



Primeros pasos con Elasticsearch y el Elastic Stack

Enrique V. Kortright

27 de enero de 2021

Primer meetup del grupo de usuarios de
Elastic (EUG) de Costa Rica



Conéctese con la comunidad de Elastic

Existen User Groups en Costa Rica,
Mexico, Colombia, Argentina y Uruguay -
encuentra el tuyo:



- <https://community.elastic.co/>

User Group Virtual:



- <https://community.elastic.co/amer-virtual/>

Agenda

- La experiencia es la búsqueda
- Sitios con gran experiencia de búsqueda
- Detrás del escenario se encuentra Elasticsearch
- Elasticsearch es parte de el Elastic Stack
- Ejercicio: CRUD y búsqueda
- Funcionamiento de Elasticsearch: relevancia y velocidad
- Ejercicio: Creación de una experiencia de búsqueda
- Preguntas y respuestas
- Episodios futuros: Kibana y Logstash/Beats

La experiencia es la búsqueda

The screenshot shows the homepage of Mercado Libre (mercadolibre.co.cr). At the top, there's a yellow header with the Mercado Libre logo, a search bar, and links for 'Categorías', 'Historial', 'Vender', and 'Ayuda'. Below the header, there's a large banner with the text '¡Encuentra lo que buscas!' and 'Hay miles de productos publicados, las mejores marcas y los precios más bajos.' followed by images of various products like a toy car, makeup, a smartphone, a game controller, and flowers. A section for 'Categorías populares' follows, displaying icons and names for categories such as Vehículos, Animales y Mascotas, Autos, Motos y Otros, Celulares y Teléfonos, Computación, Cámaras y Fotografía, Agro, Arte y Antigüedades, Bebés, Coleccionables y Hobbies, Consolas y Videojuegos, and Deportes y Fitness.

The screenshot shows a browser window displaying the Elastic Blog page (elastic.co.es/blog). The URL in the address bar is elastic.co.es/blog. The page has a blue header with a search bar containing 'Blog'. Below the header, there's a list of articles with titles, dates, and brief descriptions. Some visible titles include 'Previewing Native Support for Java Plugins in Logstash' (29 - 01 2019), 'Elasticsearch: Java 9 and Beyond' (06 February 2018), 'Elasticsearch Java Clients' (14 December 2016), 'Monitoring Java applications and Getting started with the Elastic APM Java Agent' (02 September 2020), and 'Meet the New Logstash Java Execution Engine' (13 June 2018). On the right side of the page, there's a sidebar with a dark blue background featuring a magnifying glass icon and some small preview images.

The screenshot shows the homepage of the Rappi delivery app (rappi.co.cr). The top navigation bar includes the Rappi logo, a search bar with the placeholder 'Busca cualquier producto', and a 'Ingresar dirección' button. The main headline reads 'Pedí en supermercados, restaurantes y mucho más.' Below this, there are several icons representing different delivery categories: a burger, a shoe, an avocado, and a donut. A text box says 'CONSIGUE LO QUE NECESITAS' and 'Nuestras tiendas'. Below this, there are six cards with icons: 'Restaurantes' (burger), 'Tiendas y Super' (grocery cart), 'Licores' (bottles), 'Conveniencia' (fresh market logo), 'Gift Cards' (gift card), and 'Ver más' (more).

Denominador común de una gran experiencia de búsqueda

¿Qué tienen en común todos estos sitios?

- Fácilmente encuentro lo que busco
 - Con tan solo unos pocos términos
- Obtengo resultados de alta relevancia
 - Los mejores resultados aparecen al principio
- Obtengo resultados rápidamente
 - La respuesta aparece normalmente en milisegundos

Casos de uso de Elasticsearch <https://www.elastic.co/customers/>

Observability

 **ZURICH**

Zurich Insurance increases customer trust and underwrites the future with Elastic

Zurich speeds up time to market for new insurance products and services with Elastic. Moving to Elastic Cloud on Kubernetes empowers staff to resolve claims quickly, increasing customer satisfaction and trust.

[Read case study](#) ➔



 **P&G**

Proactive optimization at Procter & Gamble Cloud Enterprise with Elastic

Elastic is a part of the toolset provided to ACC by the Cyberspace Vulnerability Assessment/Hunter Program Office for Defensive Cyber Operations.

[Watch video](#) ➔

 **U.S. AIR FORCE**

Air combat command enables mission defense teams with Elastic

Elastic is a part of the toolset provided to ACC by the Cyberspace Vulnerability Assessment/Hunter Program Office for Defensive Cyber Operations.

[Watch video](#) ➔



 **NetApp**

NetApp uses machine learning to fight cyber threats and power security analytics

[Watch video](#) ➔

 **UNIVERSITY OF OXFORD**

University of Oxford protects devices, users, and network with the Elastic Stack

[Watch video](#) ➔

Enterprise Search

 **happyfresh**

HappyFresh scales with COVID-19 shopping surge, handles jump in ecommerce traffic with App Search on Elastic Cloud

HappyFresh increased sales, revenue, and improved the customer shopping experience due to App Search on Elastic Cloud's regional storage capabilities that reduced search latency by half.

