THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

WG-SEC-SCAN

Gruppo di lavoro sulla cybersecurity
“Network Auditing”

Ermann Ripepi - ermann.ripepi@imaa.cnr.it
Consiglio Nazionale delle Ricerche - Istituto di Metodologie per l’Analisi Ambientali

Workshop GARR 2017 | Roma, 4-7 Aprile 2017

Gruppo di lavoro

- Inizio attività Settembre 2016
- 22 partecipanti al gruppo, di cui ~8 presenti alle videoconferenze
  - Riunioni generali con cadenza mensile
  - Riunioni specifiche dei sottogruppi in base alle necessità
- Web Application
  - SCARR (NESSUS) https://www.cert.garr.it/servizi/scarr
  - Kali Linux, Parrot Security OS
  - Open Web Application Security Project (OWASP)
- Best Practices di carattere tecnico
  - Hardening = processo di analisi e messa in sicurezza di un host riducendo i punti di attacco
- Analisi dei log e flussi di dati
  - ELK STACK

Analisi dei log e flussi di dati

- ELK Stack (Elastic), perché?
  - Fu proposto durante la creazione dei GdL del WS2016
  - C'erano già competenze all'interno del gruppo
  - È una piattaforma scalabile e flessibile

- Sottogruppo di lavoro "ELK"
  - Francesco Izzi: CNR-IMAA
  - Francesco Sansone: CNR-IFC
  - Fulvio Galeazzi: Consortium GARR
  - Nino Ciurleo: Consortium GARR
  - Ermann Ripepi: CNR-IMAA

Analisi dei log e flussi di dati

- Componenti di ELK
  - Logstash – collettore di dati
  - Elastichsearch – cerca, analizza e archivia i dati
  - Kibana – front end per visualizzare i dati

