Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Aggregazione e analisi centralizzate dei log di dorsale

Silvia d'Ambrosio

Roma, 8-10 ottobre 2019

Workshop GARR 2019

Log analysis avanzata per i device GARR

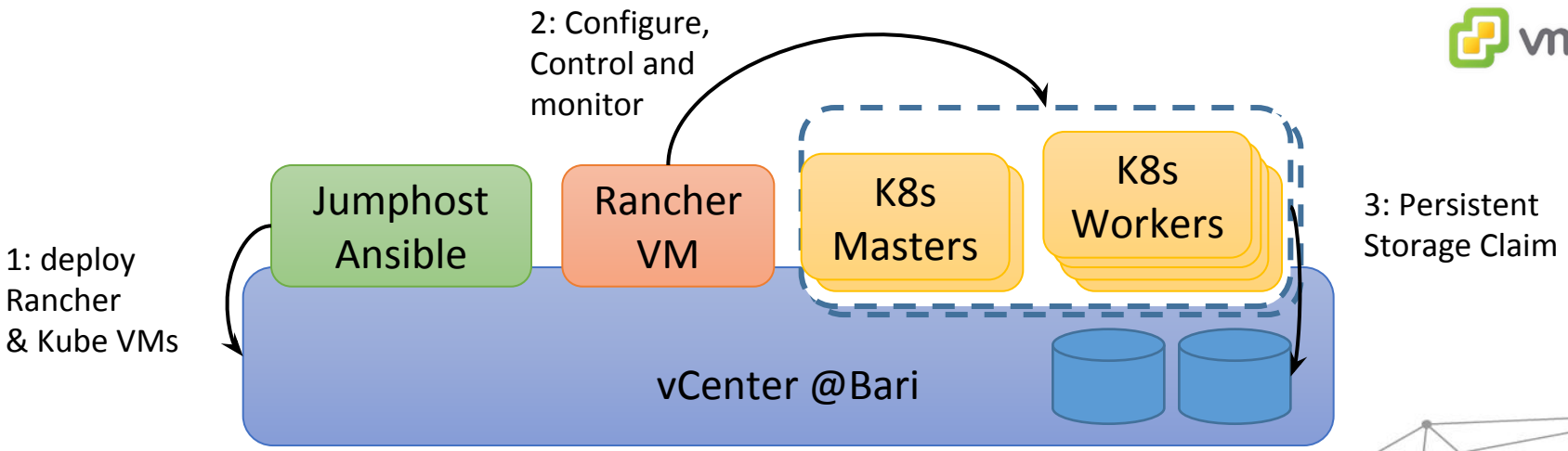
- Obiettivo
  - Evoluzione in produzione del pilota presentato lo scorso WS GARR
  - Centralizzazione dei log dagli apparati della rete
  - Strumento di analisi post-mortem, monitoring in tempo reale e quality assurance delle configurazioni

- Peculiarità
  - Sforzo congiunto tra i Dipartimenti INFRA e RETE
  - Primo servizio completamente Container Native
  - Attività iniziata di recente e tuttora in itinere

Architettura del servizio (1/2)