[Read case study](#) ➔



 **H-E-B**

H-E-B provides a better shopping experience with faster, relevant app search

[Watch video](#) ➔

 **INGRAM MICRO**

Ingram Micro speeds up searches and boosts conversions with Elastic

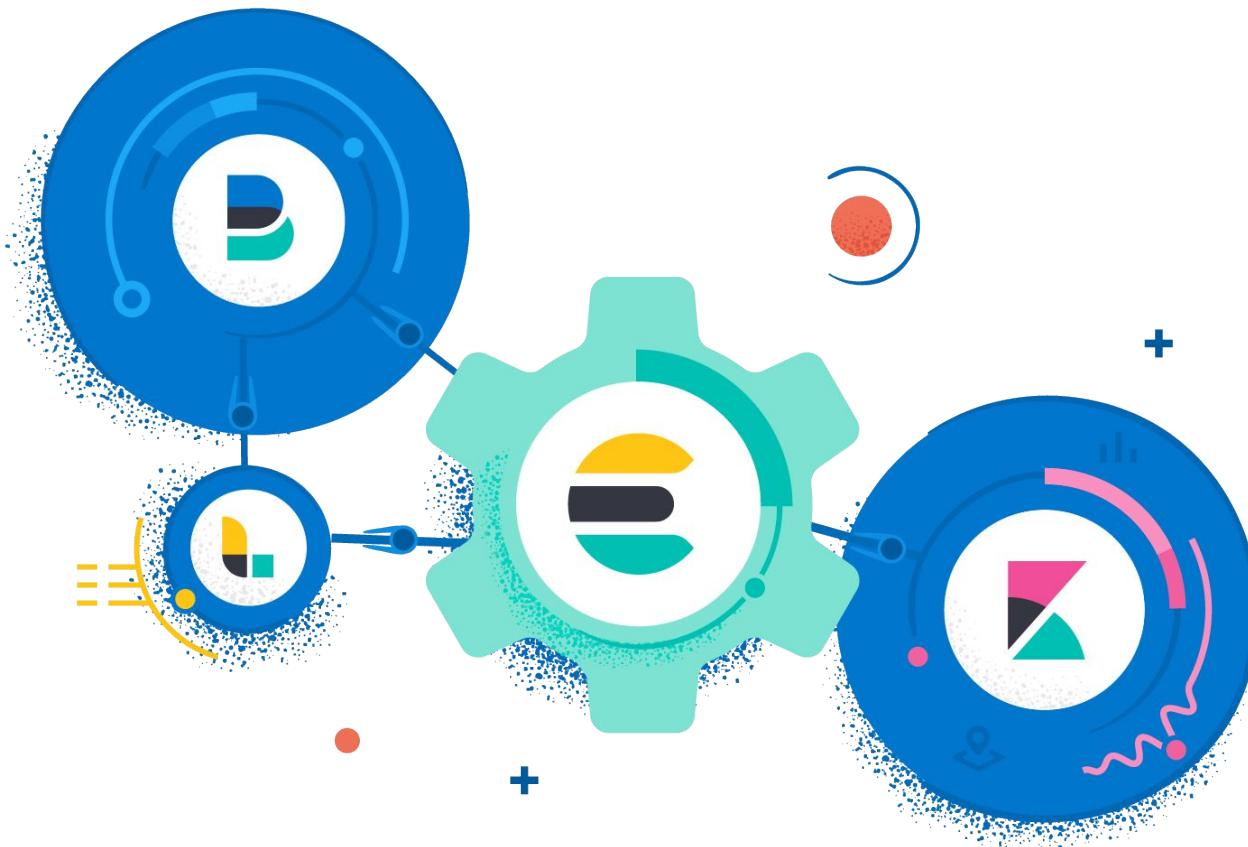
[Read case study](#) ➔

[All security stories](#)

[All enterprise search stories](#)



Elasticsearch es parte del Elastic Stack



El Stack de Elastic

Casos de uso



Elastic Stack

Kibana



Visualiza, analiza, administra y alerta

Elasticsearch



Guarda, busca y procesa

Beats



Logstash



Captura, enriquece, transforma y carga

SaaS

Elastic Stack

- Elasticsearch
 - es un almacén de documentos de JSON
 - es una máquina de búsqueda de alto rendimiento
 - Maneja y procesa los datos a través de una serie de APIs de REST
- Kibana
 - es la interfaz de usuario (UI)
 - proporciona operaciones de administración y monitoreo de un cluster de Elasticsearch
 - proporciona funciones de visualización en tiempo casi-real
 - proporciona UIs para trabajos de aprendizaje de máquina
 - proporciona UIs especializadas para áreas que incluyen observabilidad, seguridad, aprendizaje de máquina, visualización de datos geoespaciales, infográficos usando Canvas, grafos de relaciones entre objetos y otras más
- Logstash
 - es la herramienta de transformación, enriquecimiento y carga de datos
 - puede jalar y empujar datos almacenados en fuentes muy diversas como bases de datos
- Beats
 - son agentes ligeros (generalmente) desplegados en el punto de origen de datos
 - se encargan de capturar logs, métricas o trazas y enviarlos a Elasticsearch directamente o a través de Logstash

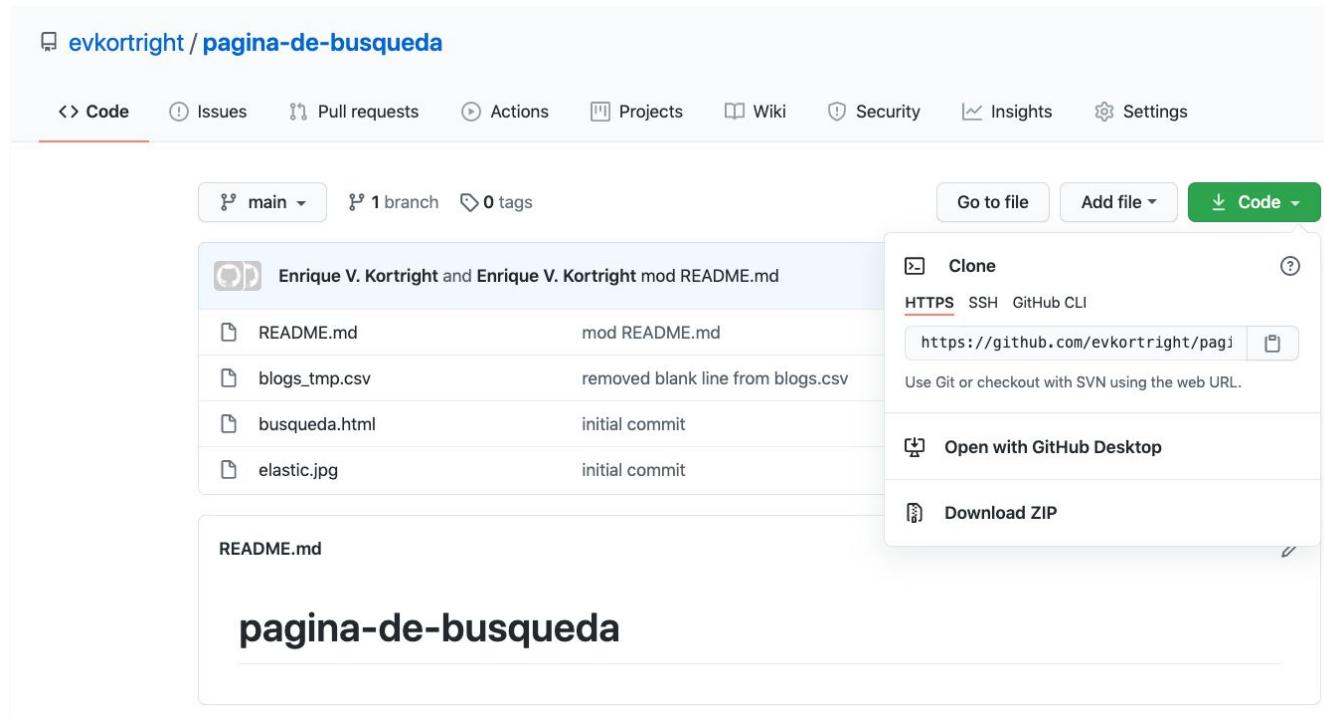
Plan de esta serie de primeros pasos

- En este episodio nos enfocamos en Elasticsearch
 - Creación, lectura, actualización, y borrado de datos (CRUD) individualmente o a granel
 - El lenguaje de dominio específico (DSL) de Elasticsearch
 - El lenguaje de búsqueda para hacer consultas
 - Diseño de una gran experiencia de búsqueda
- En el segundo episodio exploramos Kibana
- En el tercer episodio nos enfocamos en Logstash y Beats

