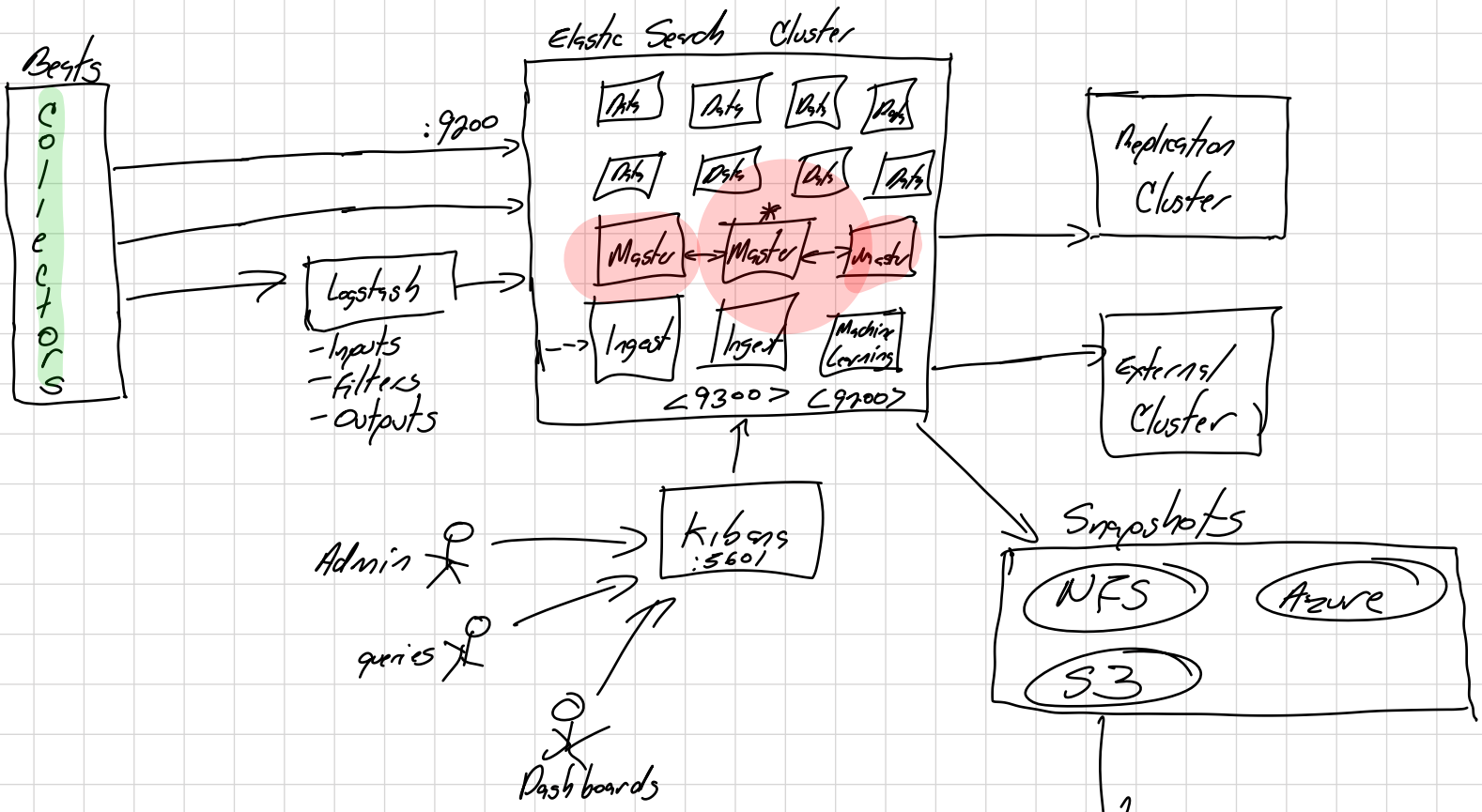
Elastic Search

- ELK (Elasticsearch, Logstash, Kibana)
- Elastic Stack (All + Beats)
  a) Filebeat
  b) Metric Beat
  c) Packet Beat
  d) WinLog Beat
  e) Audit Beat
  f) Heart Beat
  g) Function Beat

Collectors

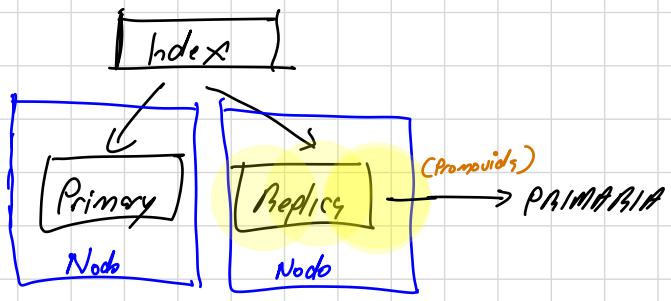
VS

OPENNISTMO
AWS



Elasticsearch:

- BD orientada a documentos (JSON)
- REST API
- Basada en Apache Lucene
- Alta escalabilidad horizontal
- Busquedas Rápidas
- Datos desnormalizados
- No es una BD tradicional
- La información se almacena en índices
- Un índice está integrado por "shards"
  a) Primarios
  b) Replicas
- Las replicas no pueden estar en el mismo nodo que su primario



Cluster Status:

a) Green – Replicas asignadas
b) Yellow – Replicas sin asignar
c) Red – Primario sin asignar (Houston....)

LAB:

- Stack docker-compose
  * 3 master
  * 2 nodos de datos
  * 1 kibana
  * Elasticsearch 7.X
- Uso básico de la API

Deployments

- On premise
- Elastic Cloud
- AWS Managed
- Azure Managed (Nueva)

Recomendaciones:

- Mucha planeación
- Benchmarking
- Asignación de recursos
- Nodos con roles dedicados.