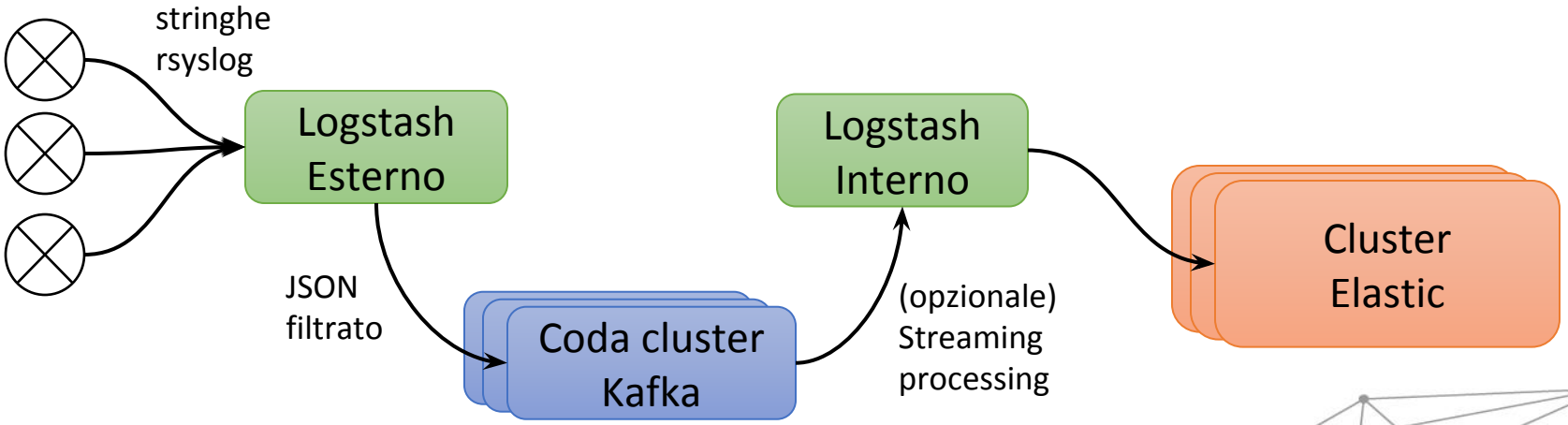
- Erogata e gestita da INFRA

- **Underlay** infrastrutturale virtualizzato
  - Cluster Kubernetes di preproduzione e produzione
  - Deploy automatico con Ansible che pilota vCenter
  - Rancher come piano di controllo
  - vCenter come provider di storage persistente



Architettura del servizio (2/2)

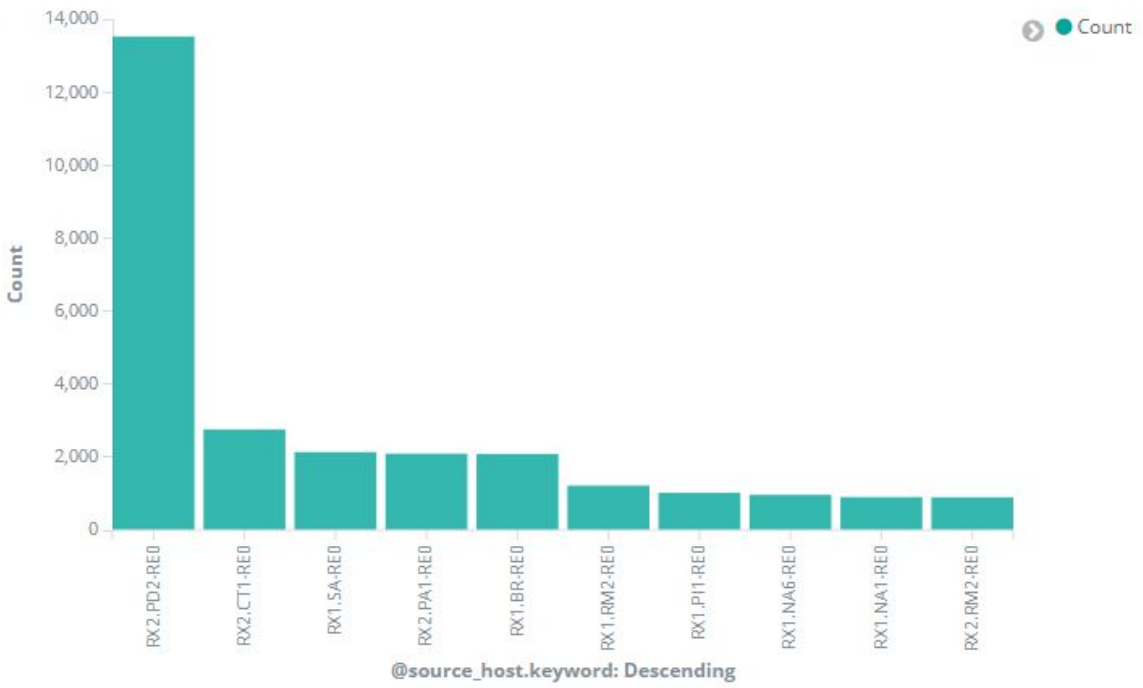
- **Overlay**
  - Deploy automatico su Kubernetes con Helm
  - ELK stack
  - Datalake Elasticsearch, 3 nodi con 450 GB storage ognuno
  - Coda Kafka in input per picchi di carico e maggiore resilienza