Ejercicio: Configura tu deployment de Elasticsearch y lanza Kibana

Paso. Baja el proyecto

- Ve a <https://github.com/evkortright/pagina-de-busqueda> y baja el archivo zip o haz un clon del proyecto



Configura tu deployment de Elasticsearch

- Ingresa a tu cuenta de nube de Elastic en <https://cloud.elastic.co/>
- Selecciona tu deployment, selecciona Edit y abre User setting overrides
- En tu proyecto, abre y copia el contenido del archivo cors_update_elasticsearch.yml como se muestra en la figura a la derecha
- Selecciona Save al final de la página
- Espera unos minutos a que vuelva a arrancar tu deployment
- *Esta acción es necesaria para que Elasticsearch acepte pedidos desde tu navegador Chrome*

>User setting overrides

Change how Elasticsearch runs with your own user settings. User settings are appended to the `elasticsearch.yml` configuration file for your Elasticsearch cluster, but not all settings are supported. [Learn more ...](#)

```
1- # Note that the syntax for user settings can change between major versions.
2- # You might need to update these user settings before performing a major version upgr
3-
4- # Slack integration for versions 7.0 and later must use the secure key store method.
5- # For more information, see:
6- # https://www.elastic.co/guide/en/elasticsearch/reference/current/actions-slack.html
7-
8- # Slack integration example (for versions after 5.0 and before 7.0)
9- # xpack.notification.slack:
10- #   account:
11- #     monitoring:
12- #       url: https://hooks.slack.com/services/T0A6BLEEA/B0A6D1PRD/XYZ123
13-
14- # Slack integration example (for versions before 5.0)
15- # watcher.actions.slack.service:
16- #   account:
17- #     monitoring:
18- #       url: https://hooks.slack.com/services/T0A6BLEEA/B0A6D1PRD/XYZ123
19- #       message_defaults:
20- #         from: Watcher
21-
22- ## Webchat and Pagebury integration are also supported. To learn more, see the docum
23- http.cors.enabled: true
24- http.cors.allow-origin: '*'
25- http.cors.allow-methods: "OPTIONS, HEAD, GET, POST, PUT, DELETE"
26- http.cors.allow-credentials: true
27- http.cors.allow-headers: "X-Requested-With, Content-Type, Content-Length, accept, auth
28|
```

Copia el endpoint de Elasticsearch

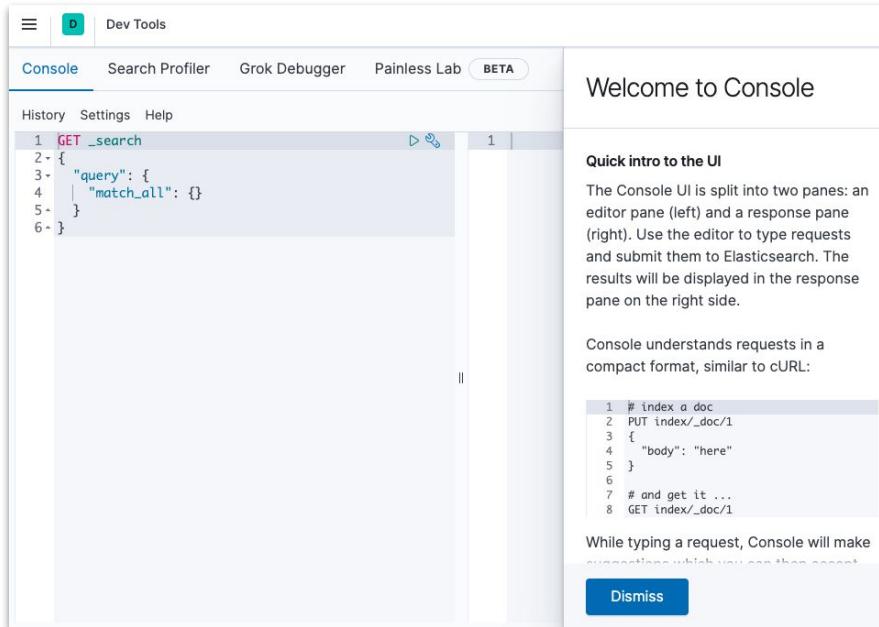
- Vuelve a tu deployment y copia el endpoint de Elasticsearch -- **no lo confundas con el Cloud ID**
- Ya debes tener guardada tu password que fue generada cuando creaste el deployment -- el nombre de usuario va a ser elastic

enrique-primeros-pasos

Deployment name	Deployment status
enrique-primeros-pasos	● Healthy
Edit	
Deployment ID: a525049	
Deployment version	
v7.10.2	
Applications <small>?</small>	Cloud ID <small>?</small>
 Elasticsearch / Copy endpoint	enrique-primeros-pasos:dXMtY2VudHJhbDEuZ2NwLmNs... 50Dg3MTRiZTA4MzQzOD1iZGRlMGQ5MzU4JDk2Mzg4YzF1OGVhMjRi Yzd1NGNhNWNmYTJ1ZmFjMjEy
 Kibana / Launch / Copy endpoint	
 APM / Launch / Copy endpoint	

Lanza Kibana

- Lanza Kibana, selecciona Explore on my own y ve a Management - Developer Tools
- Selecciona Dismiss en la sección Welcome to the console
- Ya estás listo para trabajar en la consola de desarrollo



