

Práctica Elasticsearch

Introducción

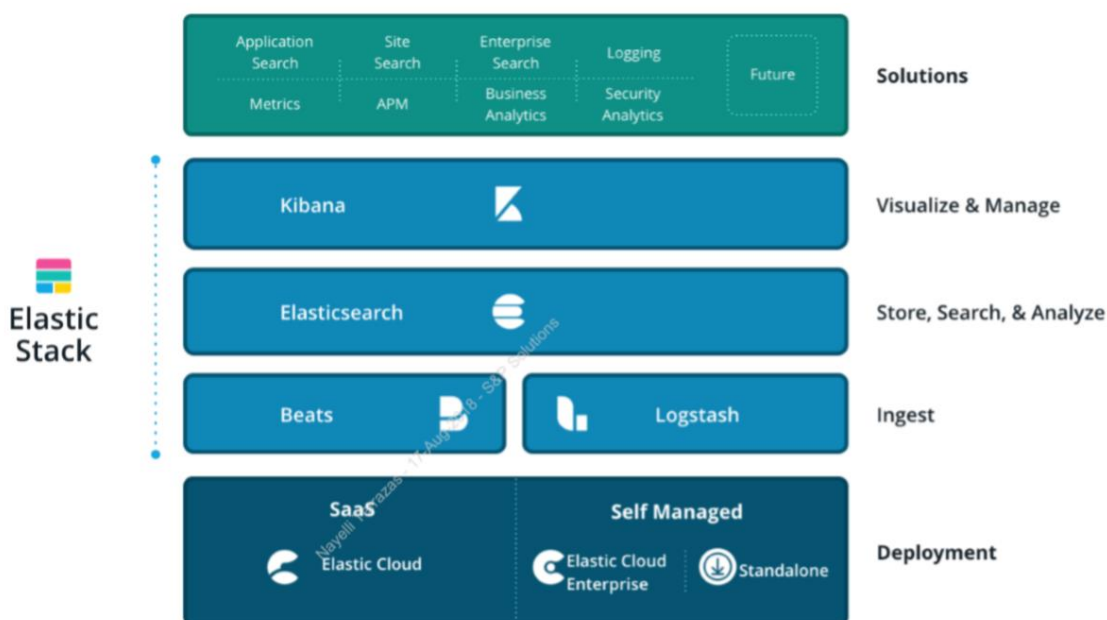
Esta práctica tiene como objetivo identificar las habilidades de autoaprendizaje y resolución de problemas, a través de la exploración de una tecnología relativamente nueva llamada “**Elasticsearch**”.

¿Qué es Elasticsearch?

Motor de búsquedas distribuido y fácil de ser usado por cualquier lenguaje de programación a través de su API REST.

¿Qué es Elastic Stack?

Elasticsearch trabaja en conjunto con programas enfocados en la recolección de información (Logstash-Beats), visualización y análisis de datos (Kibana). Estos productos han sido creados y diseñados para trabajar en conjunto para proveer potentes soluciones de búsqueda.



De la imagen anterior,

1. **Beats** son expedidores de datos de código abierto que instala como agentes en sus servidores para enviar datos operativos a Elasticsearch.

