

Introducción a ELK

Adrián Santos Marrero <adsaman@gmail.com>



elasticsearch.



logstash



Flujo de datos



Data



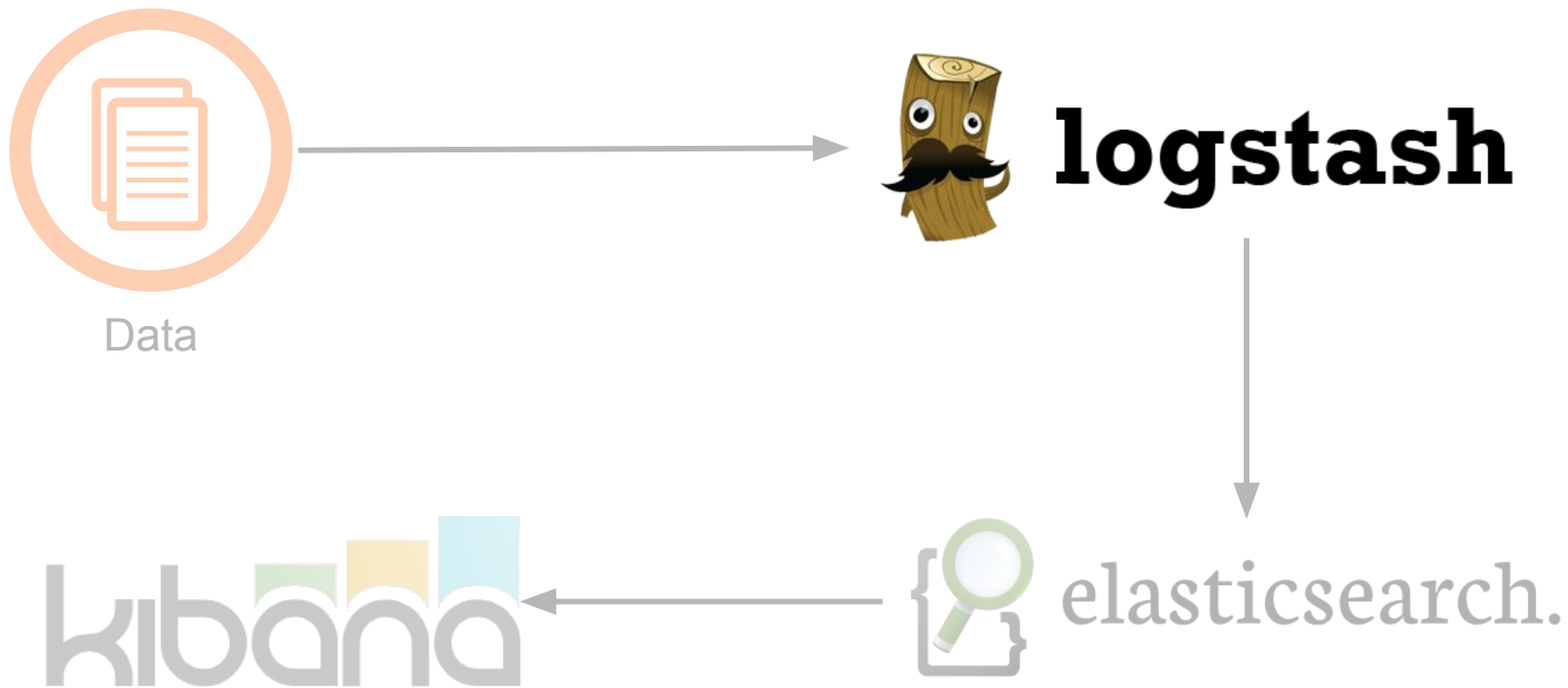
logstash



elasticsearch.