Ejercicio: Practica operaciones CRUD en Elasticsearch

Ejercicio: CRUD con Elasticsearch

- En tu deployment en el Cloud de Elastic vas a crear, leer, actualizar y borrar datos usando el DSL de Elasticsearch
- Comienza por lanzar Kibana e ir a *Developer Tools*
- Estando ahí crea, lee, actualiza y borra el siguiente documento de JSON como sigue (cada pedido de REST se debe correr por separado):

```
PUT productos/_doc/1
{
  "sku": 101,
  "nombre": "telefono celular",
  "descripción": "Buen telefono para cualquier situación.",
  "precio": 1000.99
}

GET productos/_doc/1

POST productos/_update/1
{
  "doc": {
    "precio": 9999.99
  }
}

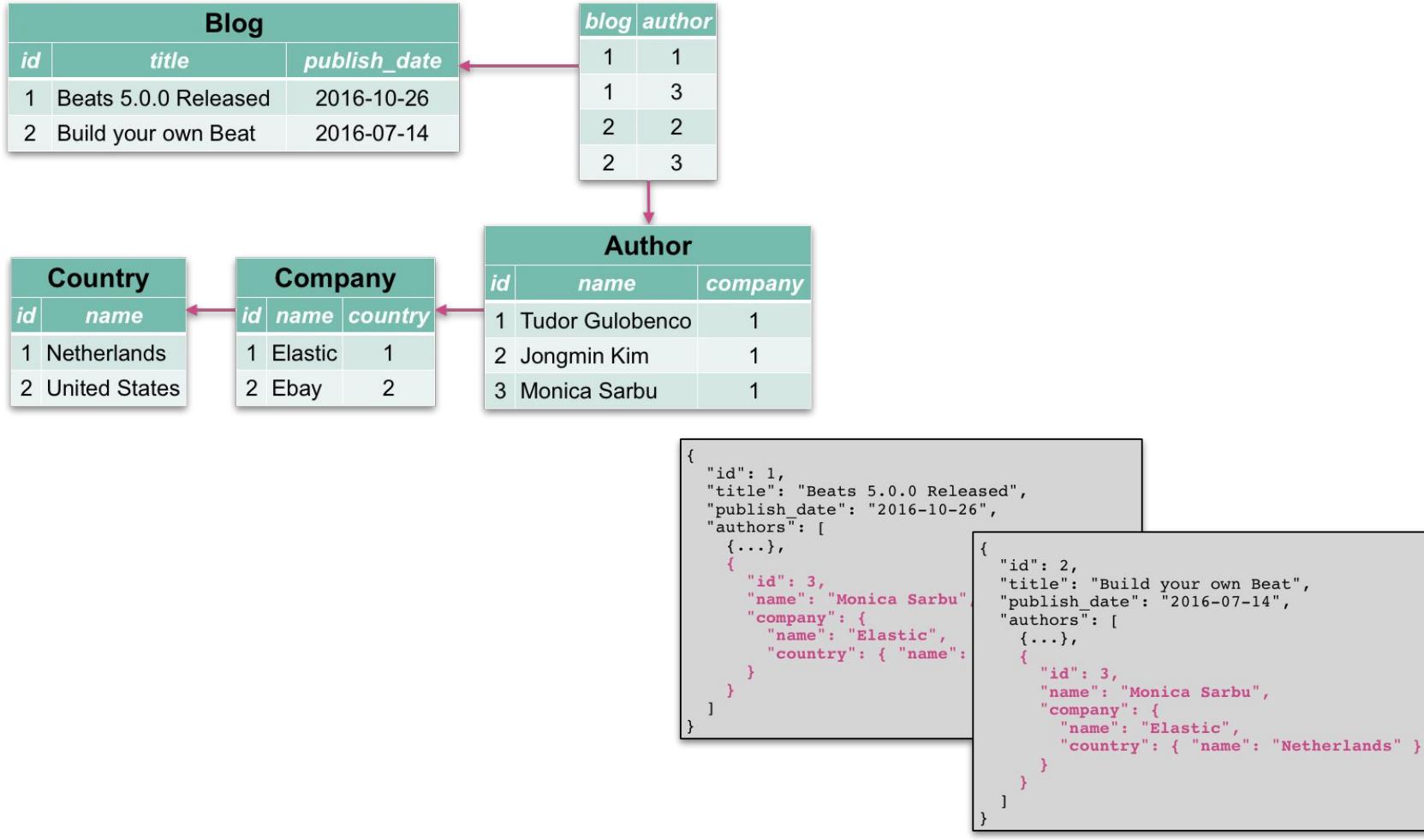
DELETE productos/_doc/1
```

Organización de datos en Elasticsearch

- Todo *documento* de JSON es miembro de un *índice*
- Todo índice tiene un *mapeo* que define el nombre y el tipo de cada una de las *propiedades* (o campos) del documento
- ¿Notaste que no tuviste que definir el índice antes de guardar un documento?
 - Elasticsearch crea el índice dinámicamente si tu no lo has definido de antemano
 - En producción esta no es tan buena idea -- es una puerta abierta a errores y a hackers
 - Por lo pronto vamos a disfrutar el no tener que definir el índice -- vamos a dejar a Elasticsearch crear el índice, añadir sus propiedades (así como otras configuraciones) y adivinar el tipo de datos de cada propiedad

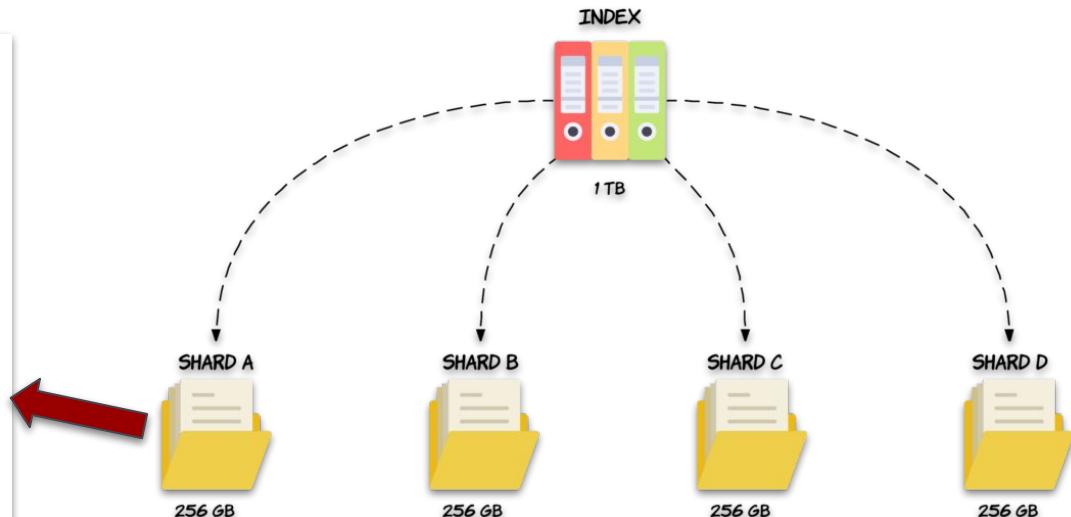
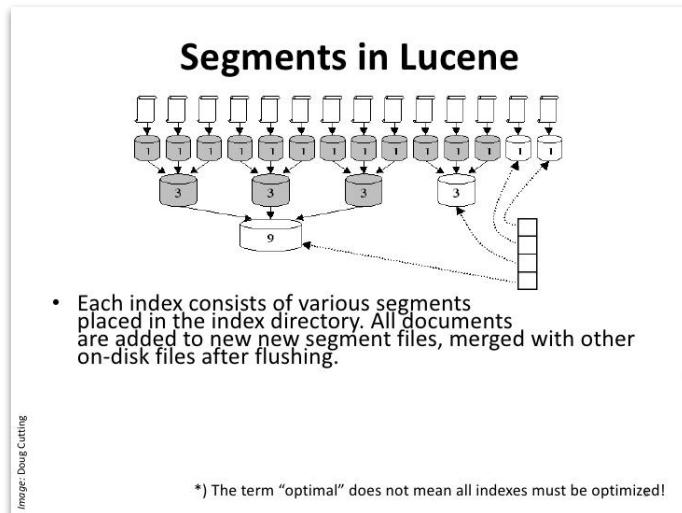
En que se parece Elasticsearch a una base de datos

