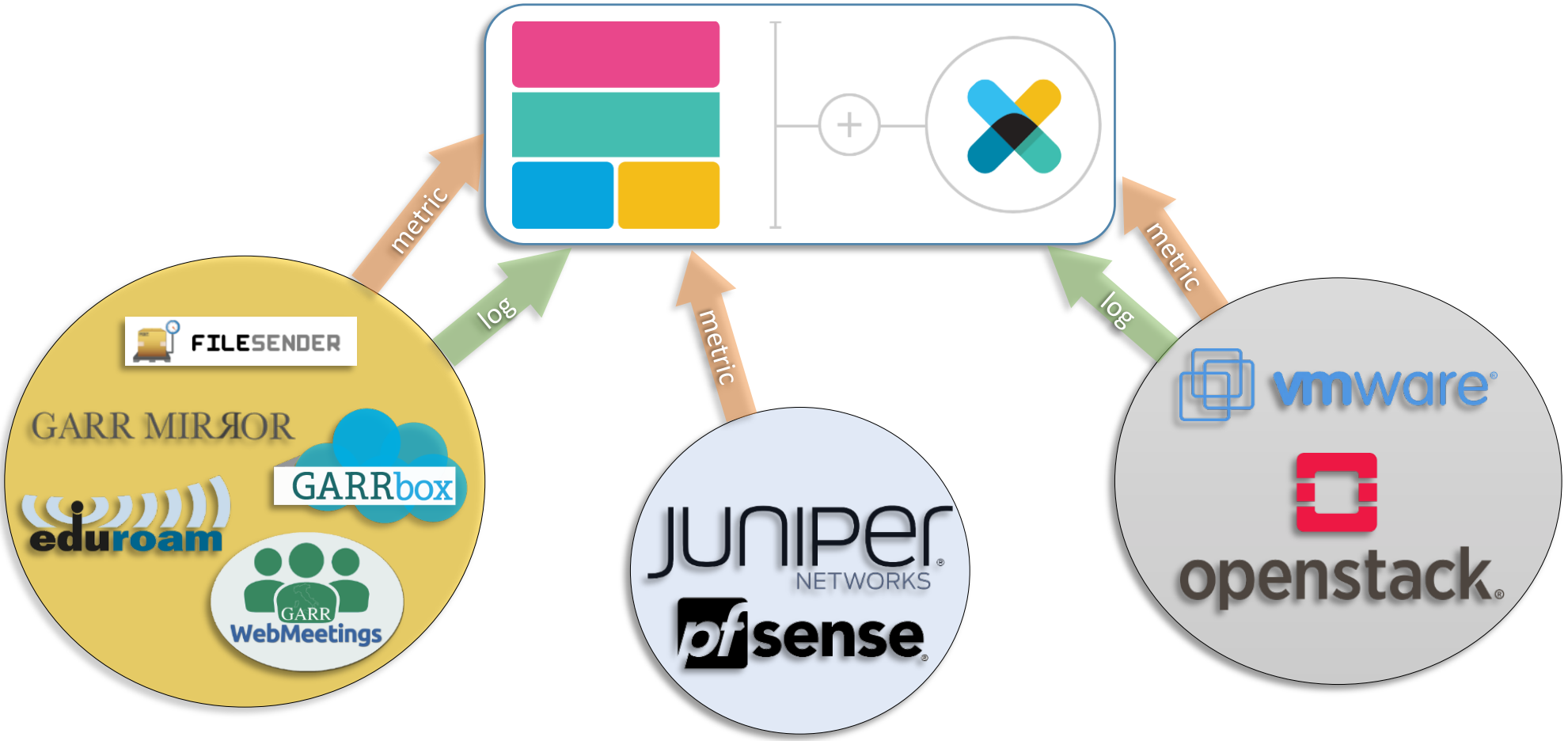
Architettura nel dettaglio



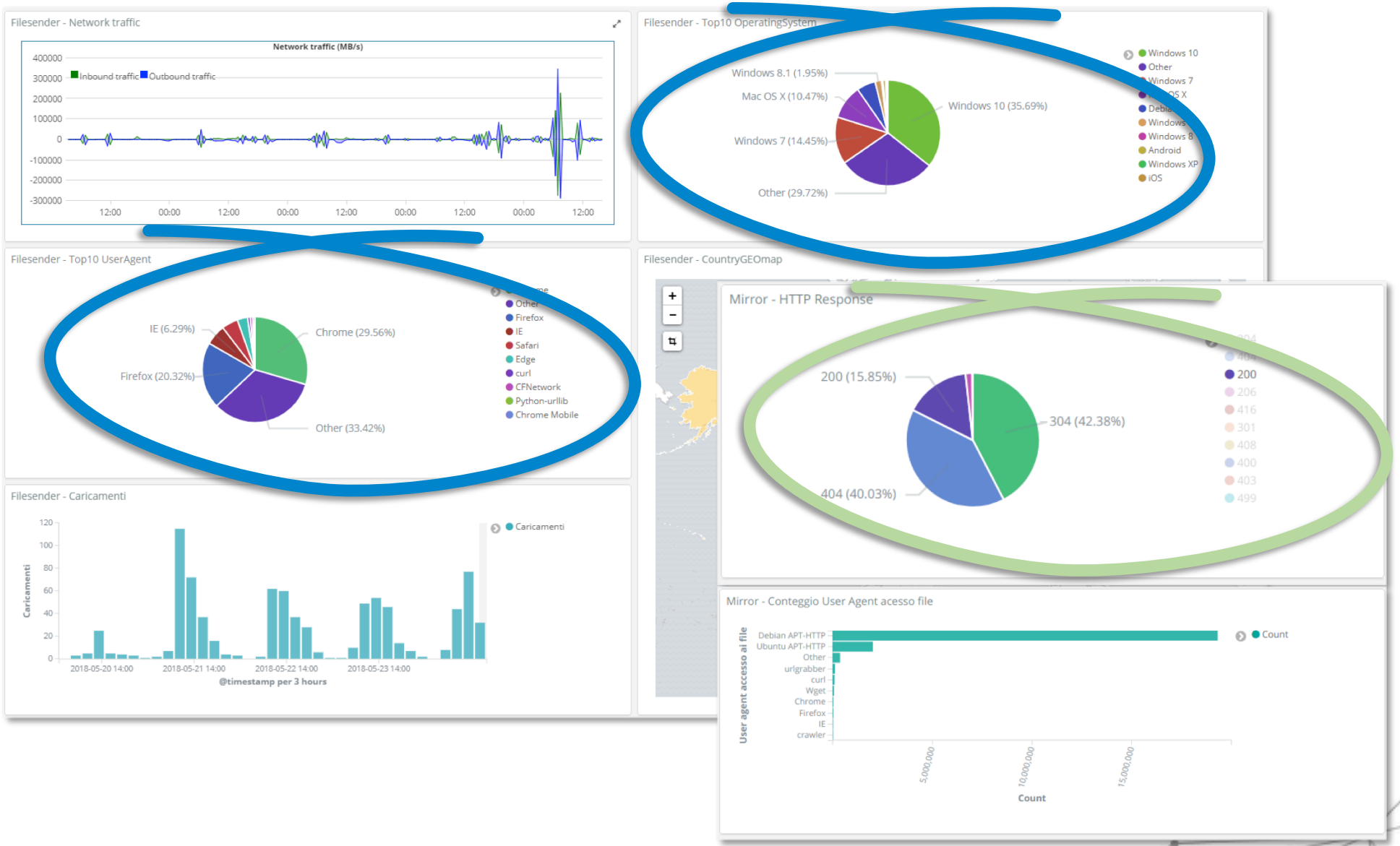
Elemento	Componenti
3 nodi di backend	• elasticsearch • logstash • kibana
2 nodi tampone/coda (queue)	• redis-server
2 nodi di frontend	• logstash
1 nodo proxy (non presente nello schema)	• reverse proxy e load balancer (nginx) verso i servizi kibana
1 nodo di storage per backup (non presente nello schema)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

