Introducción a ELK

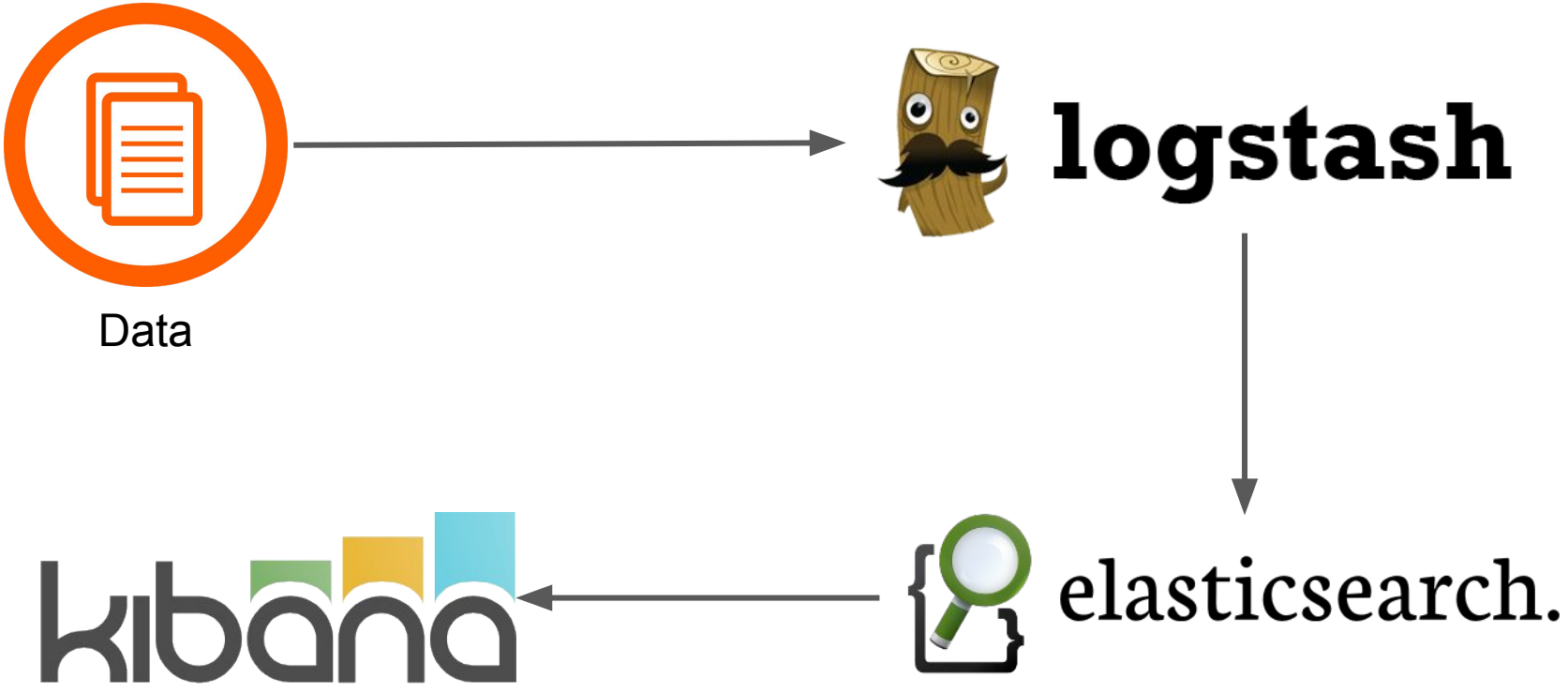
Adrián Santos Marrero <adsaman@gmail.com>

elasticsearch.