- Un índice es parecido a una tabla en una base de datos relacional
- Sin embargo,
 - Un registro o renglón de una tabla es representado como un documento de JSON en el índice
 - En Elasticsearch no hay operación de join, por lo cual un índice está altamente desnormalizado
 - Normalmente no hay correspondencia 1:1 entre índices y tablas sino que un índice contiene información de muchas tablas
 - El diseño de una base de datos es general, mientras un índice sirve a un caso de uso específico
 - Elasticsearch no reemplaza a una base de datos, sino que más bien la complementa
 - Elasticsearch puede crear un índice dinámicamente tomando como base un documento, mientras que una tabla debe ser definida de antemano y es difícil hacerle cambios
 - En cierta manera un índice de Elasticsearch se parece más a una hoja de cálculo



Por debajo de la cubierta de Elasticsearch

- Debajo de la cubierta está Lucene
 - Un índice de Elasticsearch almacena sus datos en uno o más instantes de Lucene
 - Lucene hace todo el trabajo de almacenamiento de datos y consulta, pero Elasticsearch lo administra y convierte en un sistema distribuido fácil de usar y escalar (más sobre este tema en el tercer episodio de esta serie)



- La imagen proviene de <https://codingexplained.com/coding/elasticsearch/understanding-sharding-in-elasticsearch>

Ejercicio: CRUD con Elastic (continua)

- Añade otros cuatro productos

```
PUT productos/_doc/2
{
  "sku": 102,
  "nombre": "armario",
  "descripción": "Un armario útil para todo lo que quiera guardar por eternidad. Guarde una raqueta o un traje, sus tenis de uso diario, guarde otra
raqueta, no hay límite a los usos de este armario.",
  "precio": 800.95
}

PUT productos/_doc/3
{
  "sku": 403,
  "nombre": "raqueta de tenis",
  "descripción": "Raqueta de tenis aprobada por los mejores torneos. Fácil de guardar en cualquier armario. El gran tenista Raúl Ramírez en una ocasión usó
una de estas raquetas de tenis (o una muy parecida) cuando jugó con uno de sus sobrinos.",
  "precio": 450.95
}

PUT productos/_doc/4
{
  "sku": 111,
  "nombre": "tenis de uso diario",
  "descripción": "Camine con confianza en pavimento, lodo, alfombras, madera, y mas con estos tenis de alta tecnología y de alta calidad."
}

PUT productos/_doc/5
{
  "sku": 334,
  "nombre": "pintura de color de rosa",
  "descripción": "A diario es posible el uso de esta pintura. Su uso es muy conveniente aun cuando su uso sea diario."
}
```

Ejercicio (continua)

- La búsqueda más sencilla es un GET sin cuerpo. El resultado es una muestra de los documentos en el índice

```
GET productos/_search
```

- Una consulta usando términos de búsqueda se puede formular como sigue:

```
GET productos/_search
{
  "query": {
    "match": {
      "descripción": "tenis de uso diario"
    }
  }
}
```

- Quizás te sorprenderá que la consulta es en realidad equivalente a:
(tenis OR de OR de OR uso OR diario)

Ejercicio (continua)

- Los primeros resultados no parecen muy relevantes
- El resultado exacto apareció hasta el final
- Por alguna razon productos aparentemente irrelevantes recibieron un score más alto

```
max_score: 2.9926257
hits:
- _index: "productos"
  _type: "_doc"
  _id: "5"
  _score: 2.9926257
  _source:
    nombre: "pintura de color de rosa"
- _index: "productos"
  _type: "_doc"
  _id: "2"
  _score: 2.3013537
  _source:
    nombre: "armario"
- _index: "productos"
  _type: "_doc"
  _id: "3"
  _score: 1.0865449
  _source:
    nombre: "raqueta de tenis"
- _index: "productos"
  _type: "_doc"
  _id: "4"
  _score: 0.9908233
  _source:
    nombre: "tenis de uso diario"
```

Ejercicio (continua)

- Es posible especificar el operador lógico en la consulta -- aun así, ¿qué problemas ves cuando buscas mejores tenis de uso diario? ¿Te satisfacen los resultados?

```
GET productos/_search
{
  "query": {
    "match": {
      "descripción": {
        "query": "tenis de uso diario",
        "operator": "or"
      }
    }
  }
}

GET productos/_search
{
  "query": {
    "match": {
      "descripción": {
        "query": "tenis de uso diario",
        "operator": "and"
      }
    }
  }
}

GET productos/_search
{
  "query": {
    "match": {
      "descripción": {
        "query": "tenis de uso diario",
        "operator": "or",
        "minimum_should_match": 2
      }
    }
  }
}
```

Ejercicio (continua)

- Una mejora es aceptar un alto número de resultados, pero mover algunos hacia arriba a través de una combinación de consultas:

```
GET productos/_search
{
  "query": {
    "bool": {
      "must": [
        {
          "match": {
            "descripción": "tenis de uso diario"
          }
        }
      ],
      "should": [
        {
          "match": {
            "nombre": "tenis de uso diario"
          }
        }
      ]
    }
  }
}
```

Operadores booleanos del DSL

- must `es como` AND
- filter `es como` AND
- must-not `es como` NOT
- should
 - `es como` OR cuando se usa solo
 - o le da más prioridad a sus resultados cuando se usa con `must`

Exercicio (continua)

- Otra mejora es dar más prioridad a los productos en los cuales aparecen los términos de búsqueda como una frase

```
GET productos/_search
{
    "query": {
        "bool": {
            "must": [
                {
                    "match": {
                        "descripción": "tenis de uso diario"
                    }
                }
            ],
            "should": [
                {
                    "match": {
                        "nombre": "tenis de uso diario"
                    }
                },
                {
                    "match_phrase": {
                        "descripción": "tenis de uso diario"
                    }
                }
            ]
        }
    }
}
```

Como funciona Elasticsearch: Velocidad

- Elasticsearch guarda todas las palabras de un texto en un *índice invertido*
 - El mismo principio que el índice al final de un libro
 - Cada término está asociado con una lista de identificadores de documento que contienen el término
 - Información adicional como la posición y la frecuencia del término se guarda también en esta estructura de datos
 - Elasticsearch no "lee" el texto al momento de la consulta, sino que tan solo busca los términos de consulta en el índice invertido y lee la lista de documentos que lo contienen

