

Kibana

Kibana

- Plataforma de análisis y visualización
- Interactúa con los índices almacenados en Elasticsearch
- Explotación de datos
- Visualización de datos en Dashboards de visualizaciones

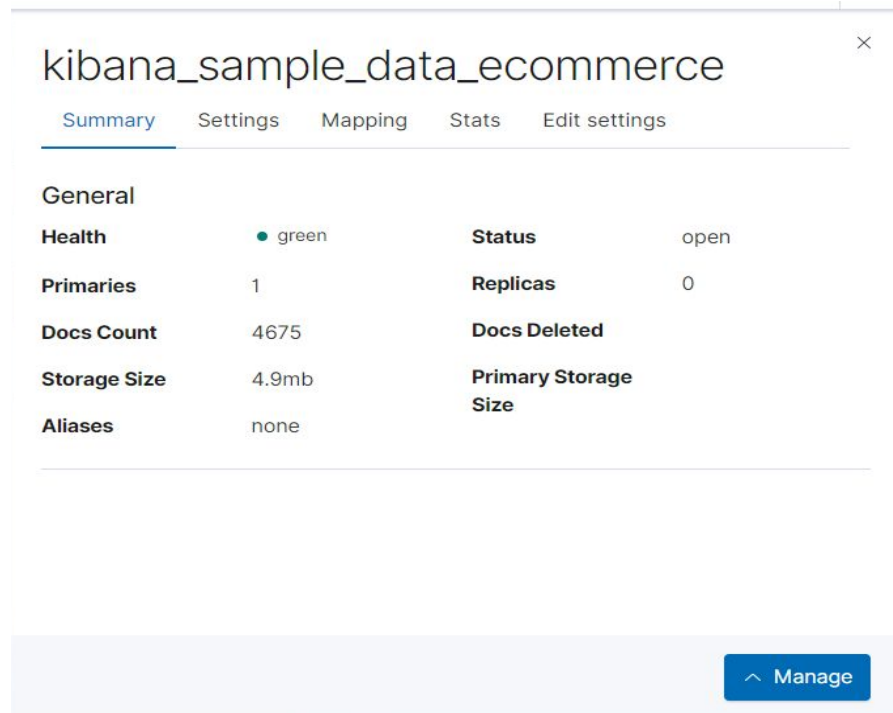


Kibana

- Management
- Explotación
- Visualización
- Monitoreo
- Dashboards
- Canvas
- Maps
- Otras..

Management Kibana: Index Management

- Visualizar estado en tiempo real del índice
- Ver y editar configuración del índice en elasticsearch
- Visualizar los campos mapeados en el index template
- Visualizar estadísticas de las operaciones ejecutadas sobre el índice



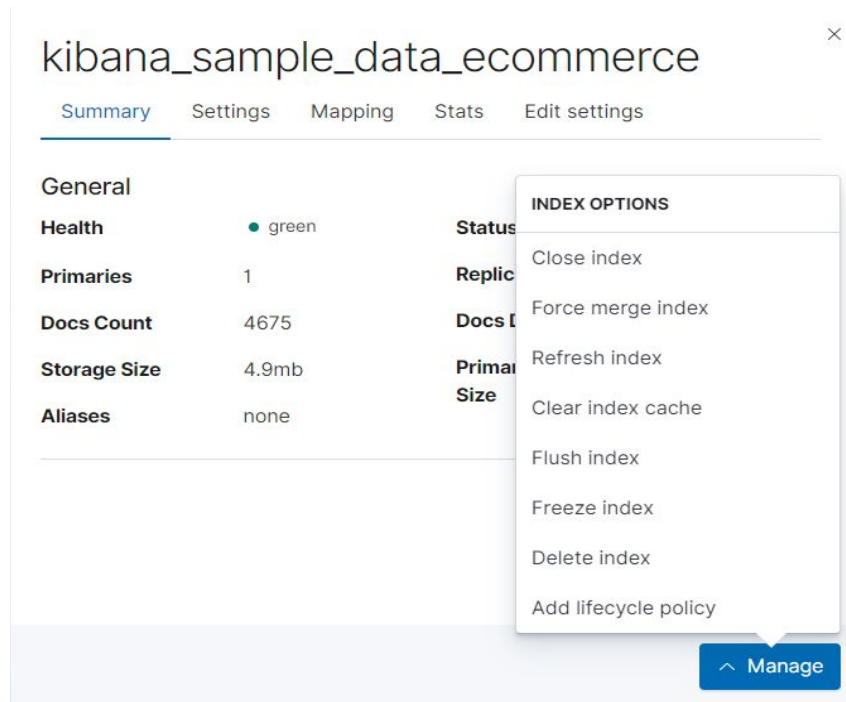
The screenshot shows the Kibana Index Management interface for the index 'kibana_sample_data_ecommerce'. The interface has a top navigation bar with tabs: Summary (selected), Settings, Mapping, Stats, and Edit settings. Below the tabs, the 'General' section is displayed, showing the following information:

General	
Health	● green
Status	open
Primaries	1
Replicas	0
Docs Count	4675
Docs Deleted	
Storage Size	4.9mb
Primary Storage Size	
Aliases	none

At the bottom right of the interface, there is a blue button labeled 'Manage' with an upward arrow icon.