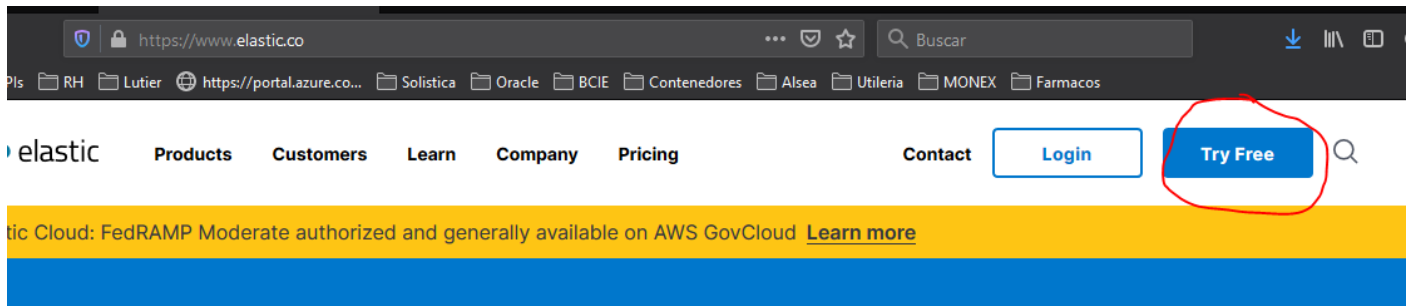
2. **Logstash** es un motor de recopilación de datos de código abierto con capacidades de canalización en tiempo real. Logstash puede unificar dinámicamente los datos de diferentes fuentes y normalizar los datos en los destinos de su elección.
3. **Elasticsearch** es un motor de búsqueda y análisis REST distribuido que almacena de forma centralizada sus datos. Está catalogada como una base de datos NO-SQL de tipo documental.
4. **Kibana** es una plataforma de análisis y visualización de código abierto diseñada para trabajar con Elasticsearch.

Práctica

¡Manos a la obra!

Aprovisionamiento de ELK

Para iniciar con esta práctica necesitaras crear una cuenta de prueba en la siguiente liga <https://www.elastic.co/>



Selecciona elasticsearch

Ready? Let's do this thing.

If you're brand new to Elastic, jump to our [quick-start guide](#).

We can [host Elasticsearch and Kibana for you](#), too.



Elasticsearch

Distributed, RESTful search and analytics.

[Launch on Elastic Cloud](#)[Download](#)

Kibana

Visualize your data. Navigate the Stack.

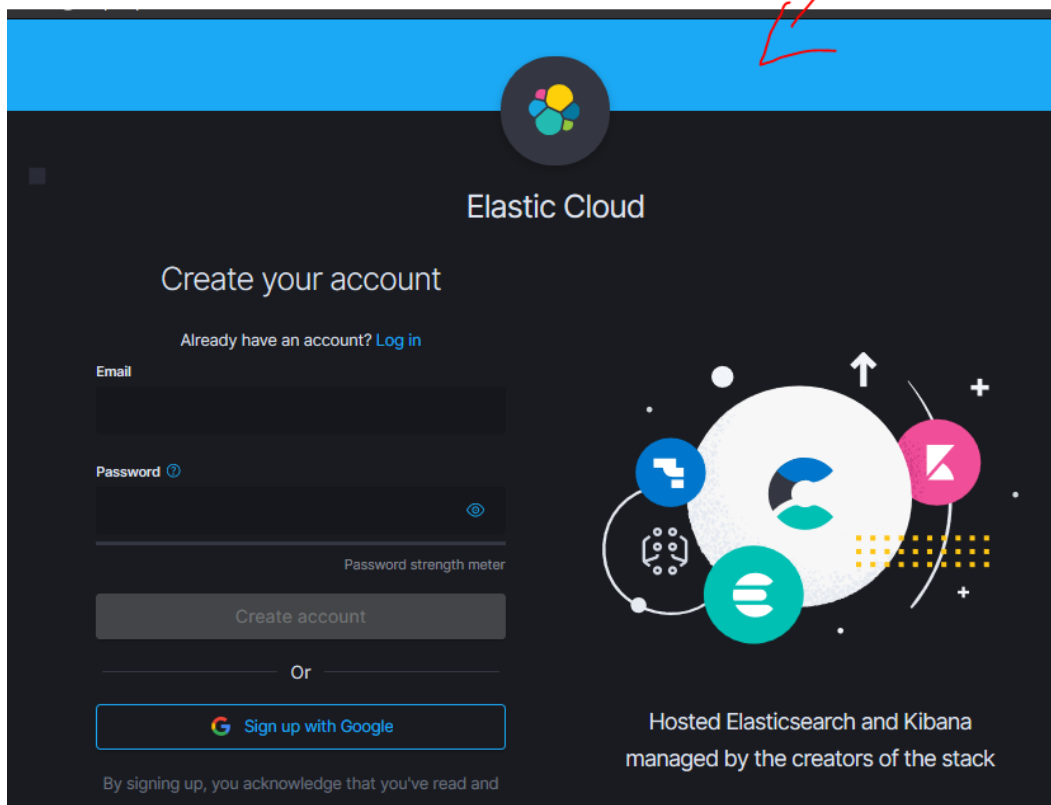
[Launch on Elastic Cloud](#)[Download](#)