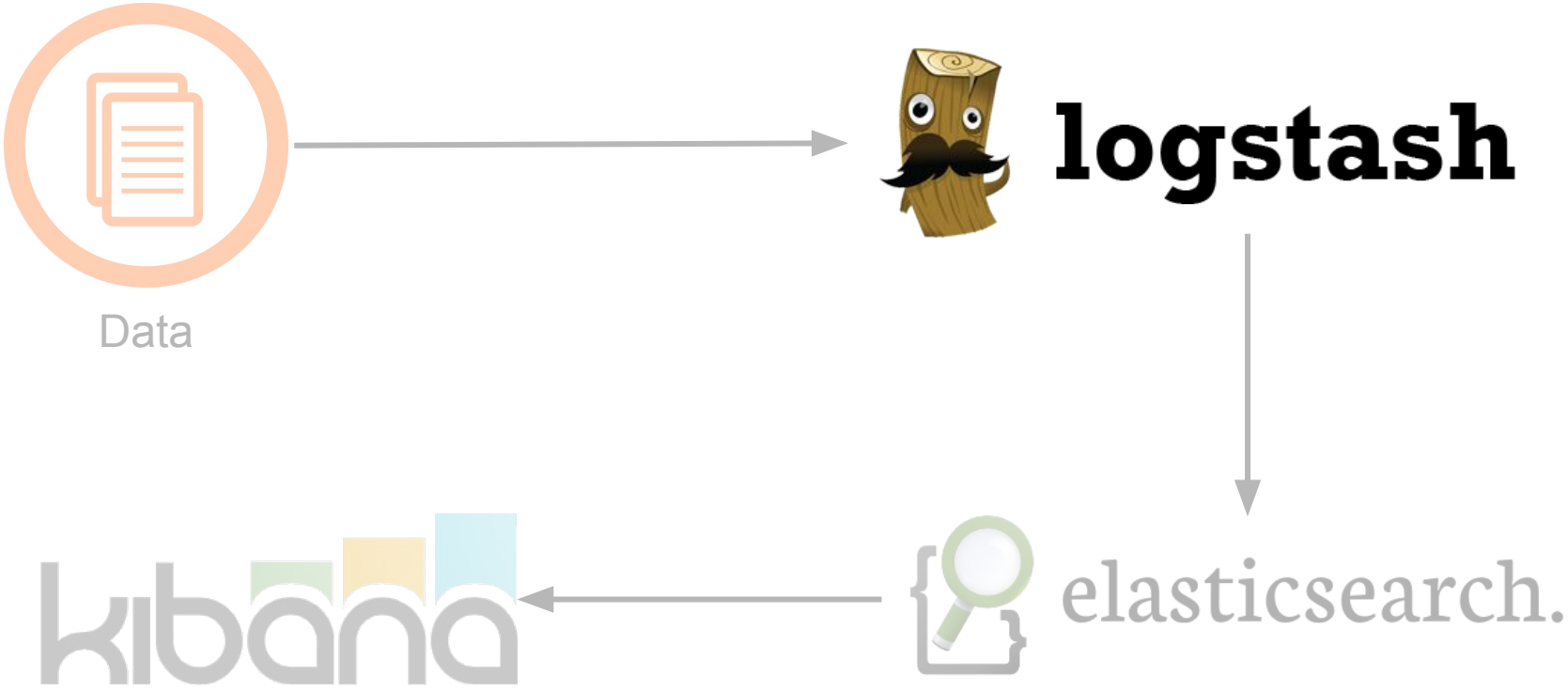
logstash

kibana

Flujo de datos



Flujo de datos



Logstash

- Gestiona eventos y logs
- Recolecta
- Analiza
- Enriquece
- Almacena datos
- Software libre: Licencia Apache 2.0