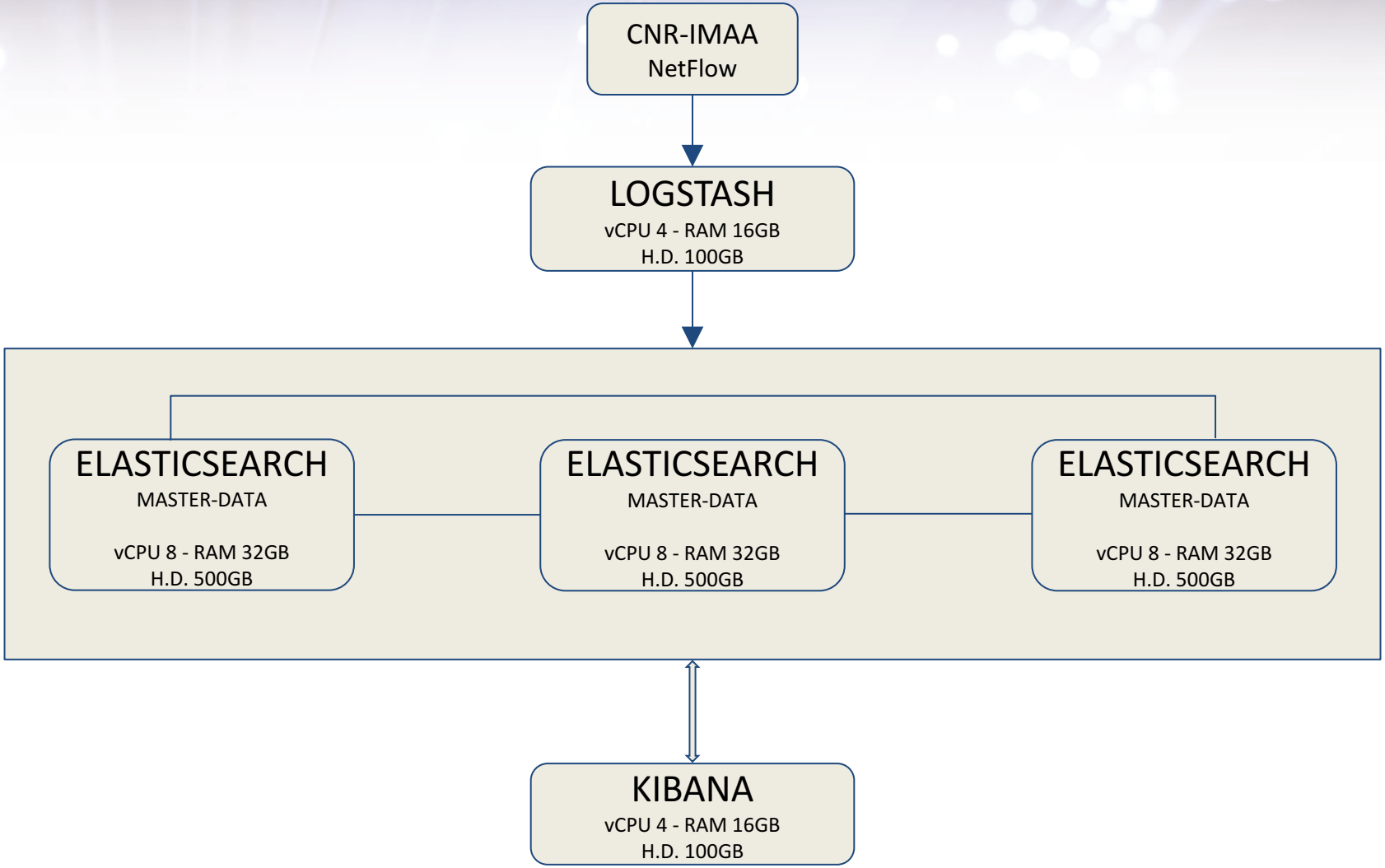
RISORSE UTILIZZATE

- Utilizzo della piattaforma Cloud OpenStack di GARR-X Progress

- 5 virtual machines
  - vCPU 32
  - RAM 128GB
  - Storage 1,7TB (~200GB per servizi e ~1,5TB per archiviazione)