El índice invertido

```
PUT my_index/_doc/1
```

```
{  
    "pais": "Estados Unidos Mexicanos"  
}
```

```
PUT my_index/_doc/2
```

```
{  
    "pais": "Republica de Costa Rica"  
}
```

```
PUT my_index/_doc/3
```

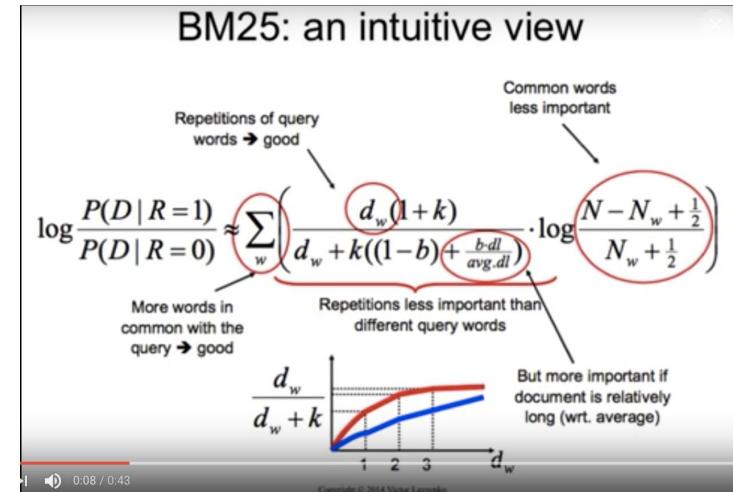
```
{  
    "pais": "Estados Unidos de America"  
}
```



term	doc id
estados	1,3
unidos	1,3
mexicanos	1
republica	2
de	2,3
costa	2
rica	2
america	3

Como funciona Elasticsearch: Relevancia

- La relevancia es un score
 - Score calculado en base a la frecuencia de un término en un documento (TF) y el inverso de la frecuencia del término en todos los documentos (IDF)
 - Si un término aparece muchas veces en un documento puede querer decir que el documento es muy relevante con respecto a término
 - Pero si el término es muy popular en muchos otros documentos, resulta que no es un término tan interesante
 - Elasticsearch calcula el score de un documento usando el método BM25
 - **La experiencia es la búsqueda = manipulación del score durante la consulta**
- Añade "explain": true a tu query para ver exactamente como se calculó el score de cada documento



Ejercicio: Crea una página de búsqueda on Elasticsearch

Paso 1. Carga los datos

- En Kibana, ve a Machine Learning - Data Visualizer - Import Data
 - Selecciona Upload file, busca el archivo blogs_tmp.json y abrelo

The screenshot shows the Kibana interface with the 'Data Visualizer' tab selected. A prominent heading says 'Visualize data from a log file EXPERIMENTAL'. Below it, a text block explains the purpose of the Data Visualizer and lists supported file formats: Delimited text files (CSV, TSV), Newline-delimited JSON, and Log files with a common timestamp. It also mentions a 100 MB upload limit and a GitHub link for feedback. At the bottom, there's a 'Select or drag and drop a file' input field with a download icon.

The screenshot shows the Kibana interface with the 'Data Visualizer' tab selected. The top section displays the file contents of 'blogs_tmp.csv'. Below this, the 'Summary' section provides an overview of the analyzed data: 101 lines, delimited format, semicolon delimiter, and true header row. The 'File stats' section contains three charts: 'title' (100 documents, 100 distinct values), 'seo_title' (19 documents, 19 distinct values), and 'url' (100 documents, 100 distinct values). The 'Import' button is at the bottom.

File contents
First 101 lines

seriously. At this time, we are not aware of any exploit on our cloud service that utilized the Meltdown or Spectre vulnerabilities. Impact Assessment: The Meltdown or Spectre vulnerabilities apply when untrusted code can execute on a system. At the host infrastructure level, we know that both our infrastructure providers (AWS and GCP) have patched their systems, and are no longer vulnerable. At the Elastic Cloud Service level, Elastic Cloud allows you to upload some artifacts, such as plug-ins, dictionaries, and scripts. These uploads provide a potential vector of attack that could exploit the old Elasticsearch clusters on version 1.x and earlier. We believe your cluster is not affected by this issue. Elastic Cloud does not allow for untrusted code execution. Based on our assessment, we believe the impact of Meltdown and Spectre to Elasticsearch to be small. We have focused our efforts on mitigation and control while we carry out our regular process for operating system patches in an accelerated fashion. Mitigation: We disabled non-standard ports on all Elasticsearch 1.x clusters as a best-practice visible measure. We have also disabled self-service access of Elasticsearch buckets from you as we have fully controlled patching behind the scenes. We've further increased our observability of system-level calls and isolated clusters running version 1.x of Elasticsearch on their own hosts. Patching and Configuration: We are using an accelerated version of our regular maintenance procedure to perform OS-level updates while maintaining service availability for user clusters. Your clusters will not experience downtime from this operating system patching. There is considerable speculation on the internet about the performance impact of the

Summary

Number of lines analyzed: 101
Format: delimited
Delimiter: ;
Has header row: true

[Override settings](#) [Analysis explanation](#)

File stats

Field	Value	Count	Distinct Values
title	top values	Alibaba Cloud to (1%)	100
title	top values	Announcing the (1%)	100
title	top values	Applications for (1%)	100
title	top values	Apply for an (1%)	100
title	top values	Beats 6.0.0 GA rel (1%)	100
title	top values	Beats 6.0.0 rc1 (1%)	100
seo_title	top values	Creating new Kib (1%)	19
seo_title	top values	Default Password (1%)	19
seo_title	top values	Deploying Elastic (1%)	19
seo_title	top values	Elasticsearch 5.6. (1%)	19
seo_title	top values	Elasticsearch 5.6. (1%)	19
seo_title	top values	Elasticsearch 6.0. (1%)	19
url	top values	/blog/alibaba-clo (1%)	100
url	top values	/blog/announcing (1%)	100
url	top values	/blog/applications (1%)	100
url	top values	/blog/apply-for-a (1%)	100
url	top values	/blog/beats-6-0-0- (1%)	100
url	top values	/blog/beats-6-0-1- (1%)	100

[Import](#) [Cancel](#)

Paso 2. Carga los datos (continua)

- Selecciona Import
 - Quita la selección a Create index pattern
 - Usa blogs como Index name
 - Selecciona Import de nuevo para hacer la carga