Management Kibana: Index Management

- **Close Index:** Cerrar el index evita el consumo de recursos, y no permite operaciones de lectura/escritura.
- **Force Merge Index:** Fusiona los segmentos de los shards de un índice haciéndolo más pequeño y borrando documentos eliminados



The screenshot shows the Kibana Index Management interface for the index 'kibana_sample_data_ecommerce'. The interface has tabs for Summary, Settings, Mapping, Stats, and Edit settings. The Summary tab is active, displaying a table of index statistics:

General	
Health	● green
Primaries	1
Docs Count	4675
Storage Size	4.9mb
Aliases	none

On the right side, there is a 'Manage' button with a dropdown menu. The dropdown menu is open, showing the following options:

- Close index
- Force merge index
- Refresh index
- Clear index cache
- Flush index
- Freeze index
- Delete index
- Add lifecycle policy

Management Kibana: Index Management

- **Refresh Index:** Actualiza el índice con todos los documentos encolados en el buffer
- **Clear Index Cache:** Limpia todas las caches asociadas al índice

kibana_sample_data_ecommerce

Summary Settings Mapping Stats Edit settings

General

Health	● green	Status
Primaries	1	Replic
Docs Count	4675	Docs I
Storage Size	4.9mb	Primar
Aliases	none	Size

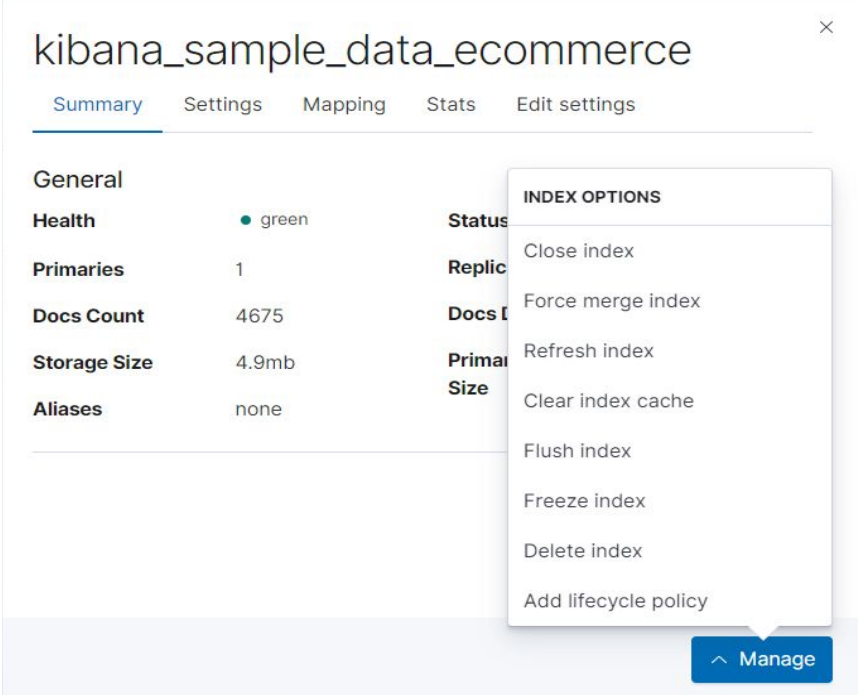
INDEX OPTIONS

- Close index
- Force merge index
- Refresh index
- Clear index cache
- Flush index
- Freeze index
- Delete index
- Add lifecycle policy

Manage

Management Kibana: Index Management

- **Flush Index:** Libera memoria sincronizando el caché del sistema de archivos con el disco y borrando dicha caché
- **Freeze Index:** Convierte el índice a solo lectura y mueve sus fragmentos de memoria a disco.
- **Delete Index:** Borra el índice permanentemente



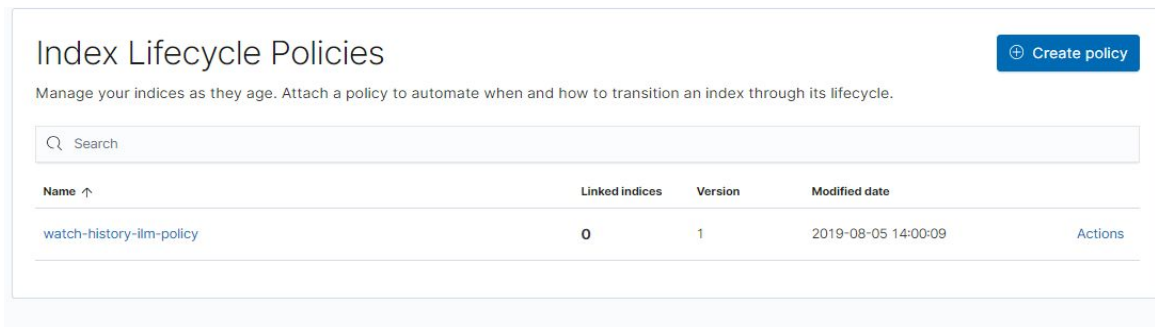
The screenshot shows the Kibana Index Management interface for the index 'kibana_sample_data_ecommerce'. The interface includes tabs for Summary, Settings, Mapping, Stats, and Edit settings. The Summary tab is active, displaying a table of index details:

General	
Health	● green
Primaries	1
Docs Count	4675
Storage Size	4.9mb
Aliases	none

On the right side, there is a 'Manage' button. A dropdown menu titled 'INDEX OPTIONS' is open, showing the following actions:

- Close index
- Force merge index
- Refresh index
- Clear index cache
- Flush index
- Freeze index
- Delete index
- Add lifecycle policy

Management Kibana: Lifecycle Policies



The screenshot shows the 'Index Lifecycle Policies' page in Kibana. At the top, there's a title 'Index Lifecycle Policies' and a 'Create policy' button. Below the title is a description: 'Manage your indices as they age. Attach a policy to automate when and how to transition an index through its lifecycle.' There is a search bar with the placeholder text 'Search'. Below the search bar is a table with the following columns: 'Name ↑', 'Linked indices', 'Version', 'Modified date', and 'Actions'. The table contains one row with the policy name 'watch-history-ilm-policy', 0 linked indices, version 1, and a modified date of '2019-08-05 14:00:09'.