- Sistema Operativo
  - Ubuntu Server 16.04 LTS 64 bit

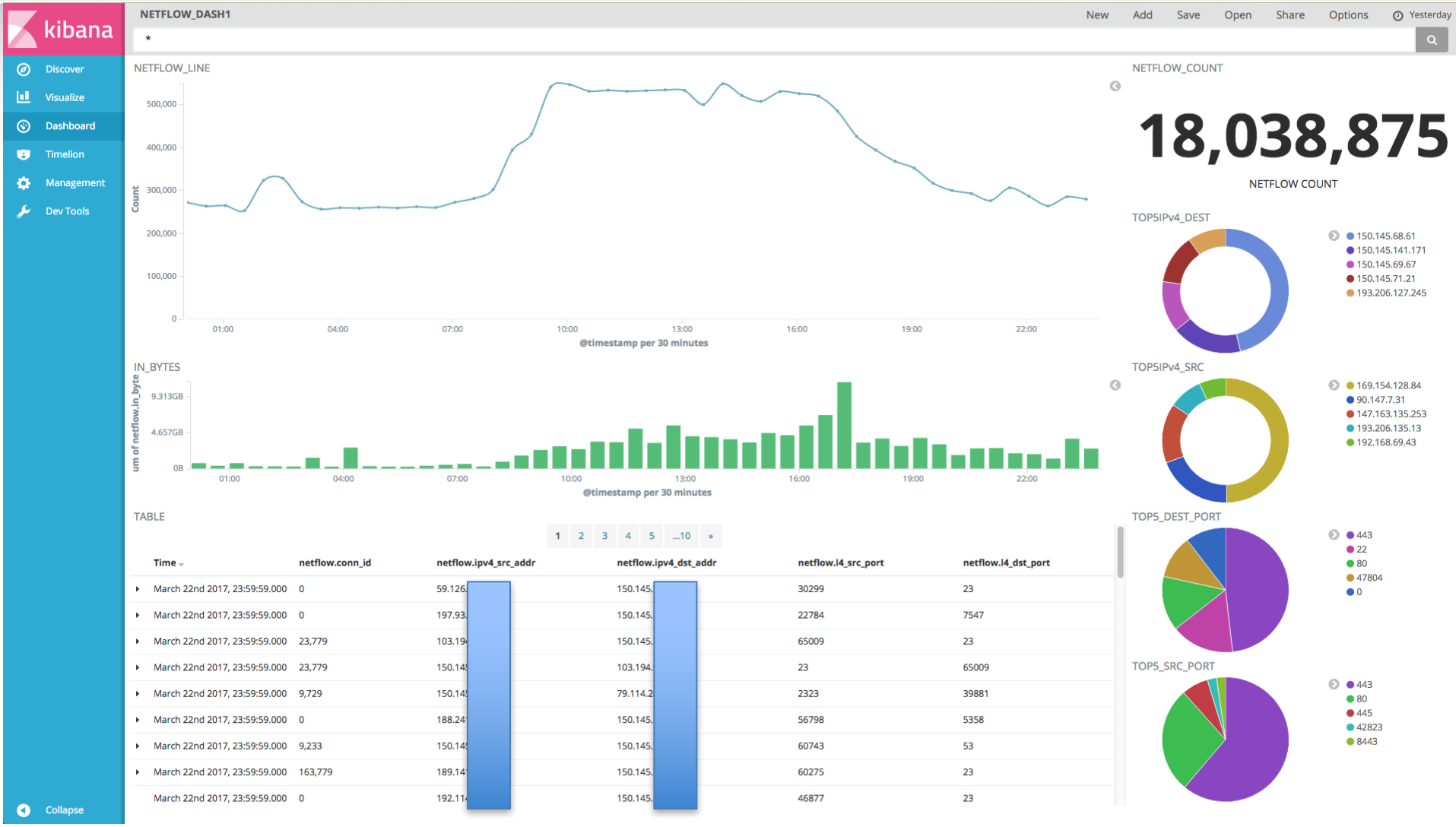
CLUSTER ELK


CNR-IMAA
NetFlow
LOGSTASH
vCPU 4 - RAM 16GB
H.D. 100GB
ELASTICSEARCH
MASTER-DATA
vCPU 8 - RAM 32GB
H.D. 500GB
ELASTICSEARCH
MASTER-DATA
vCPU 8 - RAM 32GB
H.D. 500GB
ELASTICSEARCH
MASTER-DATA
vCPU 8 - RAM 32GB
H.D. 500GB
KIBANA
vCPU 4 - RAM 16GB
H.D. 100GB