Beats

Collect, parse, and ship in a lightweight fashion.

[Download](#)

Crea tu cuenta



The image shows the Elastic Cloud account creation page. At the top, there is a blue header with the Elastic logo. Below the header, the text "Elastic Cloud" is displayed. The main heading is "Create your account". Below this, there is a link "Already have an account? Log in". The form consists of an "Email" field, a "Password" field with a strength meter, and a "Create account" button. Below the form, there is a link "Or" and a "Sign up with Google" button. To the right of the form, there is a graphic with various icons and a central circular logo. Below the graphic, the text "Hosted Elasticsearch and Kibana managed by the creators of the stack" is displayed. A red arrow points to the top right corner of the page.

Elastic Cloud

Create your account

Already have an account? [Log in](#)


Email

Password [?]

Password strength meter

Create account

Or

 Sign up with Google

By signing up, you acknowledge that you've read and agree to the [Terms of Service](#) and [Privacy Policy](#)

Hosted Elasticsearch and Kibana
managed by the creators of the stack

Te llegará a tu buzón de correo para verificar la cuenta.

Hey!

Welcome to your free trial of our Elasticsearch Service.

The only thing standing between you and your free trial is the button below.

[Verify Email and Accept TOS](#)

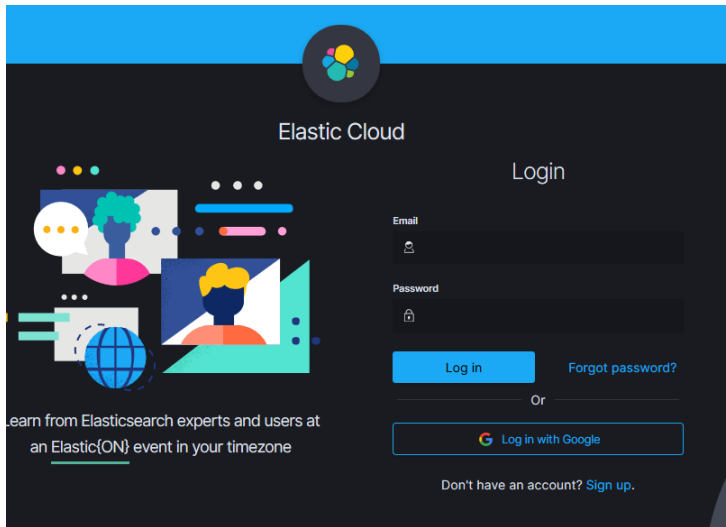
Click the button to verify your email, agree to the [Terms of Service](#), and start putting our Elasticsearch Service to the test.

Please note this link is valid for 72 hours.