Name ↑	Linked indices	Version	Modified date	Actions
watch-history-ilm-policy	0	1	2019-08-05 14:00:09	

- Define las fases que se habilitan al índice
- Asigna prioridad al índice en el recovery
- Define los tiempos para cada fase durante el ciclo de vida de un índice

Management Kibana: Lifecycle Policies

- **Hot Phase:** Rollover sobre el índice en caso de que el actual cumpla una condición designada (Índices read-write).
- **Warm Phase:** Para índices de solo lectura, asigna hardware de menor rendimiento, como también encoge el índice para mayor rendimiento de la búsqueda.
- **Cold Phase:** Para índices con poca actividad, asigna hardware de menor rendimiento y disminuye el número de réplicas.
- **Delete Phase:** Define cuando es seguro eliminar el índice.

 Read  Write

 Read

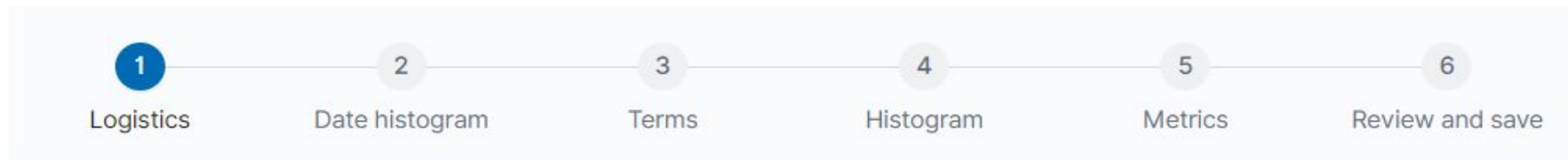
 Read

 Index

Index Management: Rollup Jobs

- Resumen de todos los índices que cumplan el patrón definido
- Compacta información de meses y años
- Facilita la visualización y generación de informes sobre sus datos

Create rollup job



Index Management: Index Patterns

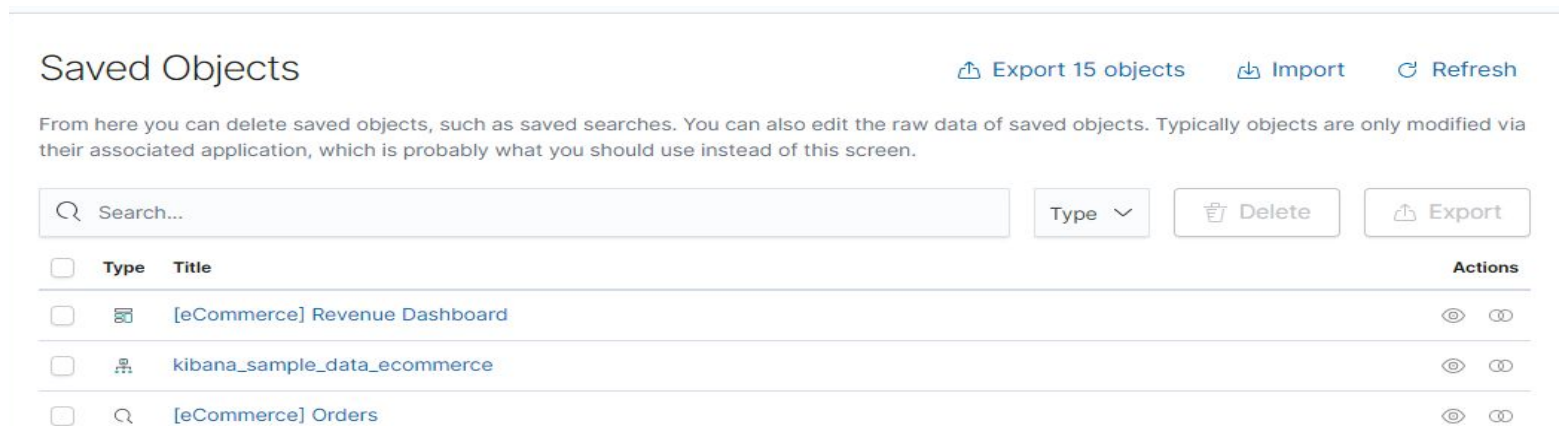
- Catálogo de los patrones de índices
- Estructura de los índices que forma parte del patrón
- Crear, Editar o Eliminar Index Patterns

The screenshot shows the Kibana Index Management page for the index pattern `kibana_sample_data_ecommerce`. The interface includes a sidebar with a 'Create index pattern' dropdown and a list of index patterns. The main content area displays the index name, a time filter field name of `order_date`, and a description of the page's purpose. Below this, there are tabs for 'Fields (59)', 'Scripted fields (0)', and 'Source filters (0)'. A search bar labeled 'Filter' is present, along with a dropdown for 'All field types'. A table lists the fields in the index, showing columns for Name, Type, Format, Searchable, Aggregatable, and Excluded. The table lists two fields: `_id` and `_index`, both of type `string`.