Operation e NOC – primi feedback 1/4

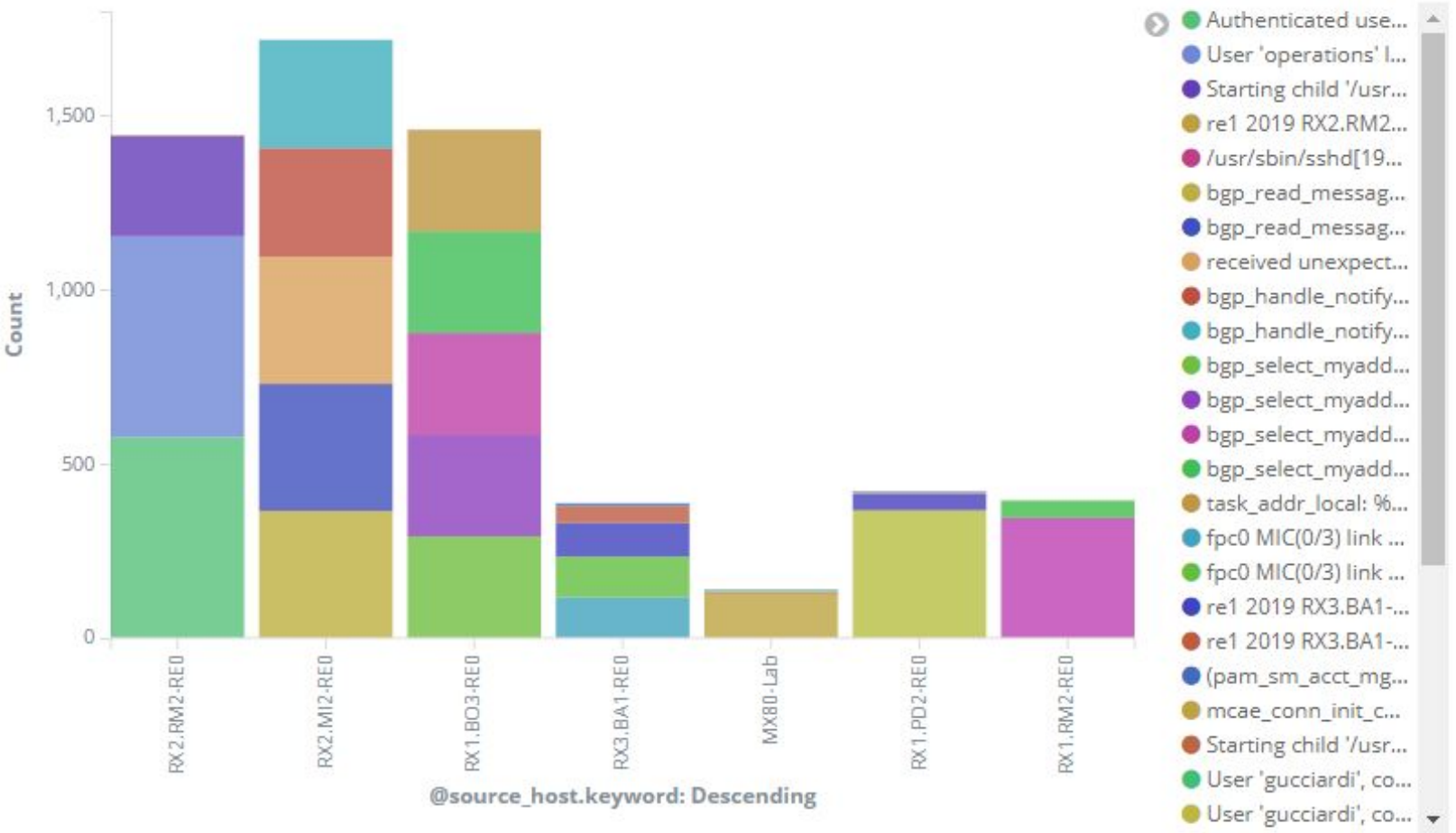
- Setup del target Syslog su tutti i router Juniper della Rete GARR
  - Selezione e configurazione dei log
  - Eliminazione dei log spuri (bachi in processi «chatty» di JunOS)

- **Potenzialità** dello strumento
  - Individuazione router più «rumorosi»