Machine Learning / Data Visualizer / File

Overview Anomaly Detection Data Frame Analytics **Data Visualizer** Settings

blogs_tmp.csv

Import data EXPERIMENTAL

Simple Advanced

Index name

blogs

Create index pattern

Import

Machine Learning / Data Visualizer / File

Overview Anomaly Detection Data Frame Analytics **Data Visualizer** Settings

blogs_tmp.csv

Import data EXPERIMENTAL

Simple Advanced

Index name

blogs

Create index pattern

Reset

File processed ✓

Index created ✓

Ingest pipeline created ✓

Data uploaded ✓

✓ Import complete

Index	blogs
Ingest pipeline	blogs-pipeline
Documents ingested	100

Paso 3. Crea la plantilla de búsqueda

- En Kibana - Developer Tools, crea la plantilla busqueda_blogs

```
PUT _scripts/busqueda_blogs
{
  "script": {
    "lang": "mustache",
    "source": {
      "query": {
        "match": {
          "content": "{{terminos}}"
        }
      }
    }
  }
}
```

- Haz una prueba buscando blogs que mencionan el término Logstash

```
GET blogs/_search/template
{
  "id": "busqueda_blogs",
  "params": {
    "terminos": "Logstash"
  }
}
```

Paso 4. Actualiza la información de tu deployment

- En tu deployment en la nube de Elastic, copia to endpoint de Elasticsearch y busca tu userid y password (que guardaste cuando creaste el deployment)

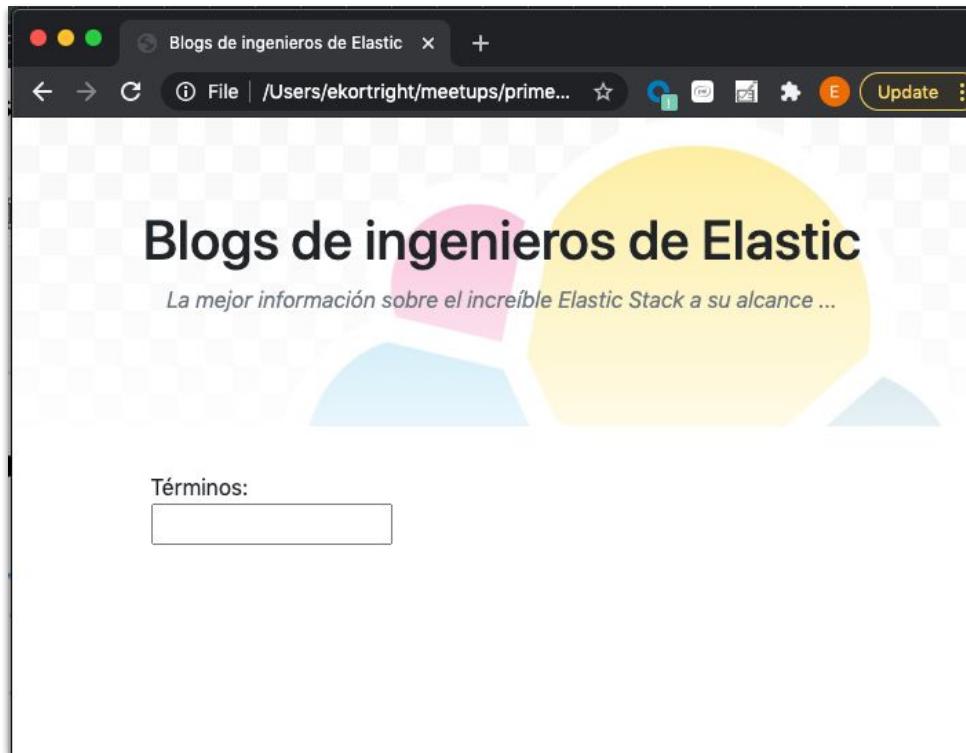
The screenshot shows the Elastic Cloud interface for a deployment named "enrique-primeros-pasos". The deployment status is "Healthy". The deployment ID is a525049. The deployment version is v7.10.2. Under "Applications", there are links for Elasticsearch, Kibana, and APM, each with "Copy endpoint" options. The "Cloud ID" field contains a long string of characters: "enrique-primeros-pasos:dXMtY2VudHJhbDEuZ2NwLmNs3VkLmVzLmlvJGEwMWRizjc50dg3MTRiZTA4MzQzODIzZGR1MGQ5MzU4JDK2Mzg4YzF1OGVhMjRiYzd1NGNhNWNmYTJ1ZmFjMjEy".

- En `busqueda.html` en tu proyecto, actualiza las siguientes líneas con tu información:

```
xhttp.open("POST", "https://f530782362b345da858bb9f228462d2b.us-central1.gcp.cloud.es.io:9243/blogs/_search/template",  
true);  
xhttp.setRequestHeader("Authorization", "Basic " + btoa("elastic:CINP4784iDbMQfcJpk7aCmPI"));
```

Paso 5. Lanza la página de búsqueda

- Abre `busqueda.html` usando Chrome
 - No va a funcionar con Firefox porque es un archivo local



Paso 6. Prueba inicial

- Inserta uno o más términos de búsqueda a manera de primera prueba:
 - En este ejemplo hemos usado elastic stack
- ¿Qué te parecen los resultados?

The screenshot shows a blog search interface with a search bar containing 'elastic stack' and a result count of 'Número de resultados: 67'. Three blog posts are listed:

- SHA-512 checksums for Elastic Stack artifacts** by Maxime Greau. It discusses the generation of SHA-512 checksum files for Elastic Stack artifacts and includes a 'Leer' button.
- PSD2: Monitoring Modern Banking API Architectures with the Elastic Stack, Part II** by Loek van Gool. It highlights the use of APIs in banking and includes a 'Leer' button.
- Elastic Advent Calendar 2017, Week 2** by Michelle Carroll. It describes the second week of the 2017 Advent Calendar and includes a 'Leer' button.
- Keeping up with Kibana: This week in Kibana for December 18, 2017**. This item is partially visible at the bottom of the list.

Paso 7. Añade highlight

- Añade la sección de highlight a la plantilla
 - Vamos a usar <mark> y </mark> como tags para aprovechar el highlight que hace bootstrap automáticamente

```
PUT _scripts/busqueda_blogs
{
  "script": {
    "lang": "mustache",
    "source": {
      "query": {
        "match": {
          "content": "{{terminos}}"
        }
      },
      "highlight": {
        "fields": {
          "title": {
            "pre_tags" : ["<mark>"], "post_tags" : ["</mark>"],
            "require_field_match": false
          },
          "content": {
            "pre_tags" : ["<mark>"], "post_tags" : ["</mark>"],
            "require_field_match": false
          }
        }
      }
    }
  }
}
```

Blogs de ingenieros de Elastic
La mejor información sobre el increíble Elastic Stack a su alcance ...