Name	Type	Format	Searchable	Aggregata...	Excluded
<code>_id</code>	string		●	●	
<code>_index</code>	string		●	●	

Index Management: Saved Objects

- Catálogo de todos los objetos guardados de kibana
- Visualizaciones, dashboards, queries, index patterns
- Permite exportar, eliminar o buscar un objeto en particular



The screenshot shows the 'Saved Objects' page in Kibana. At the top, there are buttons for 'Export 15 objects', 'Import', and 'Refresh'. Below this is a descriptive text: 'From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen.' The main area contains a search bar, a 'Type' dropdown, and 'Delete' and 'Export' buttons. A table lists the saved objects with columns for checkboxes, Type, Title, and Actions.

<input type="checkbox"/>	Type	Title	Actions
<input type="checkbox"/>	Dashboard	[eCommerce] Revenue Dashboard	
<input type="checkbox"/>	Index Pattern	kibana_sample_data_ecommerce	
<input type="checkbox"/>	Search	[eCommerce] Orders	

Index Management: Spaces



- Organización de los objetos en distintos spaces
- Permite mantener los objetos organizados y clasificados
- Por defecto todos se crea en el espacio default

Spaces

Organize your dashboards and other saved objects into meaningful categories.

Create a space

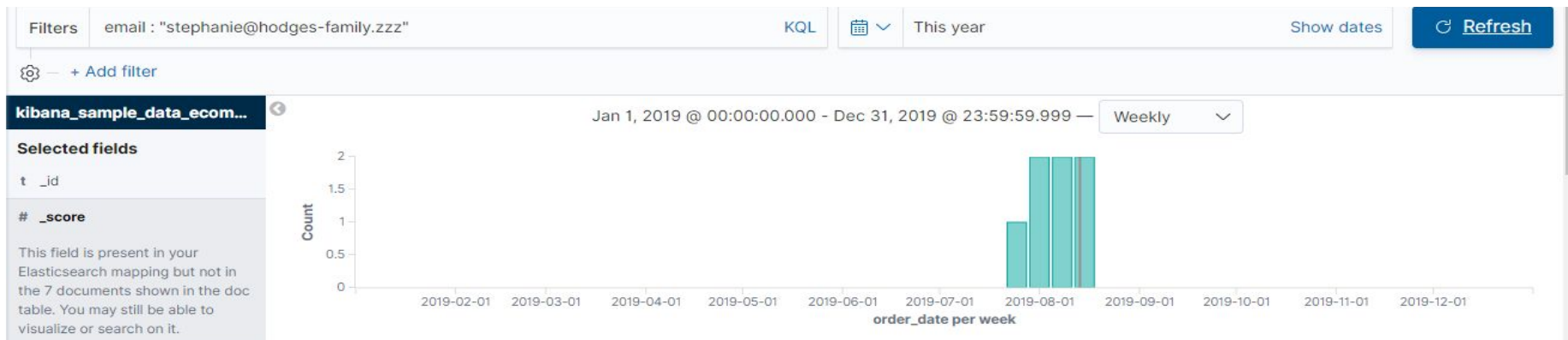
Q Search

Space	Identifier	Description	Actions
 Default	default	This is your default space!	

Rows per page: 10 ▾

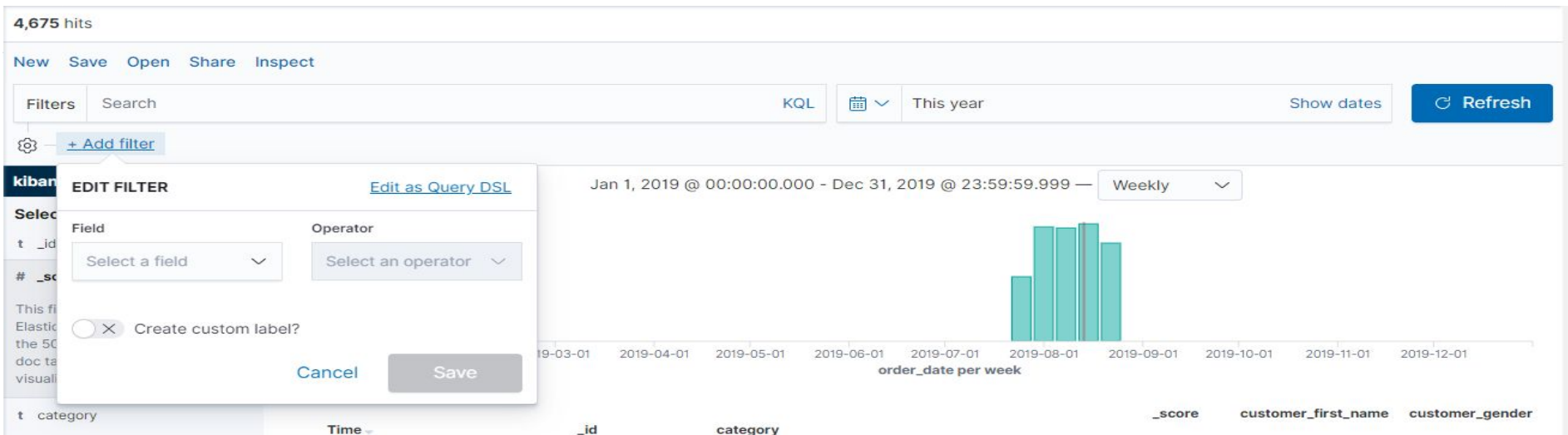
Discover: Time Filter

- Selección de documentos en función del tiempo
- Selección de período de tiempo relativo permite especificar segundos
- Selección de período de tiempo absoluto entre dos fechas
- Seleccionar período de tiempo desde el histograma