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

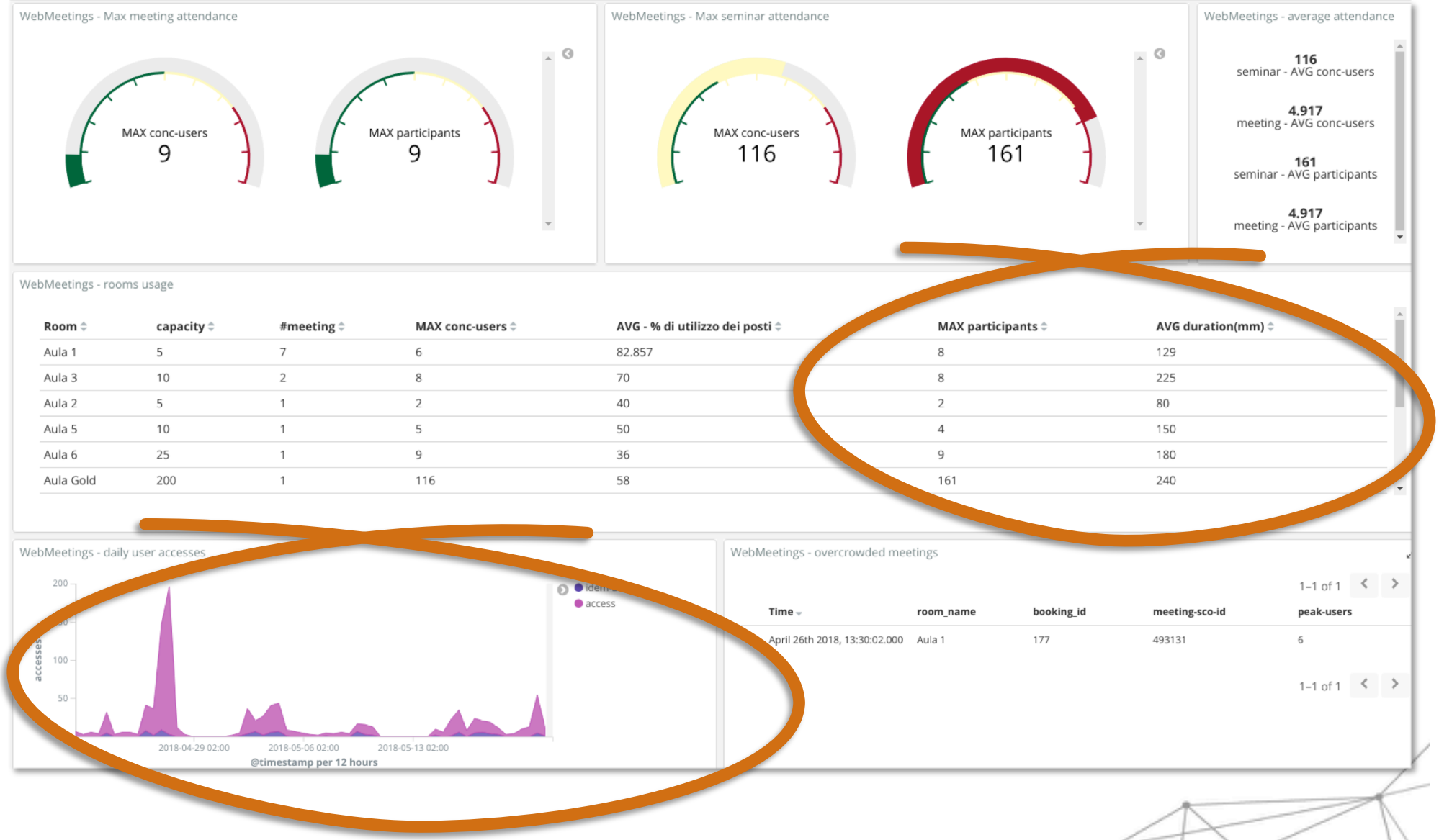
Servizi, sistemi e dispositivi connessi