Arquitectura de logstash

Input

datastore

stream

log files

files

monitoring

queue

network

Filter

parse, enrich, tag, drop

Output

datastore

files

e-mail

pager

monitoring

chat

API

queues

Arquitectura de logstash

Input

datastore

stream

log files

files

monitoring

queue

network

ip: 193.145.120.40

parse, enrich, tag, drop

ip: 193.145.120.40
city: La Laguna
country: ES

Output

datastore

files

e-mail

pager

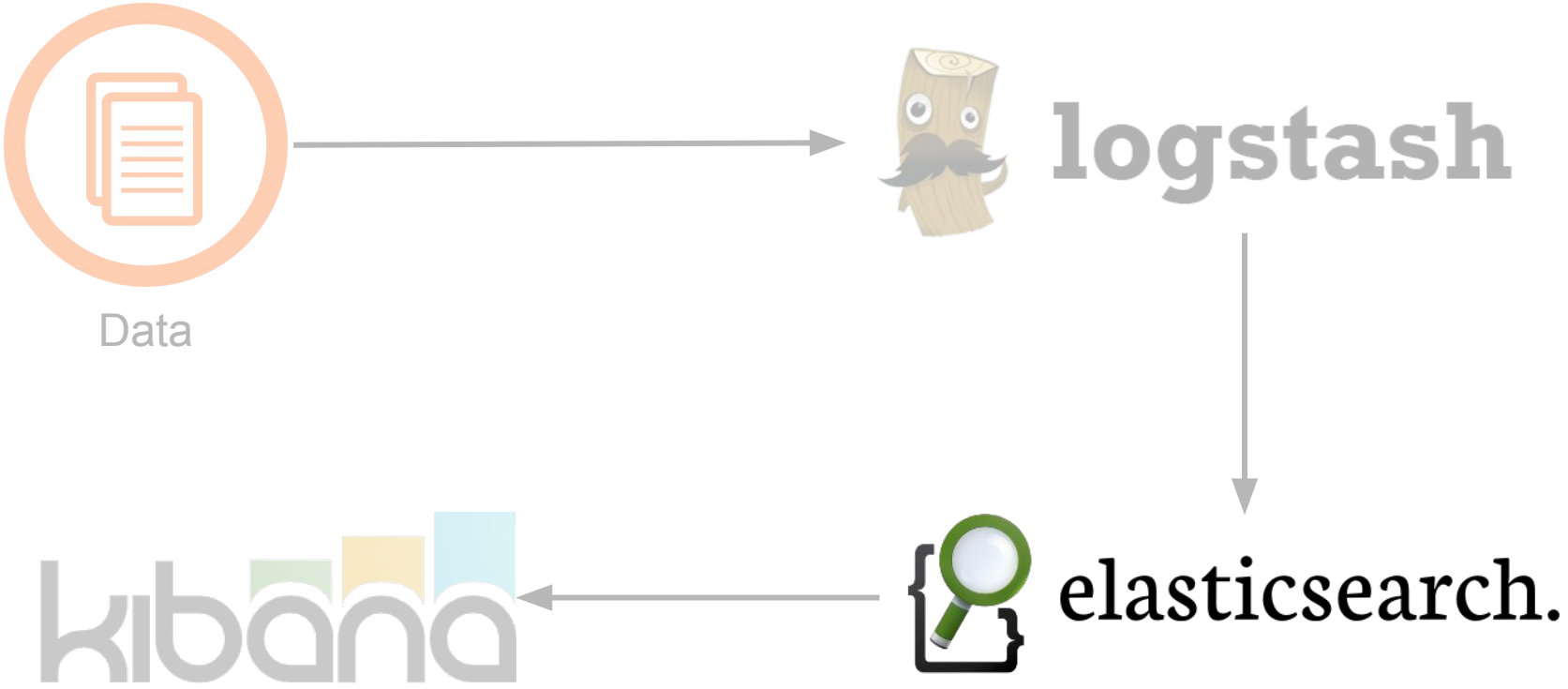
monitoring

chat

API

queues

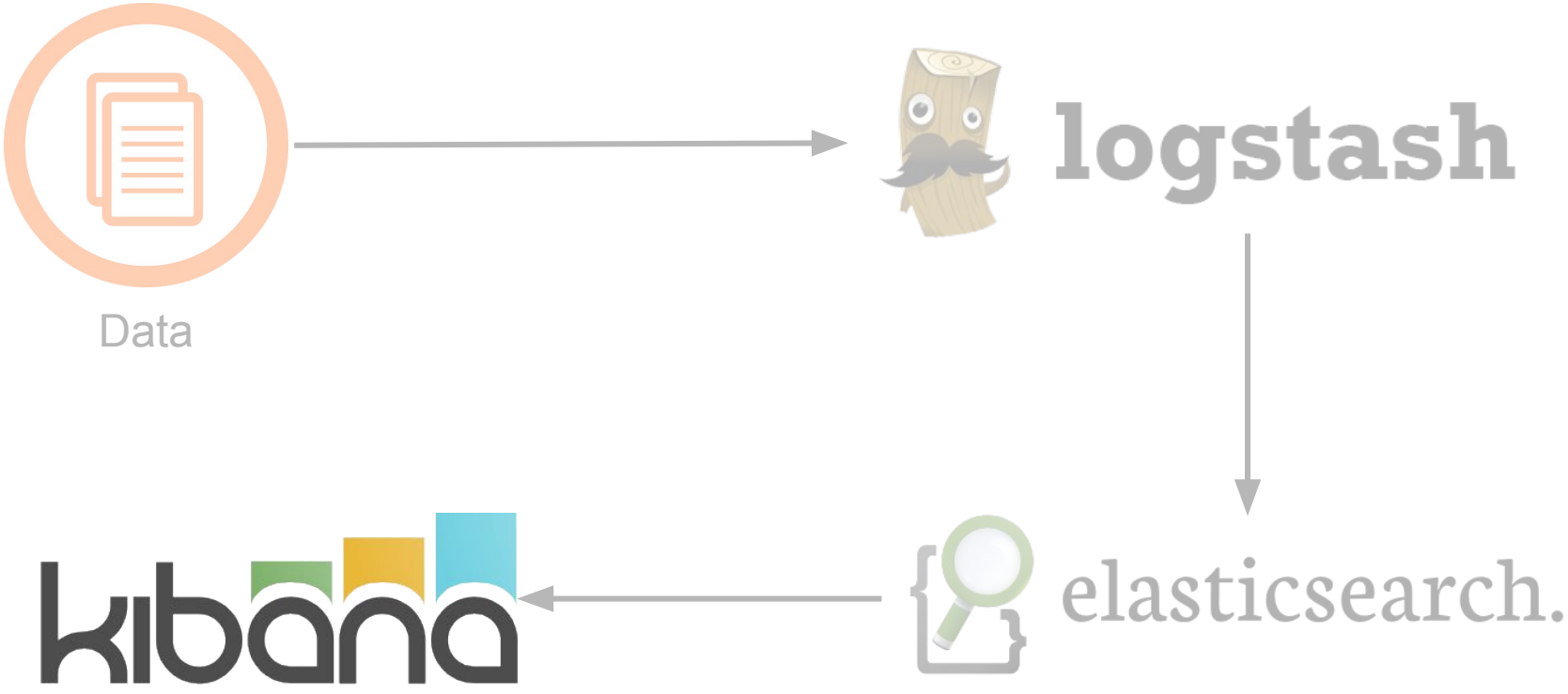
Flujo de datos



Elasticsearch

- Motor de búsqueda distribuido basado en REST y JSON
- Software libre: licencia Apache 2.0
- Lenguaje de búsquedas fácil de entender y muy potente:
  - Búsquedas de texto completo (frase, lógica difusa)
  - Búsqueda numérica (soporta rangos, fechas, direcciones IPv4)
  - Resaltado
  - Aggregations
  - Suggestions