Discover: Filters

- Barra de consultas para filtrar los datos
- Permite usar KQL por default o la API de Query DSL en formato JSON
- Actualiza el histograma y los resultados en tiempo real



Discover: Inspect

- Información detallada de la búsqueda ejecutada
- Tiempo de ejecución de la query y request time
- Cantidad de documentos devueltos y cantidad de documentos matcheados

New Saved Search

View: Requests ✕

1 request was made

Request: Segment 0 ✓ 812ms

This request queries Elasticsearch to fetch the data for the search.

Statistics Request Response

② Hits	500
② Hits (total)	4675
② Index pattern	kibana_sample_data_ecommerce
② Index pattern ID	ff959d40-b880-11e8-a6d9-e546fe2bba5f
② Query time	166ms
② Request time	823ms
② Request timestamp	2019-08-13T16:00:20.122Z

Discover: Select Fields

- Detalle de todos los campos que conforman los documentos
- Permite seleccionar los campos a visualizar en los documentos
- Despliega el contenido total de un documento en las columnas seleccionadas

kibana_sample_data_ecommerce

Selected fields

? **_source**

This field is present in your Elasticsearch mapping but not in the 500 documents shown in the doc table. You may still be able to visualize or search on it.

Available fields

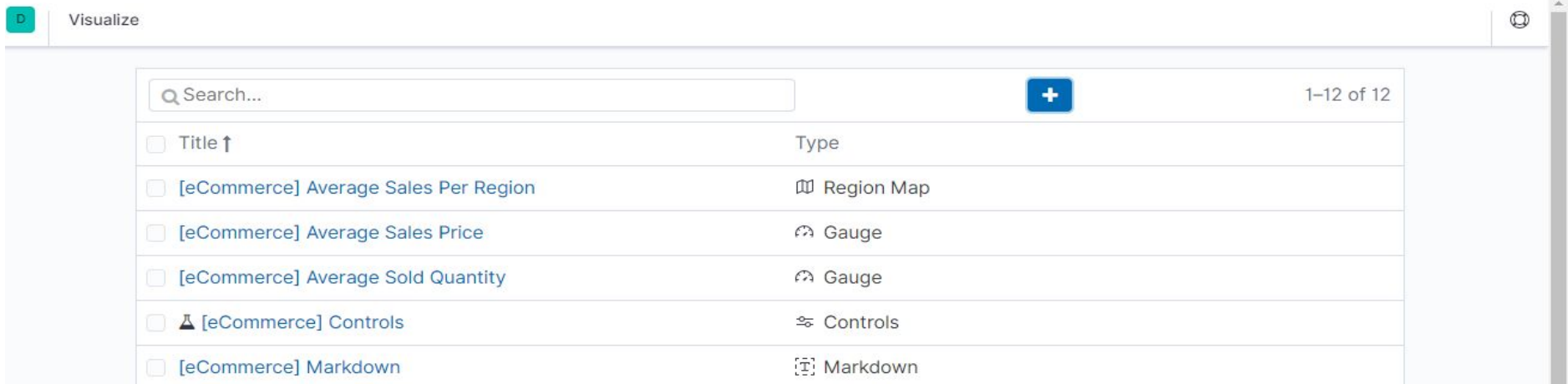
Popular

- t **_id**
- # **_score**
- t **category**
- t **customer_first_name**
- t **customer_gender**
- t **_index**
- t **_type**
- t **currency**
- t **customer_full_name**

Time ▾	customer_first_name	_type	category
> Aug 24, 2019 @ 20:45:36.000	Youssef	_doc	Men's Shoes, Men's Clothing
> Aug 24, 2019 @ 20:31:12.000	Sonya	_doc	Women's Clothing, Women's Accessories
> Aug 24, 2019 @ 20:22:34.000	Brigitte	_doc	Women's Shoes, Women's Clothing
> Aug 24, 2019 @ 20:15:22.000	Abigail	_doc	Women's Clothing
▾ Aug 24, 2019 @ 20:13:55.000	Marwan	_doc	Men's Shoes, Men's Clothing

Visualize

- Listado de las visualizaciones pertenecientes a ese espacio
- Permite editar, eliminar o crear nuevas visualizaciones
- Selección del tipo de visualización a crear