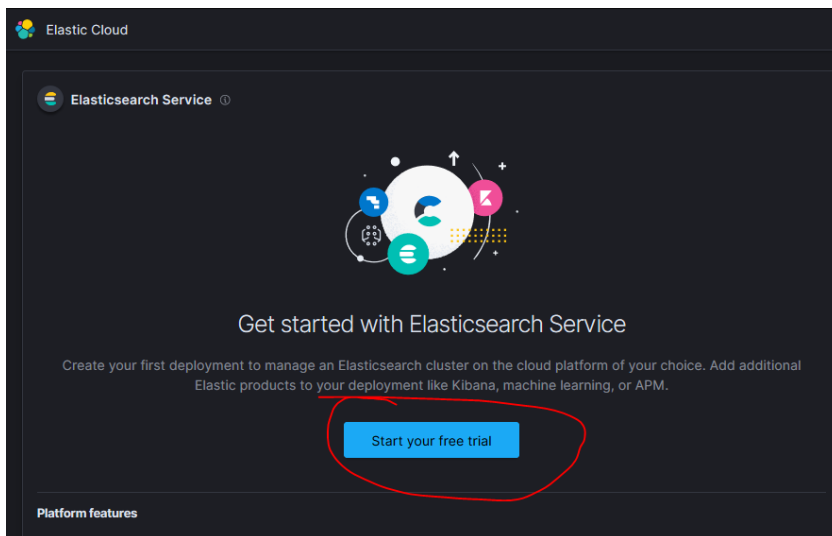
Thanks for giving us a try. And remember to have fun.

The Elastic Team

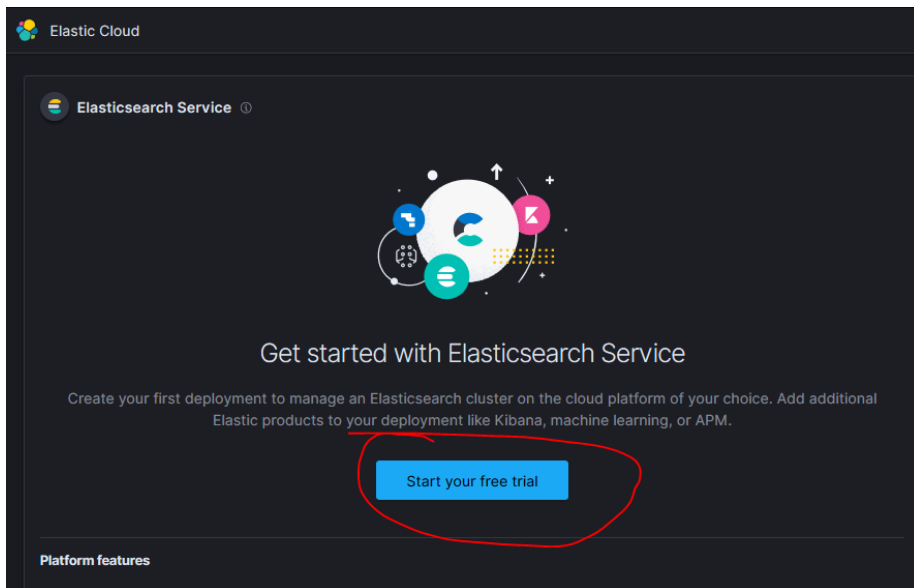
Una vez creada entrarás a la siguiente página <https://cloud.elastic.co/login> con tu usuario (correo electrónico) y contraseña.



El siguiente paso será crear un deployment con los siguientes datos:

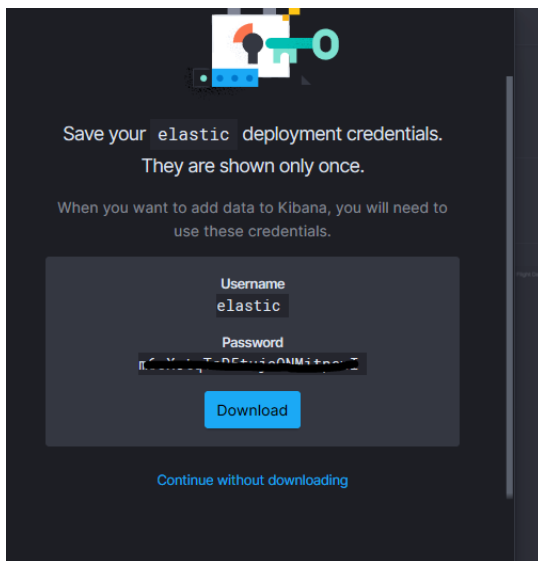


Nombre del deployment: sps_practica
Plataforma: Amazon Web Service
Region: US East (N. Virginia)
Elastic Stack version: Mas reciente
Optimize your deployment: I/O Optimized