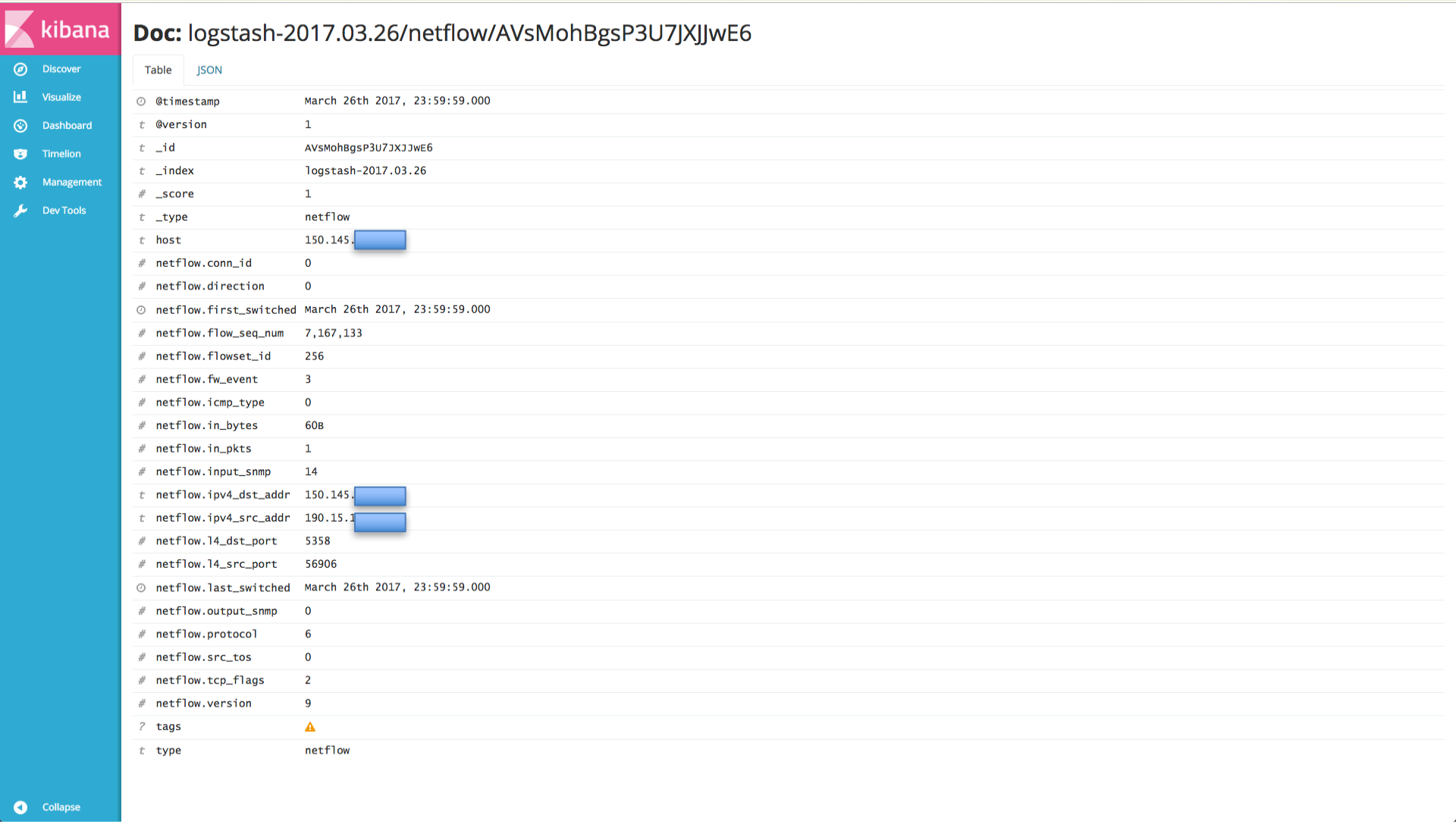
Traffico NetFlow

- Stream di dati campionati 1:1
  - Traffico sede utente ~ 25 Mbps
  - Traffico NetFlow ~ 211 Kbps, ~ 2,28 GB al giorno