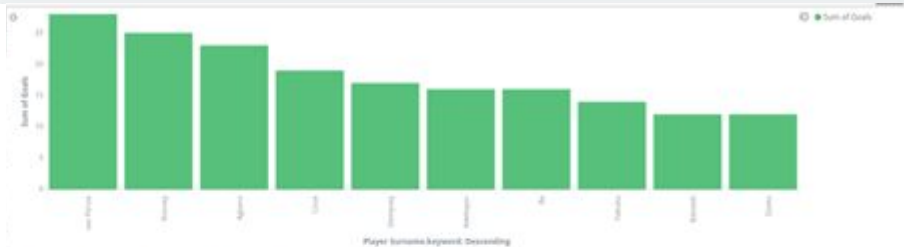
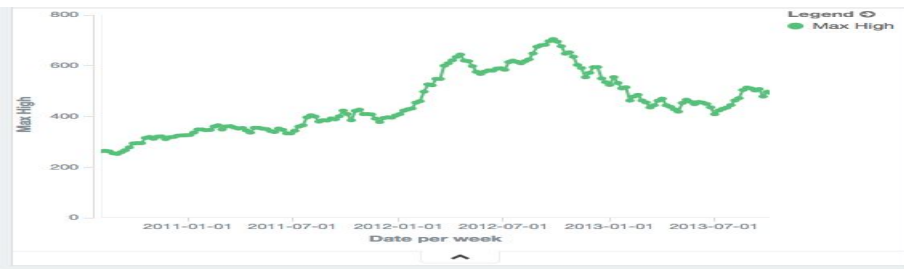
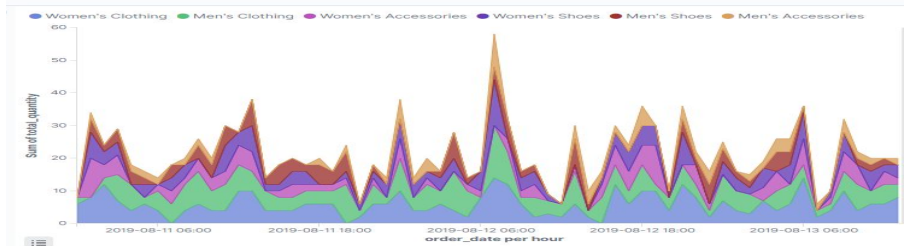


The screenshot displays the 'Visualize' interface. At the top, there is a search bar with the placeholder text 'Search...' and a blue button with a white plus sign. To the right of the search bar, it indicates '1-12 of 12' items. Below the search bar is a table with two columns: 'Title' and 'Type'. The table lists several visualizations, each with a checkbox in the 'Title' column. The visualizations are:

<input type="checkbox"/> Title ↑	Type
<input type="checkbox"/> [eCommerce] Average Sales Per Region	Region Map
<input type="checkbox"/> [eCommerce] Average Sales Price	Gauge
<input type="checkbox"/> [eCommerce] Average Sold Quantity	Gauge
<input type="checkbox"/> [eCommerce] Controls	Controls
<input type="checkbox"/> [eCommerce] Markdown	Markdown

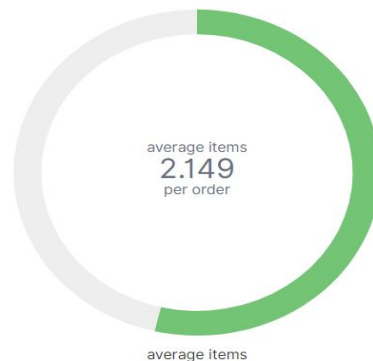
Visualize: Area & Line & Bars

- Área: Agregación numérica representada como un área
- Line: Se usan para representar tendencias en función de tiempo
- Bars: Barras horizontales o verticales para cuantificar las repeticiones de un valor



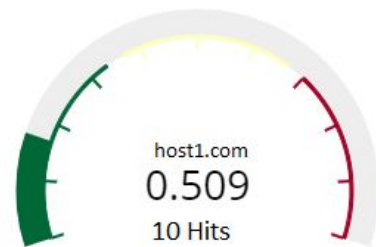
Visualize: Gauge & Goal & Metric

- Gauge: Indica el estado de una métrica en tiempo real en relación al total
- Goal: Indica lo que falta para alcanzar una meta
- Metric: Muestra un número indicando el valor de una métrica