Términos:
elastic stack

Número de resultados: 67

SHA-512 checksums for Elastic Stack artifacts
Maxime Greau
Each time we do a release of the **Elastic Stack**, are generated...
SHA-1 and SHA-512 checksums While we encourage you to move to the SHA-512 checksum, Once you have downloaded one **Elastic Stack** artifact, e.g., **Elastic Stack** 6.0.0 checksums: new SHA-512 format, no more SHA-1 With the upcoming **Elastic Stack** 6.0.0, If you already have a script doing that with the **Elastic Stack** artifacts, please for all **Elastic** releases ... Score: 2.9073086
[Leer](#)

PSD2: Monitoring Modern Banking API Architectures with the Elastic Stack, Part II
Loek van Gool
The **Elastic Stack** plays a vital role in many of the world's banks today, and that will especially be, **Stack** for Logging and Metrics. At the highest level, **Elastic** is functioning as the data platform for... The **Elastic Stack** offers a complete suite of products for API observability architectures: The **Elastic**, Kibana sits on top of the **stack** to discover data and manage **Elastic** components., Some good reads on the upcoming APM module of the **Elastic Stack**: ... Score: 2.7172174
[Leer](#)



Paso 8. Mejora los resultados usando should

- Podemos mejorar los resultados dando prioridad a los que mencionan los términos de búsqueda en el título de un blog:

```
PUT _scripts/busqueda_blogs
{
  "script": {
    "lang": "mustache",
    "source": {
      "query": {
        "bool": {
          "must": [
            {
              "match": {
                "content": "{{terminos}}"
              }
            }
          ],
          "should": [
            {
              "match": {
                "title": {
                  "query": "{{terminos}}"
                }
              }
            }
          ]
        }
      },
      "highlight": {
        "fields": {
          "title": {
            "pre_tags" : ["<mark>"], "post_tags" : ["</mark>"],
            "require_field_match": false
          },
          "content": {
            "pre_tags" : ["<mark>"], "post_tags" : ["</mark>"],
            "require_field_match": false
          }
        }
      }
    }
  }
}
```

Blogs de ingenieros de Elastic

La mejor información sobre el increíble Elastic Stack a su alcance ...

Términos:

elastic stack

Número de resultados: 67

SHA-512 checksums for Elastic Stack artifacts

Maxime Greau

Each time we do a release of the Elastic Stack, are generated., Elast ... Score:
6.508154

Leer

Elastic Stack 6.0.0-rc2 released

Tyler Hannan

During the 5.0 release, we introduced the Elastic Pioneer Program and are continuing th ... Score: 6.1353273

Leer

Elastic Stack 6.0.0 GA is Released

Tyler Hannan

This milestone would have been impossible to achieve without the effort of a variety of teams within ... Score: 5.5910406

Leer

Getting Started with the Elastic Stack on Microsoft Azure

Christoph Wurm

As cloud adoption grows, we're keeping pace at Elastic, developing integrations and mak ... Score: 5.5516987

Paso 9. Mejora los resultados usando frases y boost

- Podemos aumentar el score cuando un campo tiene los términos como frase
- Podemos aumentar la importancia de un campo usando boost
- Como ves, la alta relevancia se obtiene a través de una jerarquía de scores

```
PUT _scripts/busqueda_blogs
{
  "script": {
    "lang": "mustache",
    "source": {
      "query": {
        "bool": {
          "must": [
            {
              "match": {
                "content": "{{terminos}}"
              }
            }
          ],
          "should": [
            {
              "match_phrase": {
                "title": {
                  "query": "{{terminos}}",
                  "boost": 3
                }
              }
            },
            {
              "match_phrase": {
                "content": {
                  "query": "{{terminos}}",
                  "boost": 2
                }
              }
            },
            {
              "match": {
                "title": "{{terminos}}"
              }
            }
          ]
        },
        "highlight": {
          "fields": {
            "title": {
              "pre_tags": ["<mark>"], "post_tags": ["</mark>"],
              "require_field_match": false
            },
            "content": {
              "pre_tags": ["<mark>"], "post_tags": ["</mark>"],
              "require_field_match": false
            }
          }
        }
      }
    }
  }
}
```

Numero de resultados: 67

SHA-512 checksums for Elastic Stack artifacts

Maxime Greau

Each time we do a release of the Elastic Stack, are generated. Elastic Stack 5.6.2+: SHA-1 and SHA ... Score: 23.110947

Leer

Elastic Stack 6.0.0-rc2 released

Tyler Hannan

During the 5.0 release, we introduced the Elastic Pioneer Program and are continuing the with the 6.0. We'd encourage you to test with the ... Score: 22.21534

Leer

Elastic Stack 6.0.0 GA is Released

Tyler Hannan

This milestone would have been impossible to achieve without the effort of a variety of teams within Elastic. Not only are we releasing th ... Score: 20.141594

Leer

Getting Started with the Elastic Stack on Microsoft Azure

Christoph Wurm

As cloud adoption grows, we're keeping pace at Elastic, developing integrations and making it easier. Microsoft itself is an Elastic ... Score: 19.595415

Leer

PSD2: Monitoring Modern Banking API Architectures with the Elastic Stack, Part II

Loek van Gool

The Elastic Stack plays a vital role in many of

Conclusiones de este ejercicio

Podemos concluir que:

- Lo único que se necesita para usar Elasticsearch desde cualquier lenguaje de programación es un módulo de REST
- El uso de plantillas de búsqueda crea separación entre el backend de Elasticsearch y el cliente
- La alta relevancia de los resultados de una búsqueda es consecuencia de una cuidadosa estrategia de scores
- Elasticsearch proporciona una gran variedad de funciones de consulta y de manejo de scores -- hemos tan solo cubierto la punta del iceberg en este episodio

Preguntas y (probablemente) respuestas

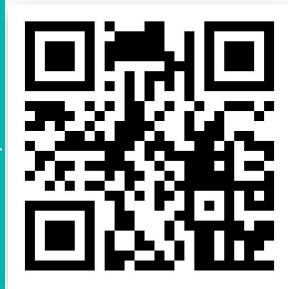


En nuestro siguiente episodio...

- En el segundo episodio nos enfocaremos en la visualización, análisis y predicción de datos con Kibana, así como maneras de reaccionar a situaciones de interés expuestas por estos procesos
- En el tercer episodio vamos a aprender cómo capturar y cargar grandes cantidades y enviarlas a Elasticsearch
 - El módulo de Import de Machine Learning es solo para conjuntos muy pequeños de datos
 - Vamos a explorar Logstash y los varios Beats que completan el Elastic Stack
- ¡No te los pierdas!

Conéctese con la comunidad de Elastic

Existen User Groups en Costa Rica,
Mexico, Colombia, Argentina y Uruguay -
encuentra el tuyo:



User Group Virtual:



- <https://community.elastic.co/>
- <https://community.elastic.co/amer-virtual/>