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



Filter



parse, enrich, tag, drop

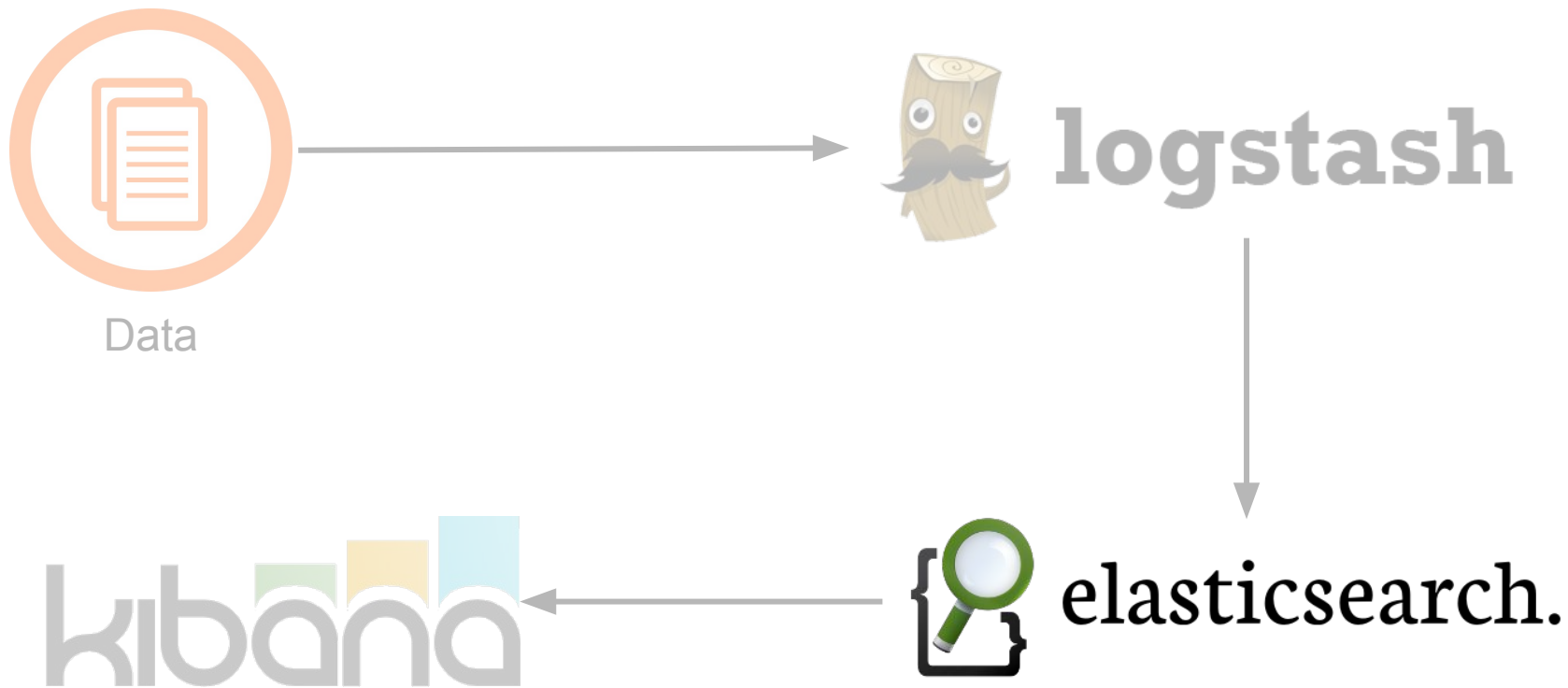
Output

datastore
files
e-mail
pager
monitoring
chat
API
queues

ip: 193.145.120.40
city: La Laguna
country: ES



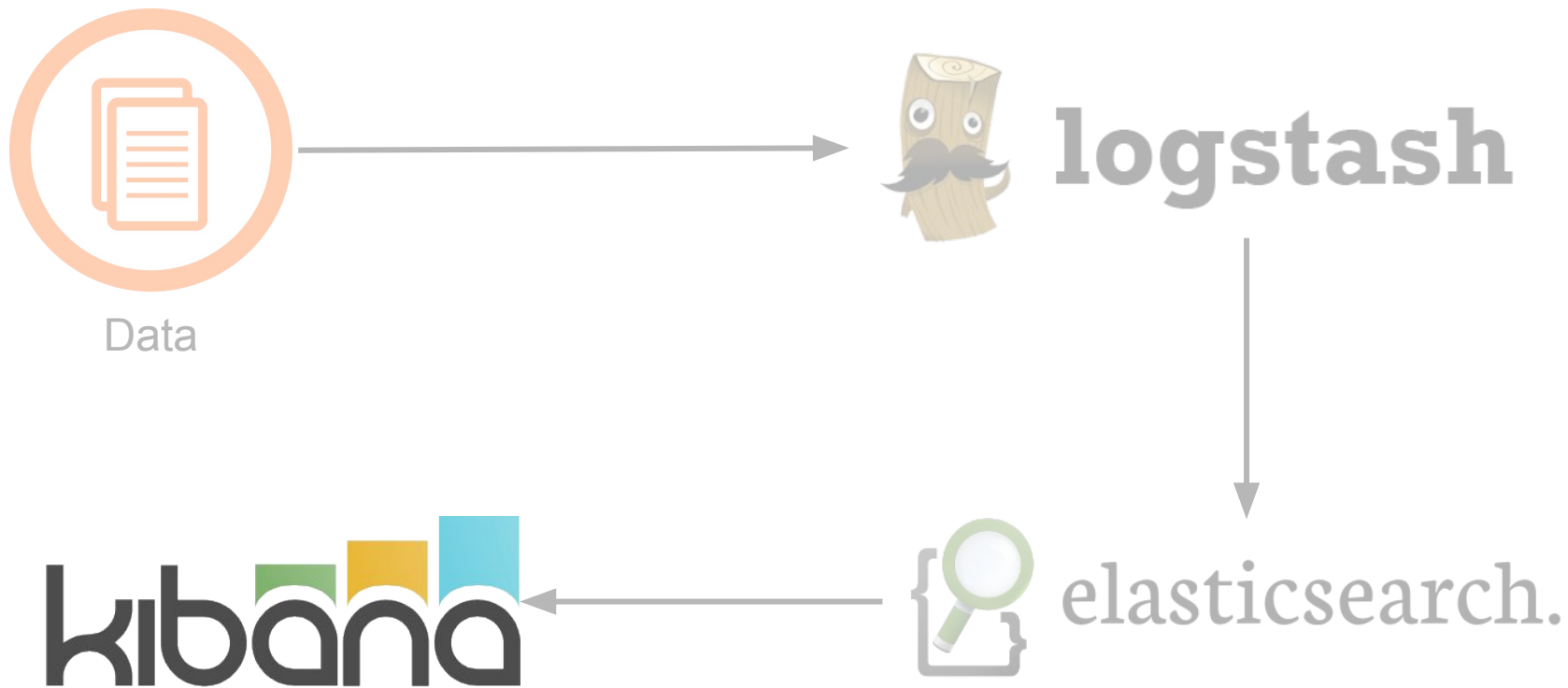
Flujo de datos



Elasticsearch