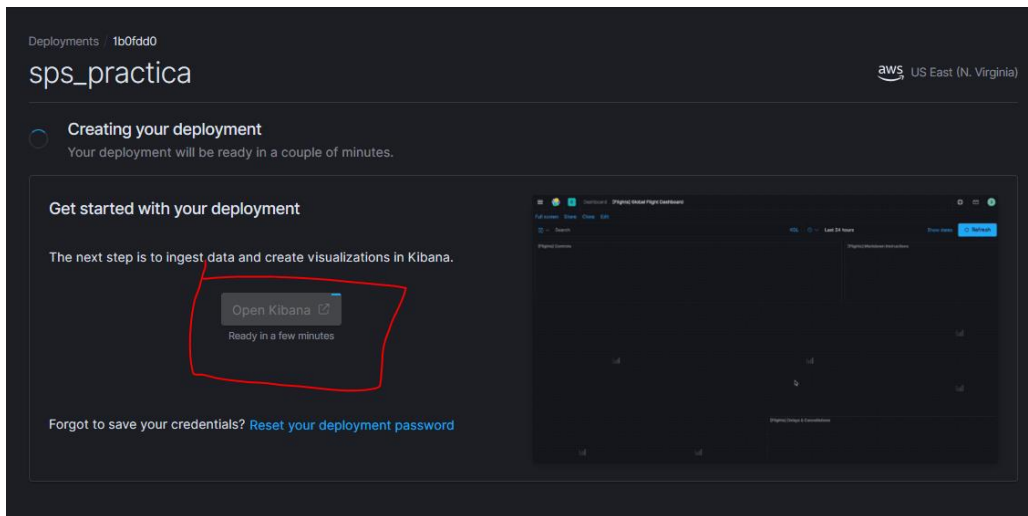


Esto tardará unos minutos ... no desesperes. Mientras tanto busca mas acerca de esta tecnología.

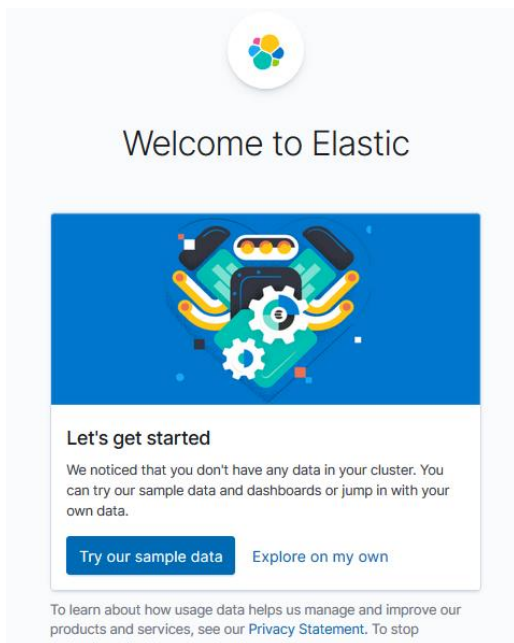
Una vez concluido el proceso copia tus credenciales de elastic:



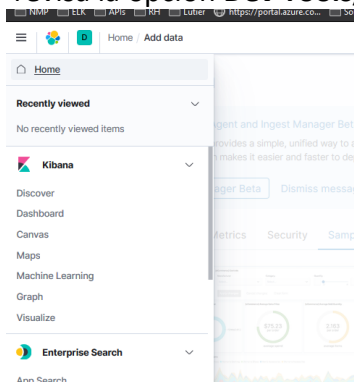
En la sección izquierda tendrás un árbol de opciones selecciona Kibana y en la sección derecha selecciona la opción Launch.



Esto te redirigirá a la consola de Kibana, pon tus credenciales de tu usuario de Elastic.



En tu menú de lado izquierdo tendrás las opciones con las que trabajaremos, por ahora revisa la opción **Dev Tools, Management, Visualize y Dashboard**.