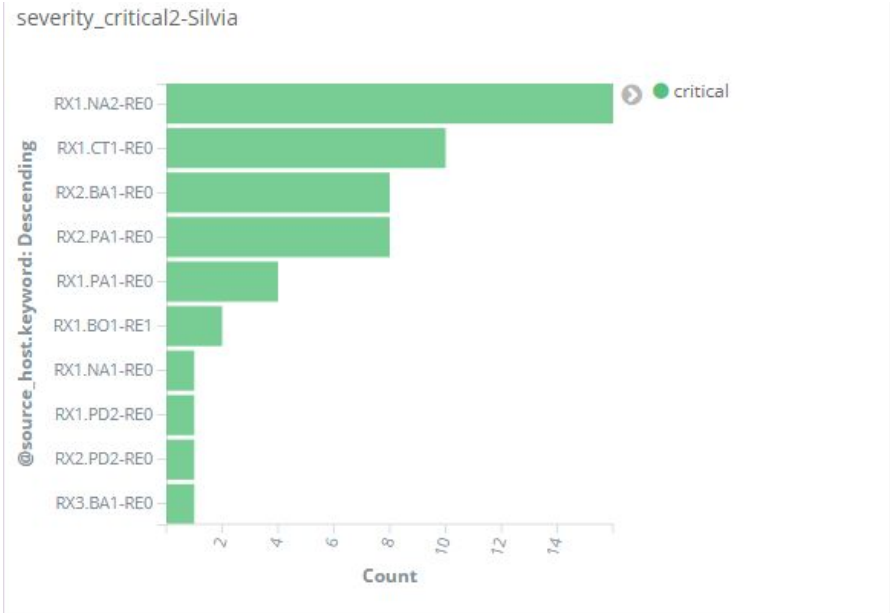
Operation e NOC – primi feedback 2/4

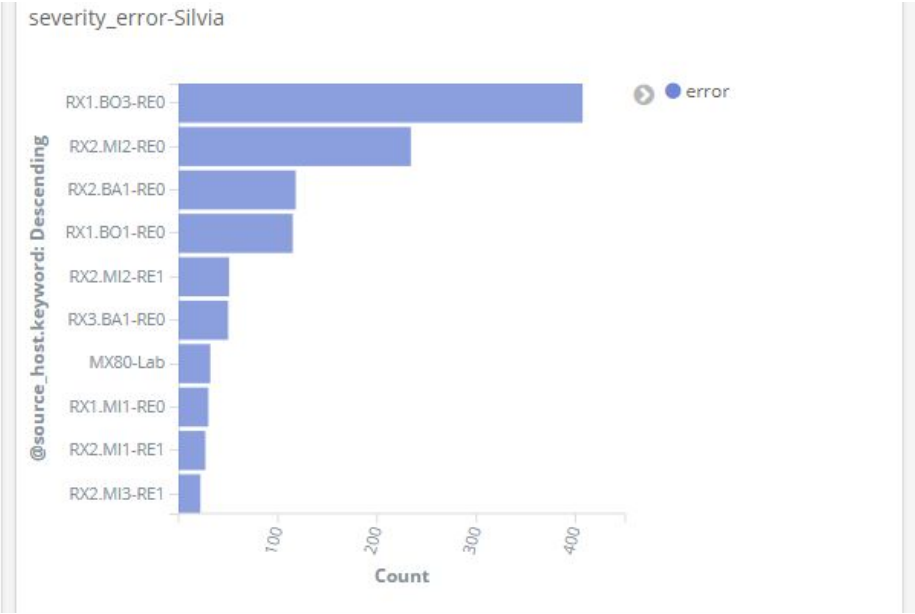
- Saturazione dei log per messaggi ripetuti