807

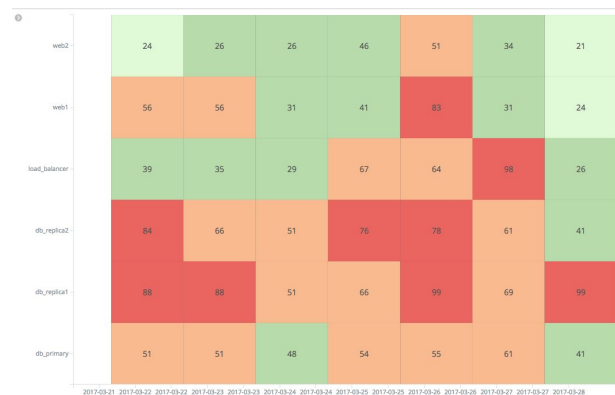
Count



Visualize: Pie & Tag Cloud & Heat Map

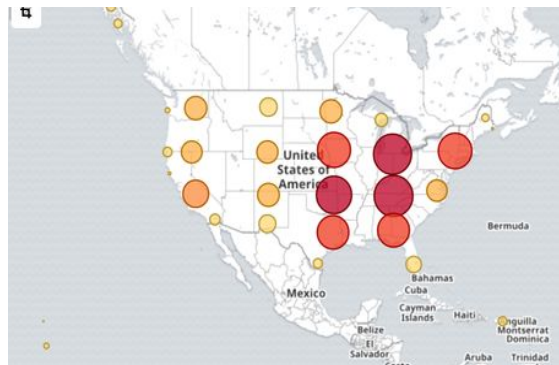
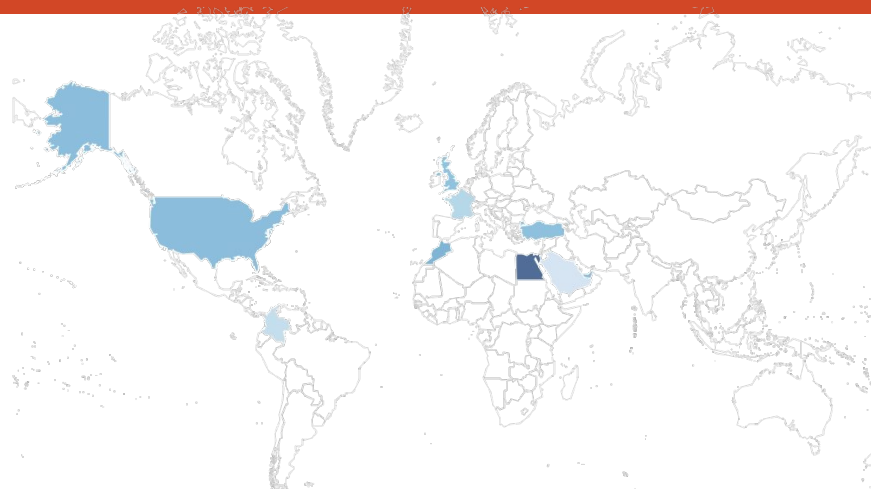
- Pie: Cuantifica una variable sobre un todo
- Tag Cloud: Nube de palabras diferenciando tamaños según repeticiones de términos
- Heat Map: Genera una matriz relacionando dos campos y diferenciados sus repeticiones por la intensidad de color

Men's Clothing
Women's Clothing
Men's Shoes Men's Accessories
Women's Shoes
Women's Accessories



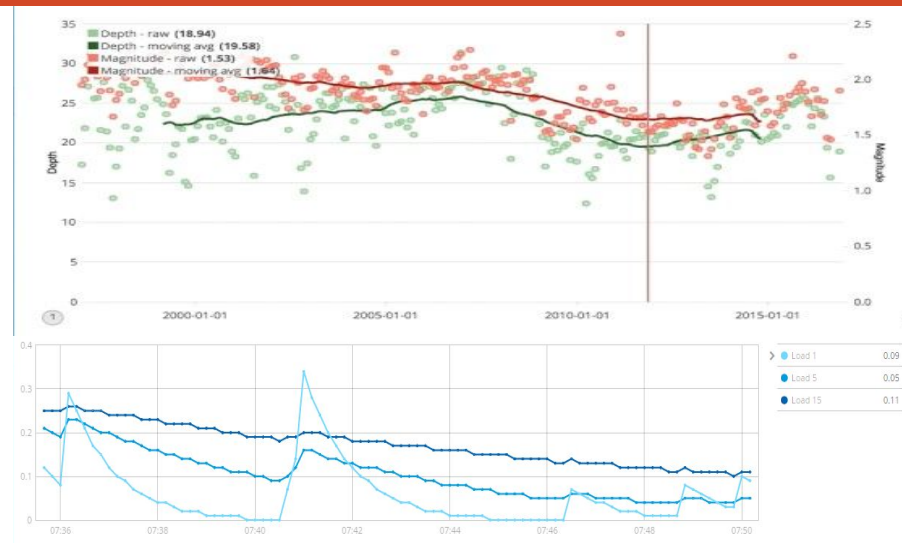
Visualize: Region Map & Coordinate Map

- Region Map: Mapa de intensidad en relación a los países indicada en códigos de 2 o 3 letras por país
- Coordinate Map: Indica los puntos exactos donde indicando sus reiteración por intensidad de color y tamaño, recibe un geohash



Visualize: Timelion & Visual Builder & Markdown

- Timelion: Genera series de tiempo basadas el resultado de una expresión funcional
- Visual Builder: Visualización de histogramas en base a una agregación aplicada sobre determinado campo
- Markdown: Visualización de documento con sintaxis markdown

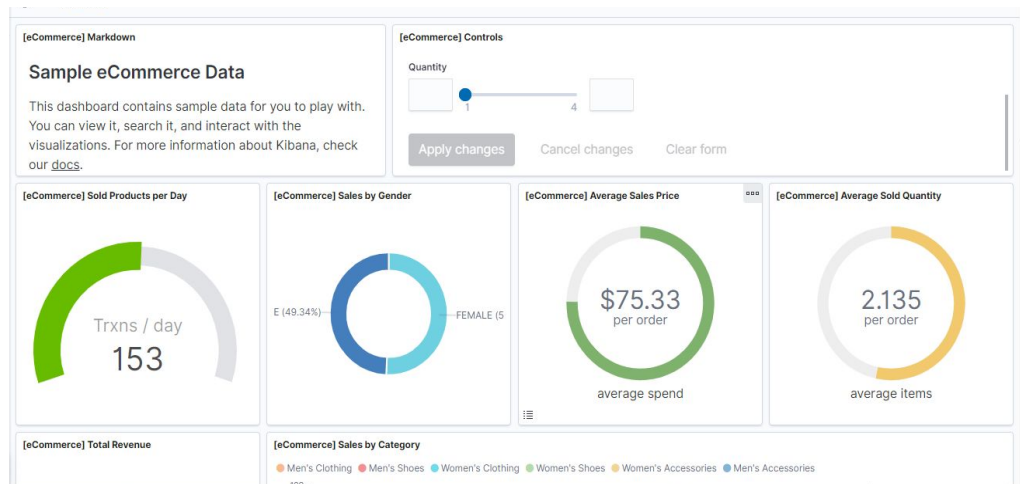


The Total CPU Usage is 5.3%

This calculation is made up of talking `system.cpu.idle.pct` and subtracting it from 1 using a calculation (bucket script) aggregation.