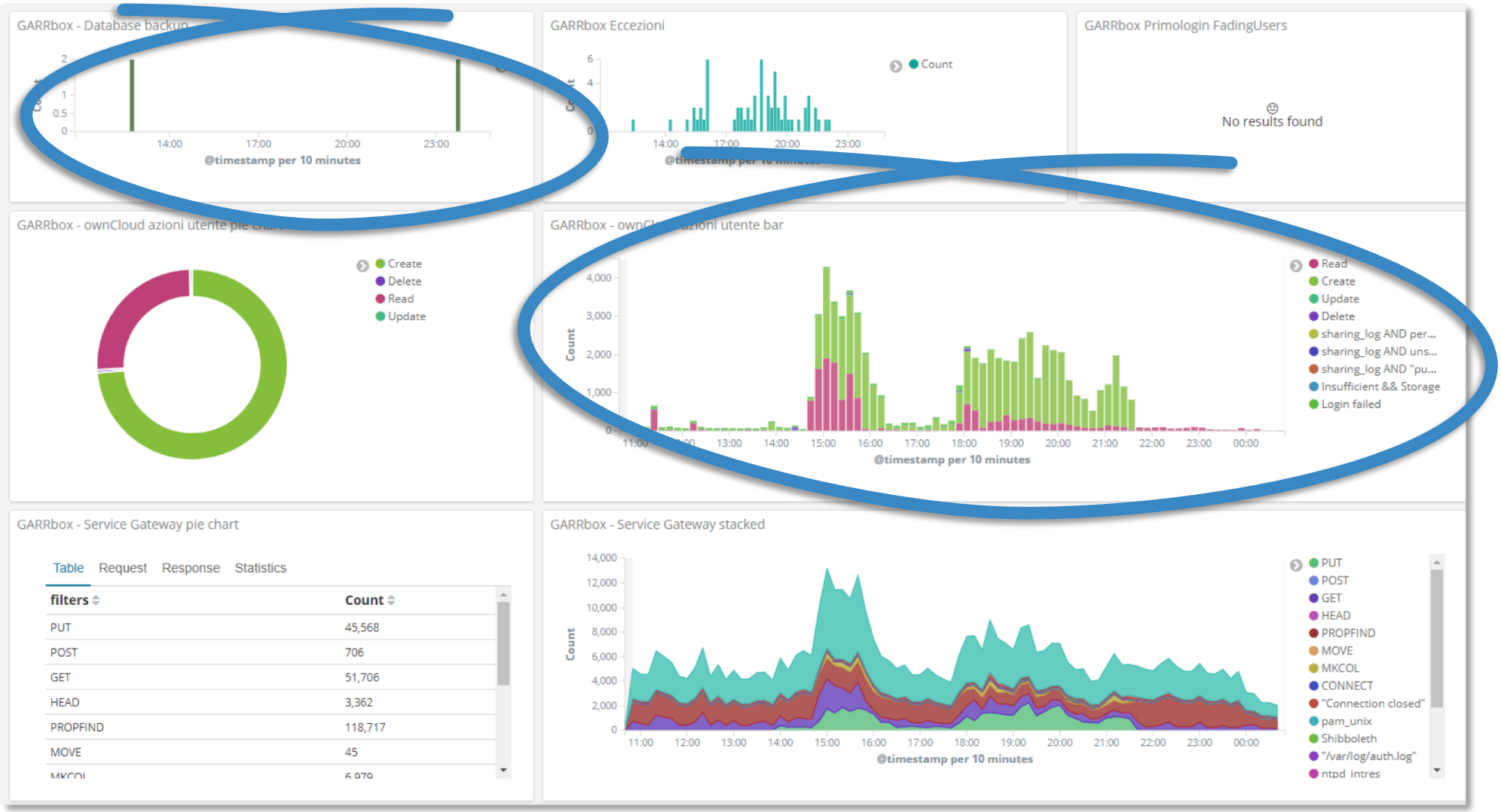
Dashboard: FileSender / Mirror



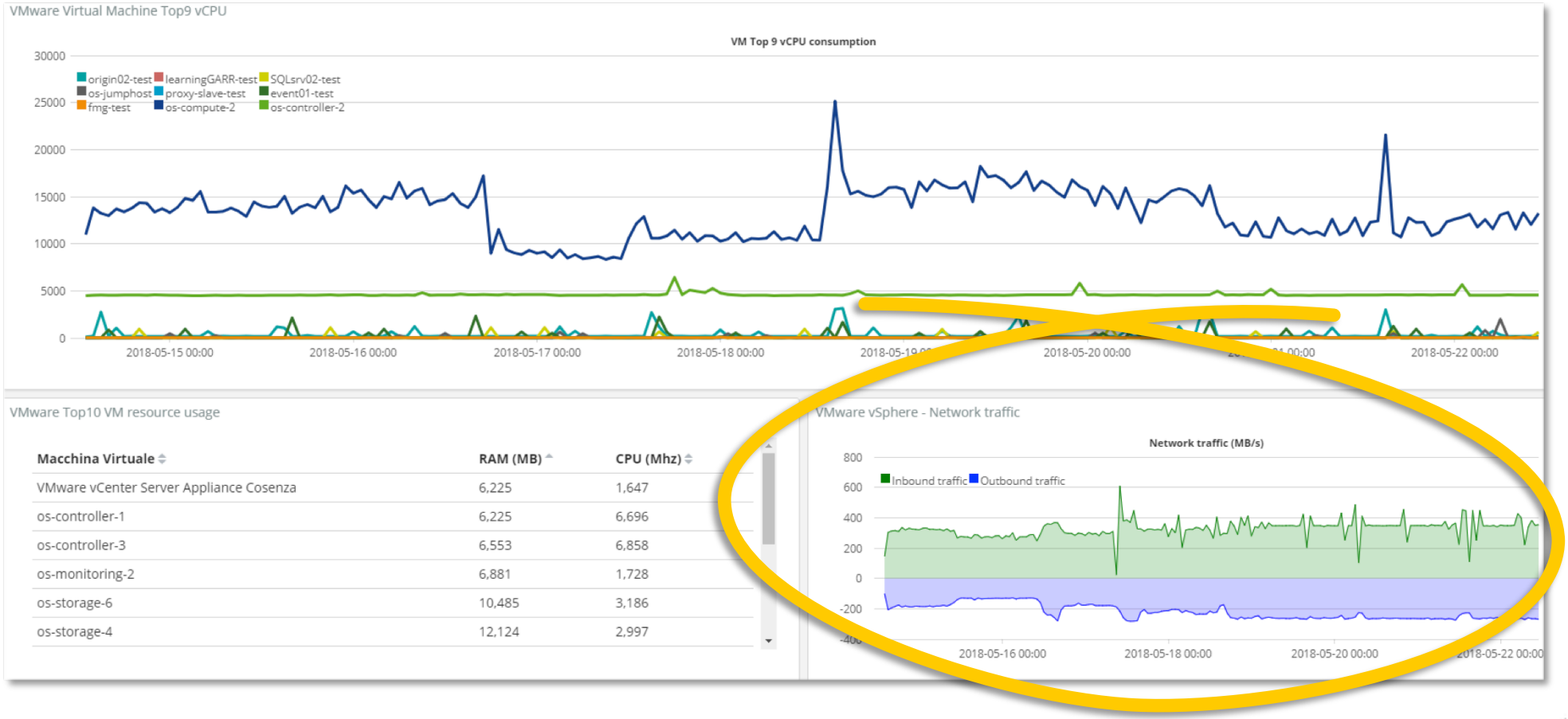
Dashboard: WebMeetings



Dashboard: GARRbox