Creación de un índice -- Tiempo 2 horas

1. Selecciona tu consola de Dev Tools para realizar la siguiente actividad.
2. Crea un índice con el nombre de `log_consultas` a partir del siguiente JSON:

```
{
  "@timestamp": "2010-05-15T22:00:54",
  "estado_consulta": "consumo",
  "servicio": "consulta",
  "administrador": "Juan Carlos",
  "consultas_realizadas": 52
}
```

3. Obtén el mapping del índice anterior y genera un template a partir de este índice haciendo uso del API de plantillas (TEMPLATE). El patrón para el índice debe ser: `"log_consultas*"`. *Verifica los tipos de datos hagan sentido con la información almacenada.*
4. Una vez definido tu template cargaras una serie de documentos en tu índice utilizando el archivo que se encuentra en el escritorio: `log_consultas.json`. Para esto utiliza el API (BULK).

Documenta cada paso

Realizar búsquedas sobre el índice -- Tiempo 2 horas

Haciendo uso del API de búsquedas (SEARCH), deberás realizar las siguientes consultas:

1. Obtener el número de registros con **estado_consulta** igual a error y consumo.
2. Obtener el número de registros realizados por el **administrador** Juan Lara.
3. Obtener el número de registros con **estado_consulta** igual a informativo y **servicio** igual a borrado
4. Obtener la suma de los valores en **consultas_realizadas** con **estado_consulta** igual a error

Consulta extra

Documenta cada paso

Realizar un tablero para visualizar información de empleados - - Tiempo 2 horas

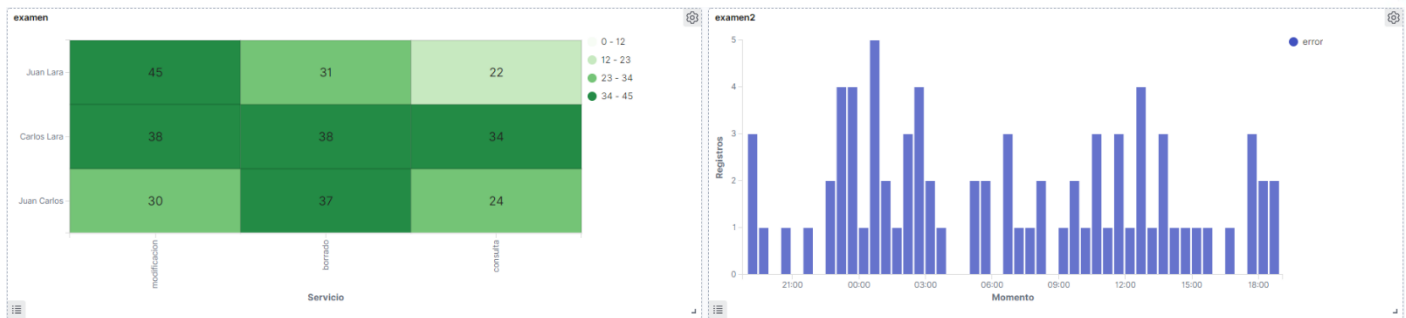
Crea un patrón de índice en **Kibana**, dirígete a la opción de **Management** y selecciona la opción **Kibana > Index Patterns** y selecciona el índice que creaste en los pasos anteriores **log_consultas** tomando como **Time Filter** el campo de `@timestamp`.

Ahora dirígete a la opción del menú **Visualize**, en esta sección vas a crear las siguientes vistas:

1. Vista de heat map, donde mostraras el número de servicios realizados por administrador.
2. Vista de Barras, donde se grafique el número de registros con **estado_consulta** igual a error a través del tiempo.

¡EXTRA!

Si te da tiempo genera un tablero con las 2 visualizaciones que acabas de crear. Para ello dirígete a la opción del menú Dashboard.



Sube la documentación paso a paso y los resultados que obtuviste al repositorio de código de tu elección y envíalo a Abigail Alanis, aalanis@spsolutions.com.mx

¡Mucho éxito!