Operation e NOC – primi feedback 3/4

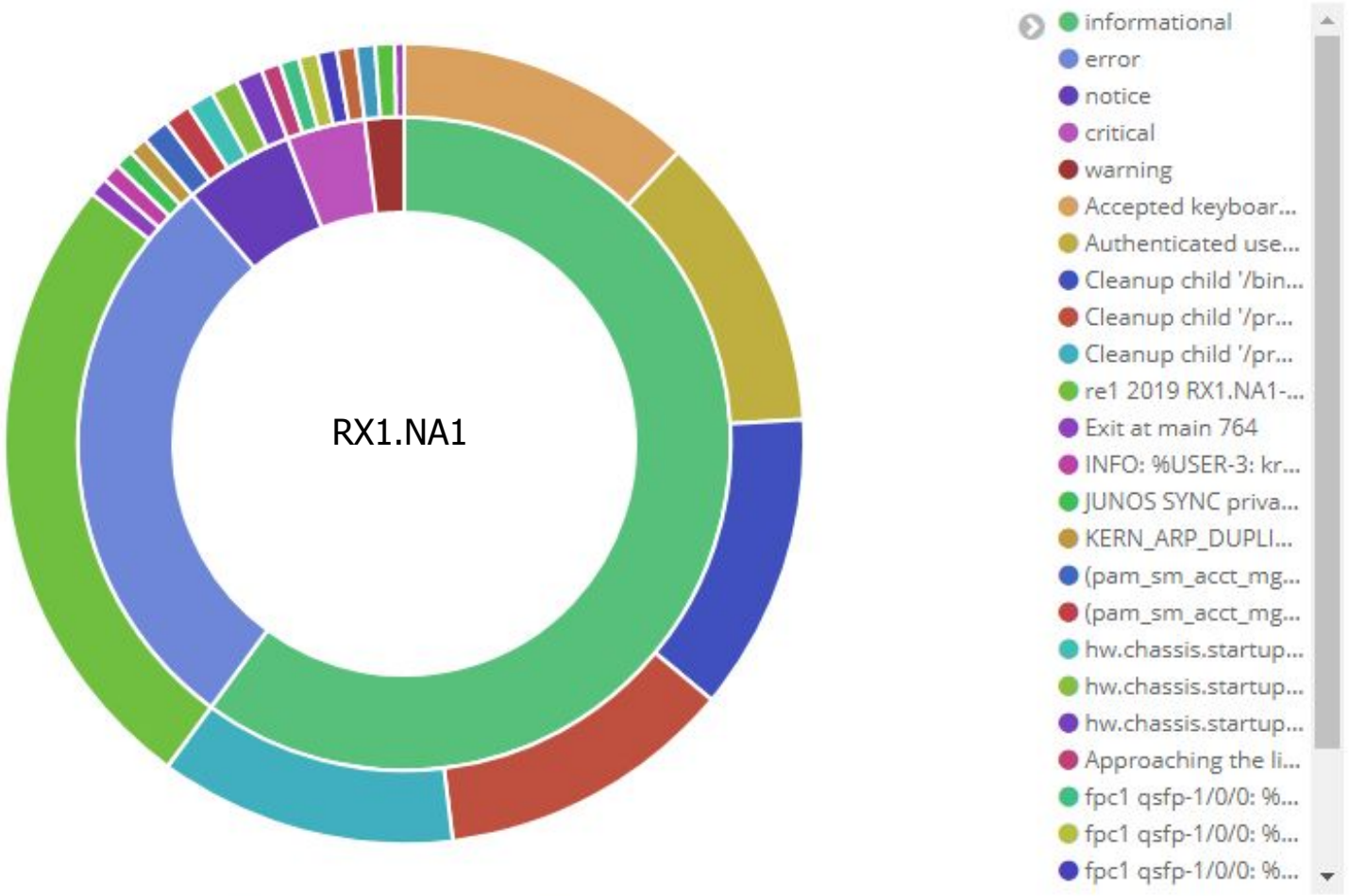
- Monitoraggio dei log a severity maggiore: critical ed error





Operation e NOC – primi feedback 4/4

- Analisi specifica su un singolo apparato



Operation e NOC – considerazioni e prossimi passi

- Circa due mesi di presa dati: 80k eventi/giorno in media, 60 MB/gg
- Eliminazione impurità: -30% dei dati raccolti nei primi giorni

- Rafforzare la collaborazione INFRA-NETOPS
  - Tempo per assimilare funzioni, sintassi e prendere confidenza con il sistema
  - Creazione di opportune dashboard per l'operatore
  - Immaginare il ciclo di sviluppo per query e dashboard

- Funzionalità aggiuntive
  - Acquisizione dei log dai CPE utente e delle trap SNMP
  - Allarmistica e notifica di query periodiche inviate via email
  - AuthN & AuthZ, aree di sviluppo personali delle viste e successiva condivisione

GRAZIE!