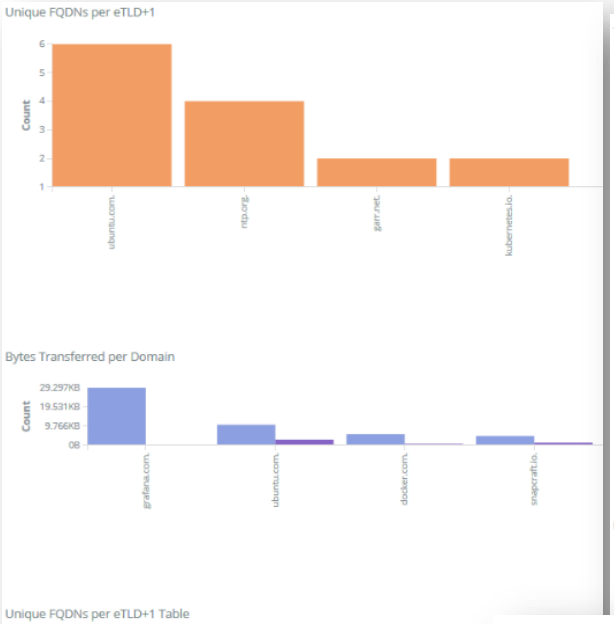
Dashboard: VMware

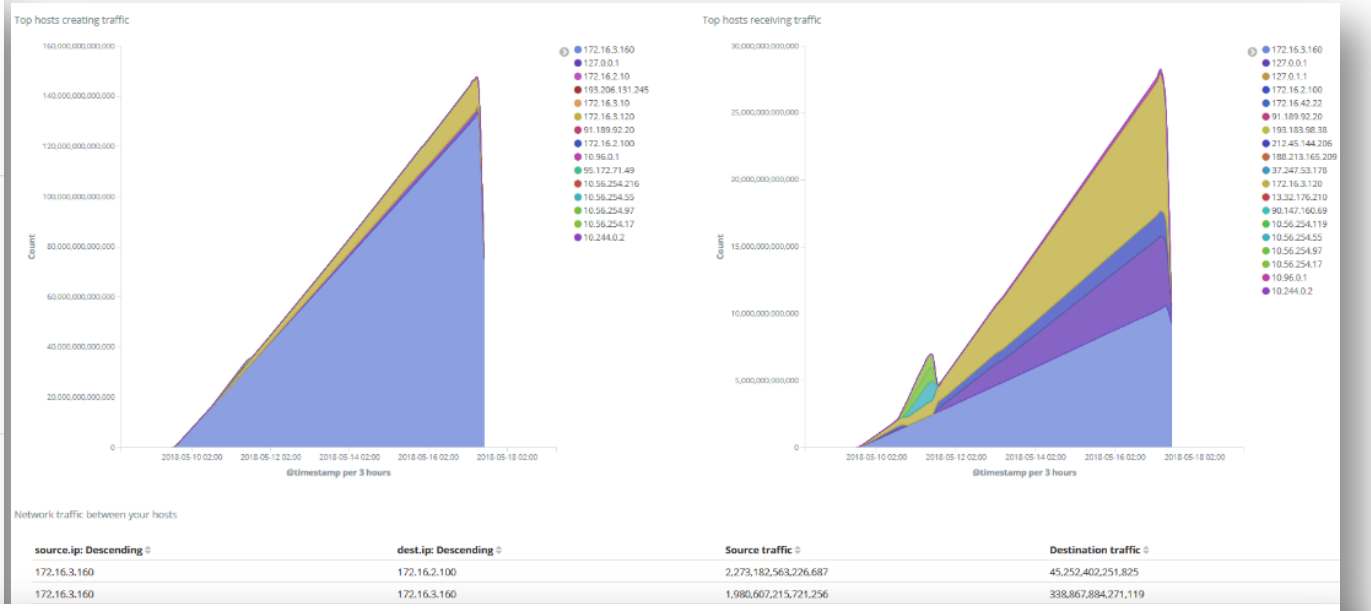


Dashboard: vRouter e infrastruttura ELISA

Traffico DNS