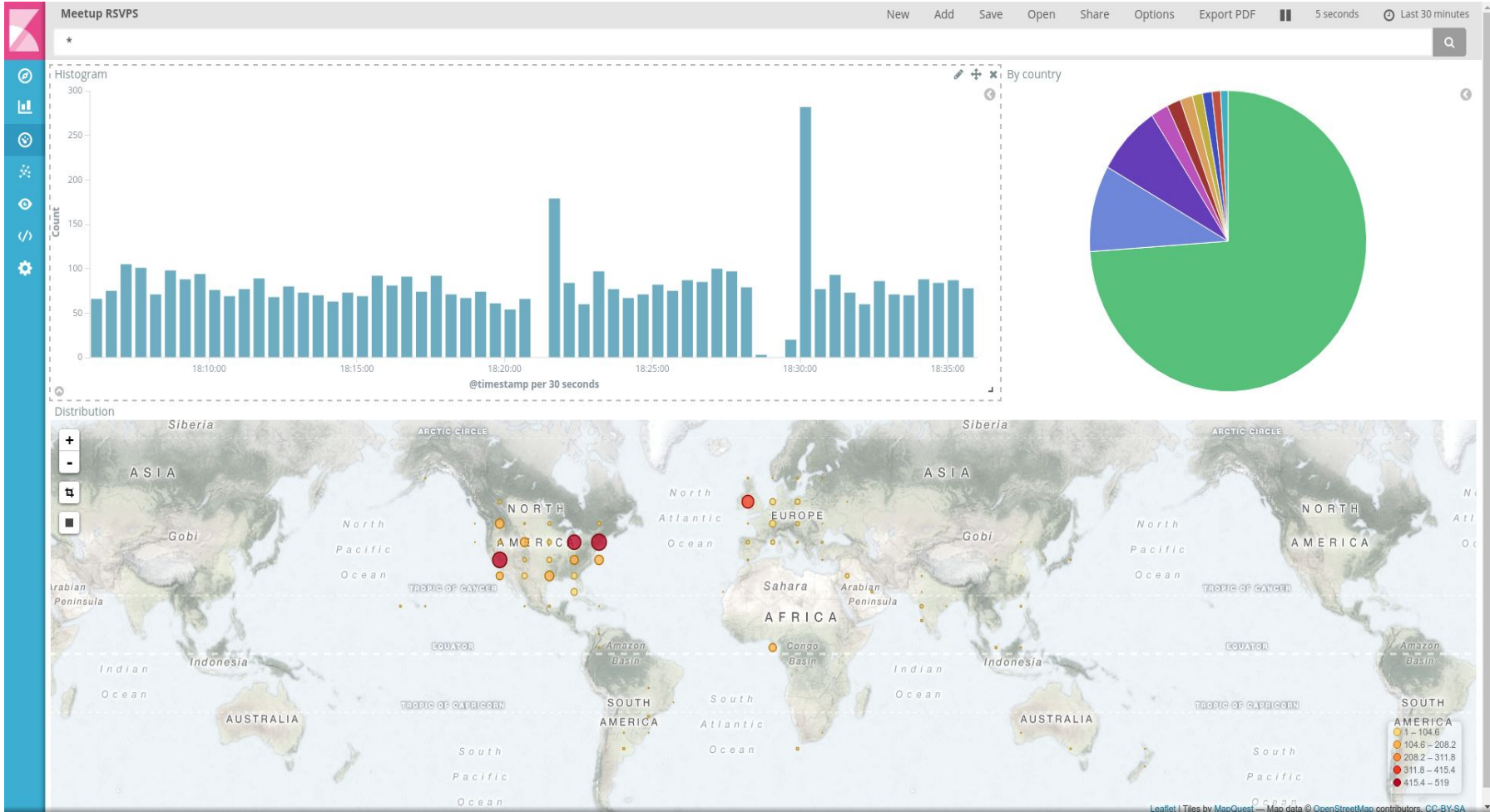
- Motor de búsqueda distribuido basado en REST y JSON
- Software libre: licencia Apache 2.0
- Lenguaje de búsquedas fácil de entender y muy potente:
 - Búsquedas de texto completo (frase, lógica difusa)
 - Búsqueda numérica (soporta rangos, fechas, direcciones IPv4)
 - Resaltado
 - Aggregations
 - Suggestions