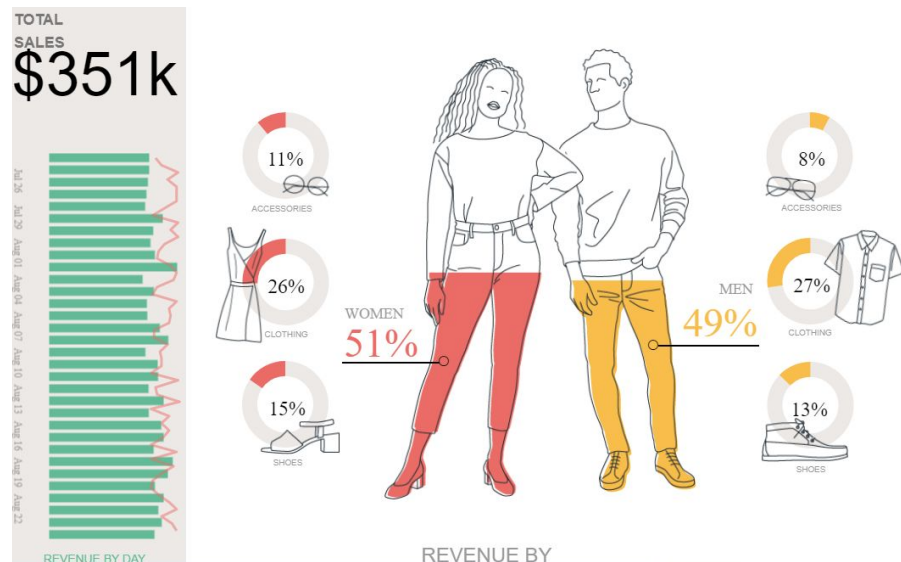
Dashboards

- Visualización de múltiples visualizaciones en una pantalla
- Actualiza datos en relación a los filtros en tiempo real
- Permite editar, crear y eliminar dashboards



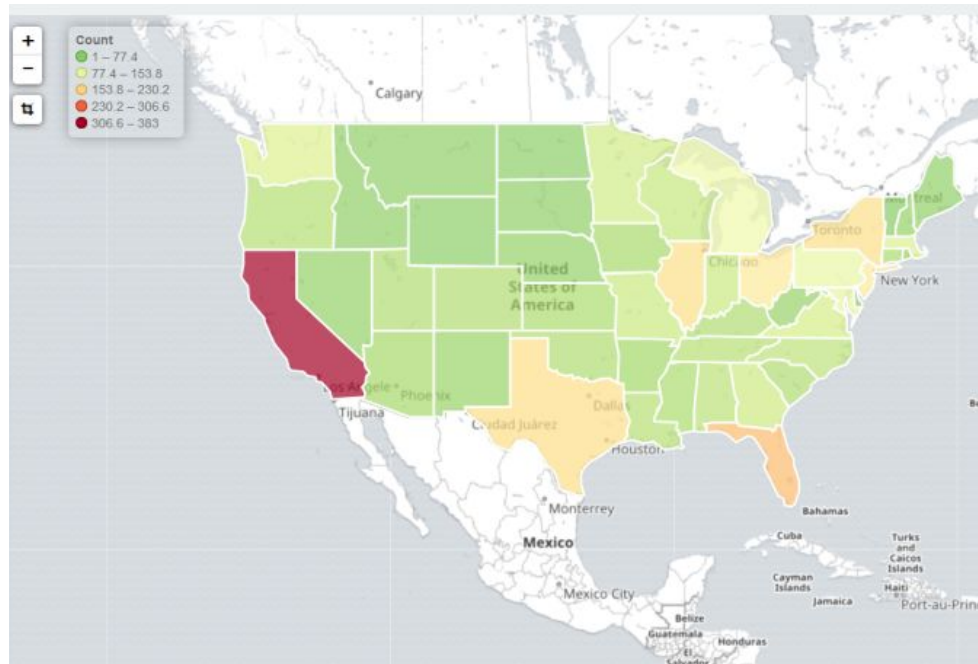
Canvas

- Lienzo con diseño propio para personalizar estéticamente como prefiera el usuario
- Combinación de colores, imágenes y texto
- Permite filtrar los datos del lienzo en tiempo real



Maps

- Visualización de mapa interactiva
- Diferenciación por múltiples formatos (países, formatos, geopoint)
- Referenciación en base a otros campos



Dev Tools



- Console: Consola para ejecución de las APIs de Elasticsearch
- Search Profiler: Ejecuta y brinda el rendimiento de una query en particular
- Grok Debugger: Evalúa si una expresión de grok corresponde con una línea de texto

Monitoring

- Brinda información sobre el estado de los procesos en ejecución
- Se habilita por configuración con la opción de monitoreo de **xpack**
- Provee especificaciones sobre rendimiento de búsquedas y gestión de recursos