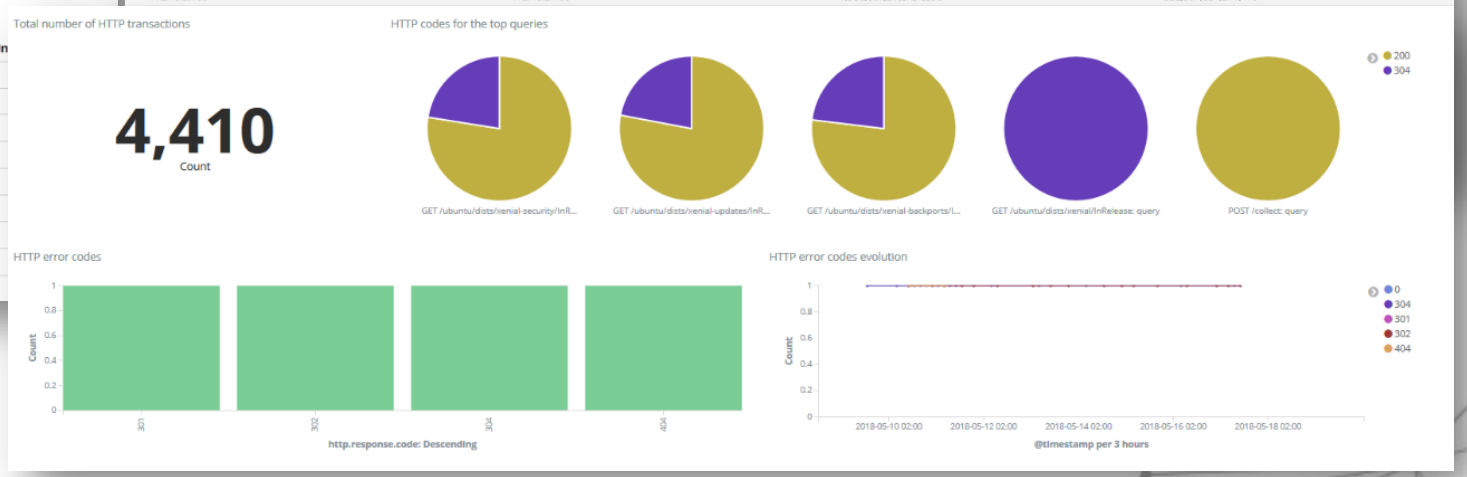
Flussi e Top-talker





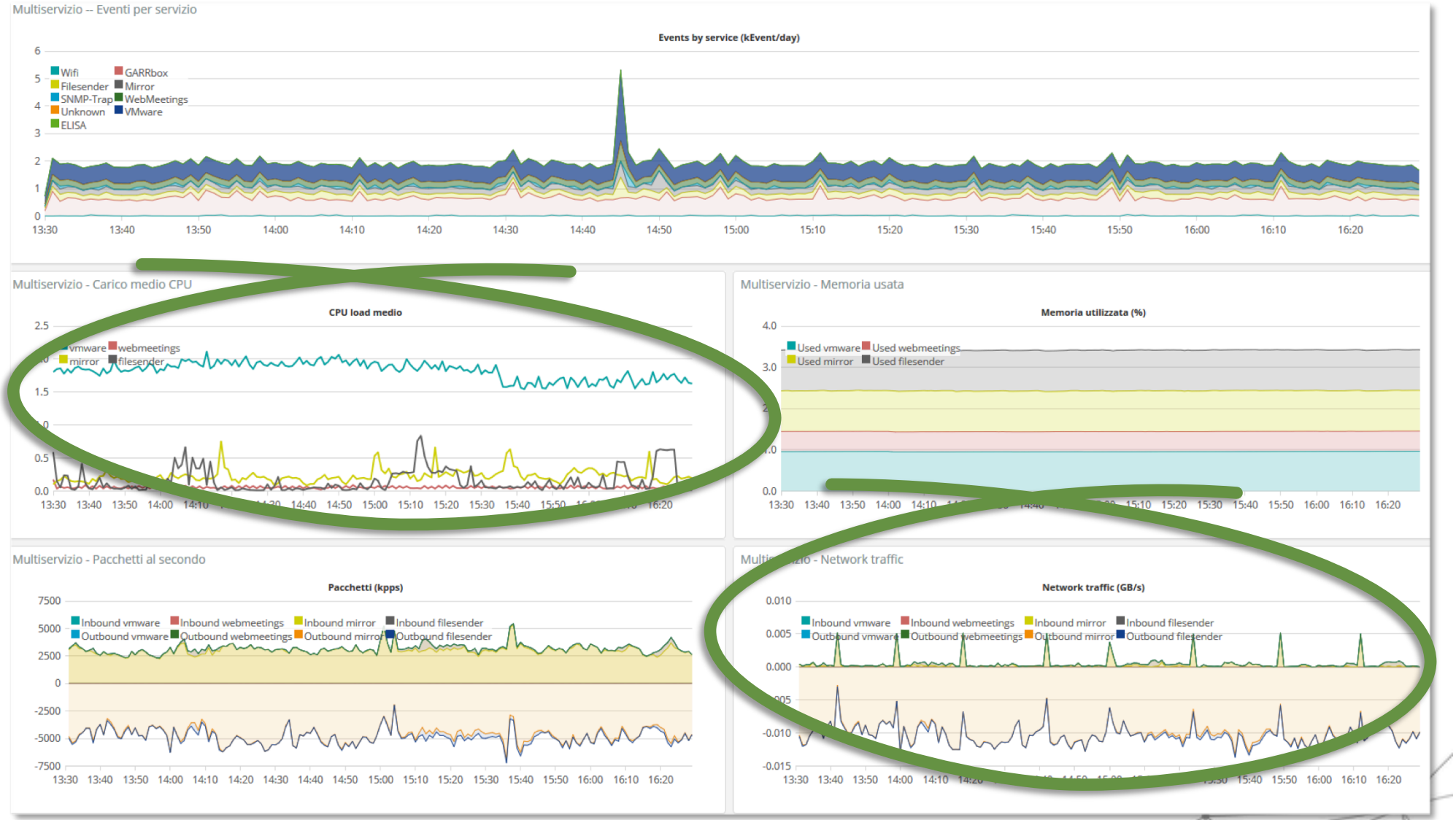
Unique FQDNs per eTLD+1 Table

ETLD+1	Count	Un
grafana.com.	436	1
ubuntu.com.	70	6
ntp.org.	36	4
snapcraft.io.	36	1
docker.com.	16	1
dockerproject.org.	16	1
kubernetes.io.	15	2
google.com.	10	1
garr.net.	8	2