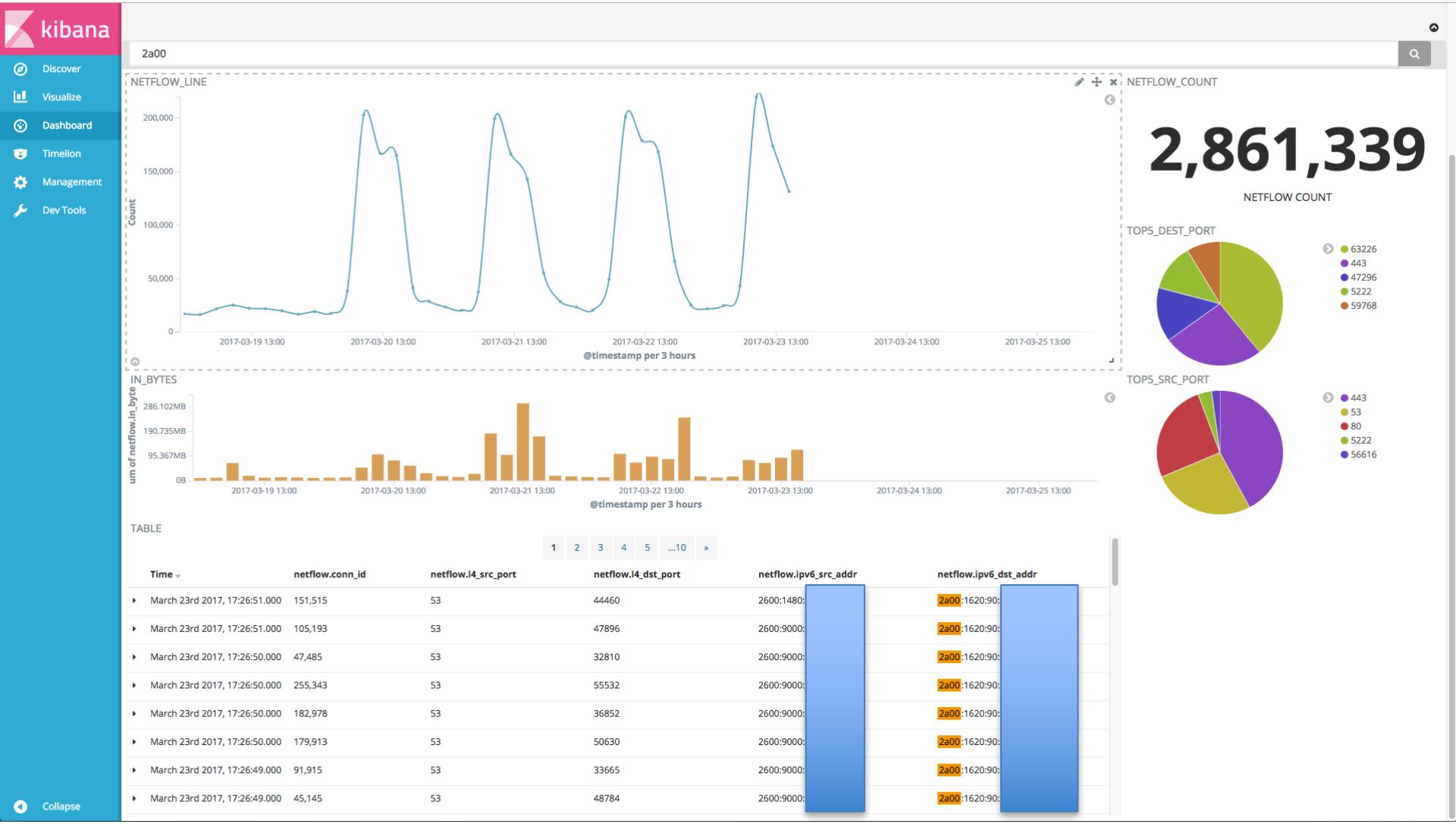
Dashboard NetFlow IPv4



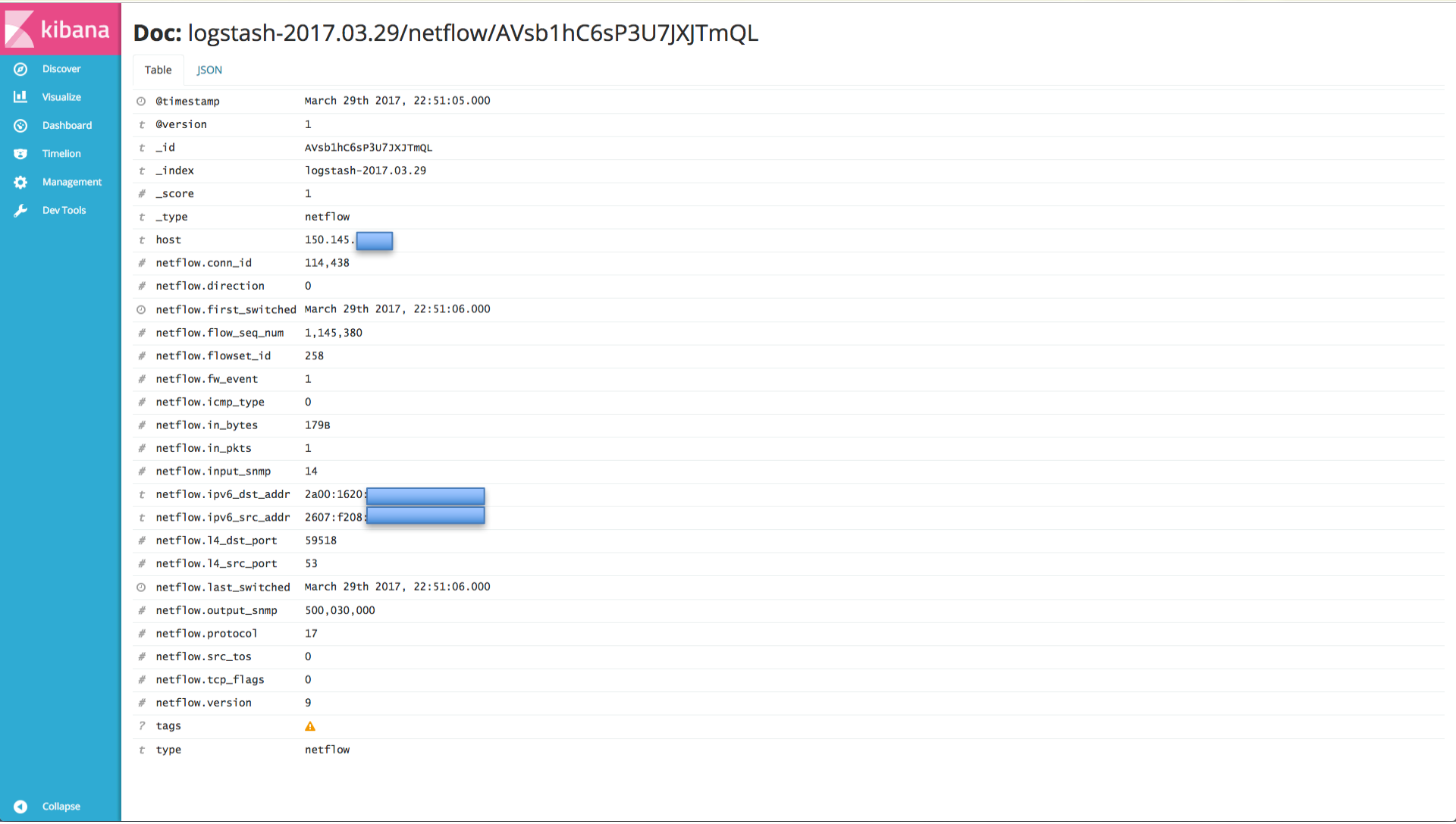
Dashboard NetFlow IPv4



Dashboard NetFlow IPv6



Dashboard NetFlow IPv6



Strategie per il futuro

- ELK STACK
  - Integrare l'analisi dei log (syslog)
  - Configurare sistemi di alert
  - Configurare automatismi che intervengano a seguito di un certo evento
- NTOP
- Continuare il lavoro relativo alle Web Application e Best Practices
- "Popolare" il wiki https://wiki-wg-sec.garr.it

GRAZIE !

wg-sec-scan@garr.it

http://lx1.dir.garr.it/cgi-bin/mailman/listinfo/wg-sec-scan

https://wiki-wg-sec.garr.it