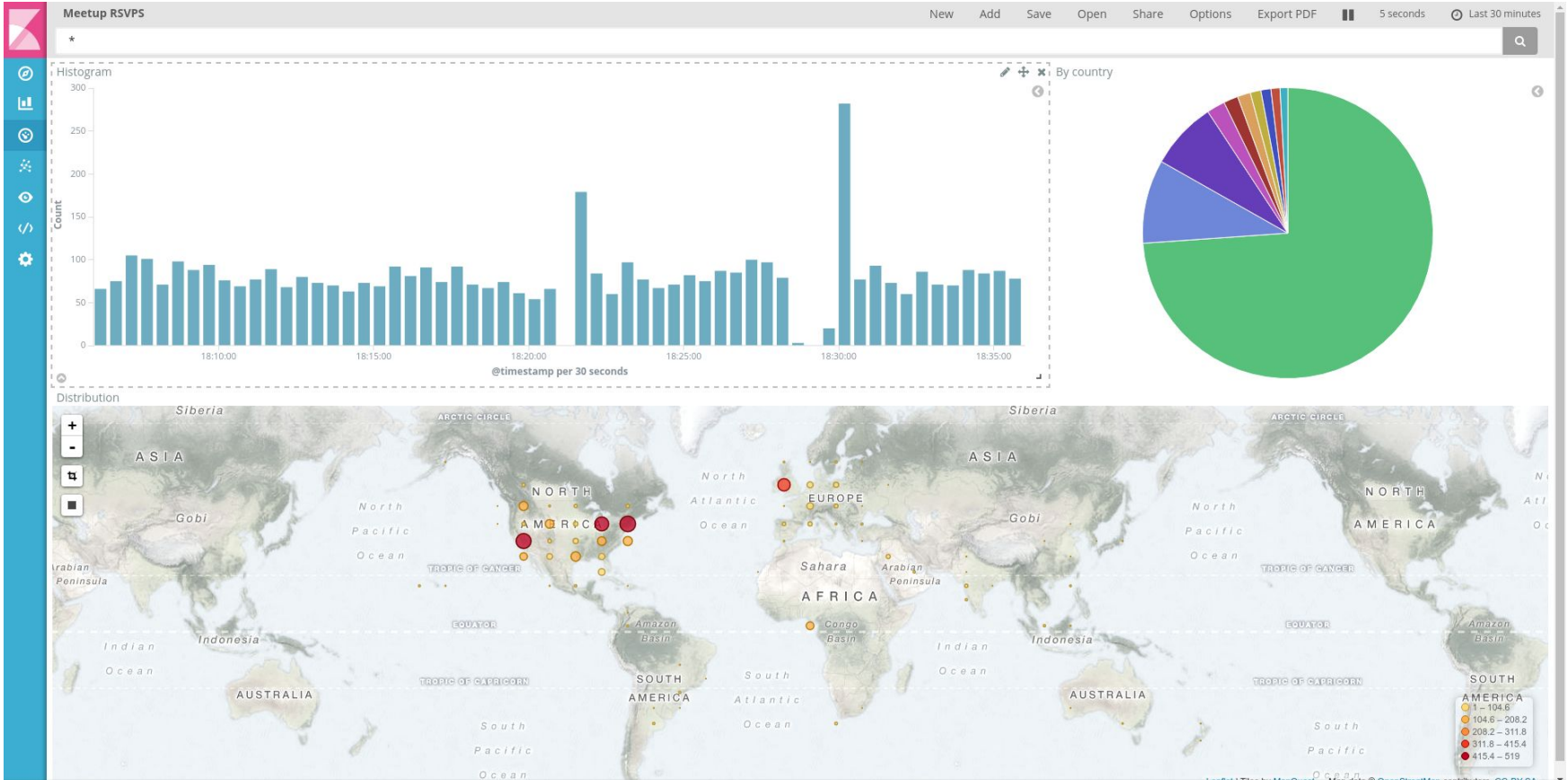
Flujo de datos



Kibana

- Ejecuta consultas sobre los datos y muestra los resultados
- Permite trabajar con widgets
- Compartir/Guardar/Cargar dashboards
- Software libre: licencia Apache 2.0

Kibana


Meetup RSVPS
New
Add
Save
Open
Share
Options
Export PDF
5 seconds
Last 30 minutes
*
Histogram
Count
300
250
200
150
100
50
0
18:10:00
18:15:00
18:20:00
18:25:00
18:30:00
18:35:00
@timestamp per 30 seconds
By country
Distribution
Siberia
ARCTIC CIRCLE
ASIA
NORTH AMERICA
EUROPE
North Atlantic Ocean
North Pacific Ocean
Gobi
Sahara
AFRICA
Arabian Peninsula
TROPIC OF CANCER
EQUATOR
Amazon Basin
Congo Basin
Indonesia
Indian Ocean
AUSTRALIA
SOUTH AMERICA
South Atlantic Ocean
South Pacific Ocean
TROPIC OF CAPRICORN
1 – 104.6
104.6 – 208.2
208.2 – 311.8
311.8 – 415.4
415.4 – 519

Ejemplos ...

¿Preguntas?