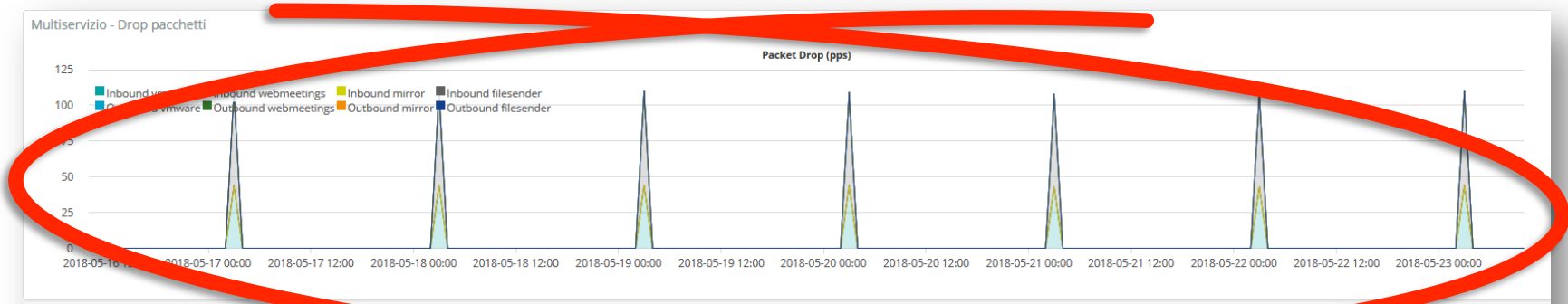


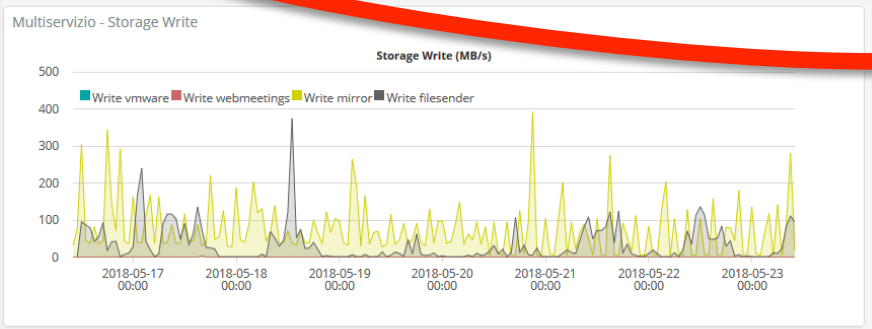
Traffico HTTP

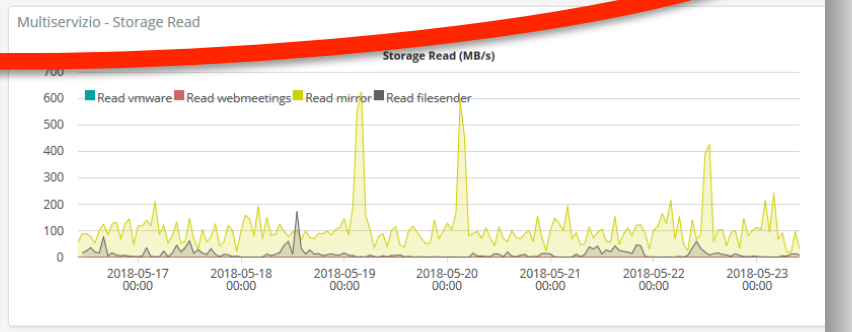
Dashboard: Multi-servizio / Multi-vista

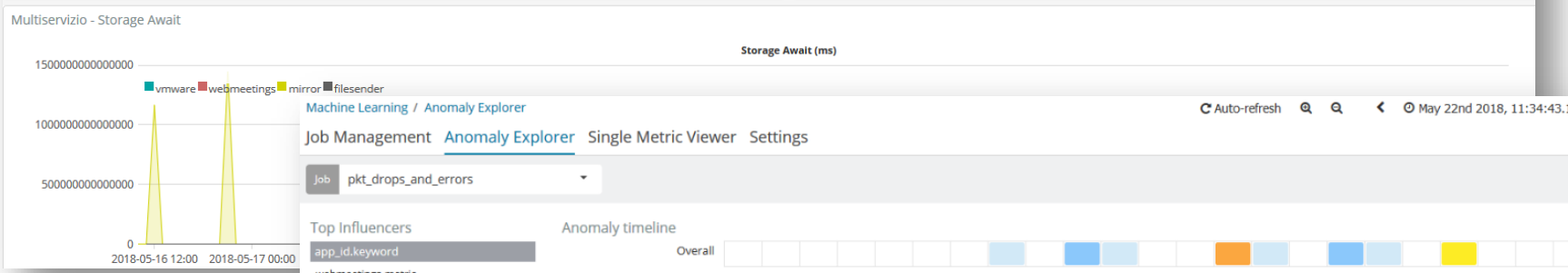


Dashboard: Multi-servizio / Multi-vista









Prime osservazioni inattese

!!!

Anomaly detection

Primi risultati…

- Molti risultati in poco tempo e poco sforzo

(Docker + Ansible + OpenStack) + Agile == 

- Opt-in dei servizi da zero e integrazione con monitoraggio esistente
  - ~1h → ~1 giorno uomo

- Creazione di viste e analisi dati
  - ½ giornata per la prima vista completa

…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

Prossimi passi

- La sperimentazione continua…
  - Aggiunta di ulteriori servizi e visualizzazioni
  - Maggiore confidenza con lo strumento

- Collaborazione con Elastic.co
  - Ampliamento dell'installazione attuale