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



Ejemplos ...

Iniciar el servicio de Elasticsearch

- `vagrant init adsaman/elk`
- `vagrant up --provider virtualbox`
- `vagrant ssh`
- `sudo service elasticsearch start`
- `sudo tail -f /var/log/elasticsearch/elasticsearch.log`

Primeras consultas...

- Comprobar si se está ejecutando ES:
 - `curl -XGET localhost:9200/`
- Estado del cluster:
 - `curl -XGET localhost:9200/_cat/health?v`
- Listar los índices:
 - `curl -XGET localhost:9200/_all/_settings?pretty`
 - `curl -XGET localhost:9200/_cat/indices?v`

Kibana

- Iniciar el servicio:
 - `sudo /etc/init.d/kibana start`
- Comprobar los logs:
 - `sudo tail -f /var/log/kibana/kibana.std*`
- Acceder a <http://localhost:5601/>
- En la versión 5 incorpora una consola (antiguo Sense)

X-Pack: Extension Pack for the Elastic Stack

- Paquete con varios plugins para ES/Kibana
- Incluye:
 - **Security:** ACL, encriptación, filtrado de IP, auditorías, etc.
 - **Monitoring:** informa del estado del cluster, índices, nodos, etc.
 - **Watcher:** alertas y notificaciones
 - **Reporting:** generación de informes
 - **Graph:** grafos que representan la relación entre diferentes términos
- <https://www.elastic.co/guide/en/x-pack/current/index.html>

URL de búsquedas


- Todos los elementos del índice meetups2, tipo meetup:
 - `curl "http://localhost:9200/meetups2/meetup/_search"`
- Respuestas a meetups en España :
 - `curl "/meetups2/_search?q=group.group_country:es"`
- Búsqueda de texto completo:
 - `curl "/meetups2/_search?q=museos&_source_include=event.event_name"`

Inverted index

- ES utiliza índices “invertidos” para acelerar las búsquedas de texto completo
- Lista de todas las palabras apuntando a los documentos donde aparecen
- El contenido de los documentos se debe “tokenizar” y normalizar

Analyzer


```
GET /_analyze
{
  "analyzer": "standard",
  "text": "El caballo blanco de Santiago"
}
```

A diagram consisting of a horizontal arrow pointing from the request box on the left to the response box on the right, with a vertical line segment extending upwards from the arrow's tail.

```
"tokens": [
  {
    "token": "el",
    "start_offset": 0,
    "end_offset": 2,
    "type": "<ALPHANUM>",
    "position": 0
  },
  {
    "token": "caballo",
    [...]
  },
  {
    "token": "blanco",
    [...]
  },
  {
    "token": "de",
    [...]
  },
  {
    "token": "santiago",
    [...]
  }
]
```

Analyzer

```
GET /_analyze
{
  "analyzer": "spanish",
  "text": "El caballo blanco de Santiago"
}
```

A horizontal arrow points from the right side of the input request box to the left side of the output response box, indicating the flow of data from the request to the response.

```
{
  "tokens": [
    {
      "token": "caball",
      "start_offset": 3,
      "end_offset": 10,
      "type": "<ALPHANUM>",
      "position": 1
    },
    {
      "token": "blanc",
      "start_offset": 11,
      "end_offset": 17,
      "type": "<ALPHANUM>",
      "position": 2
    },
    {
      "token": "santiag",
      "start_offset": 21,
      "end_offset": 29,
      "type": "<ALPHANUM>",
      "position": 4
    }
  ]
}
```

Referencias

- Empresa detrás de todo este software:
 - <http://www.elastic.co>
- Documentación:
 - <https://www.elastic.co/guide/index.html>
- Libro “Elasticsearch: The Definitive Guide”:
 - <https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html>

¿Preguntas?

Conceptos de Elasticsearch

- Los documentos son inmutables
- No se puede modificar un tipo de datos
 - Hay que crear un nuevo índice y re-indexar todo el contenido