Visualización con Kibana

ALEJANDRO PALACIO MOSQUERA
JOSE DAVID YEPES CLAVIJO
JOSE MANUEL VELASQUEZ

CONTENIDO

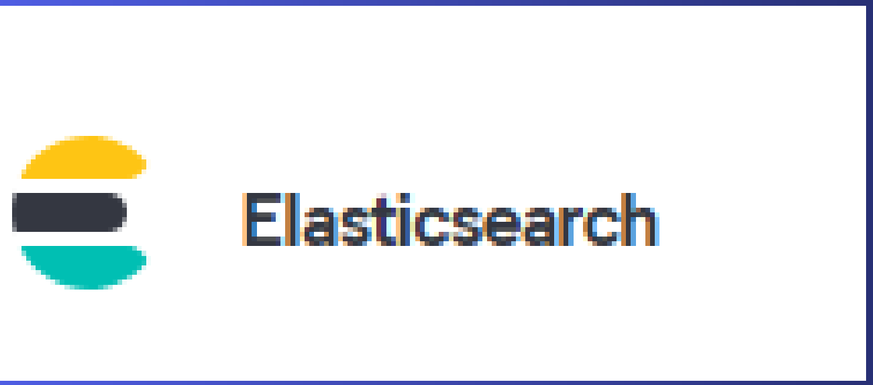
ELASTIC SEARCH

Es un motor de búsqueda y análisis distribuido y de código abierto diseñado para trabajar con grandes volúmenes de datos en tiempo real

Es el componente principal de la pila Elastic Stack, que incluye herramientas como

Logstash para la ingreso de datos

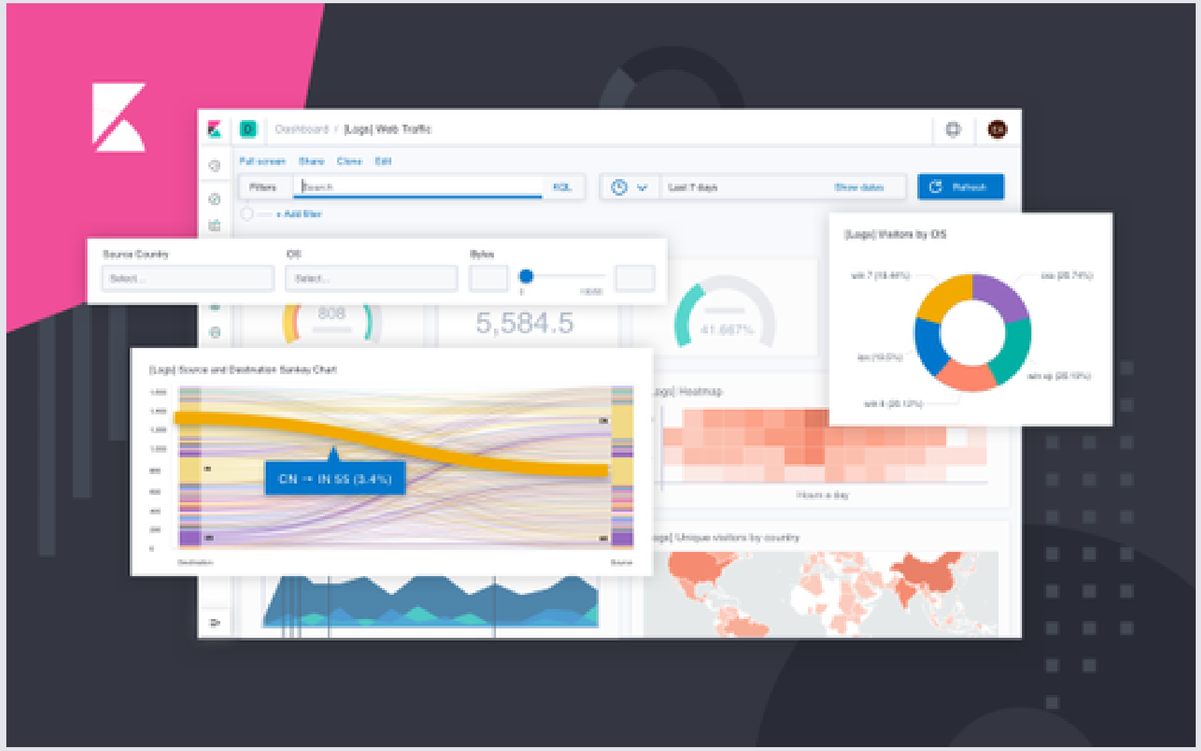
Kibana para la visualización de datos.



KIBANA

Es una plataforma de visualización de datos, permite a los usuarios visualizar y analizar datos almacenados en Elasticsearch a través de gráficos interactivos, dashboards, y mapas.

Su propósito principal es facilitar la interpretación de grandes volúmenes de datos mediante herramientas visuales que ayudan en el monitoreo, la búsqueda, y el análisis en tiempo real.



Caracteristicas principales:

- Dashboards personalizables
- Gráficos interactivos
- Exploración de datos y búsqueda
- Análisis en tiempo real
- Alertas y Machine Learning

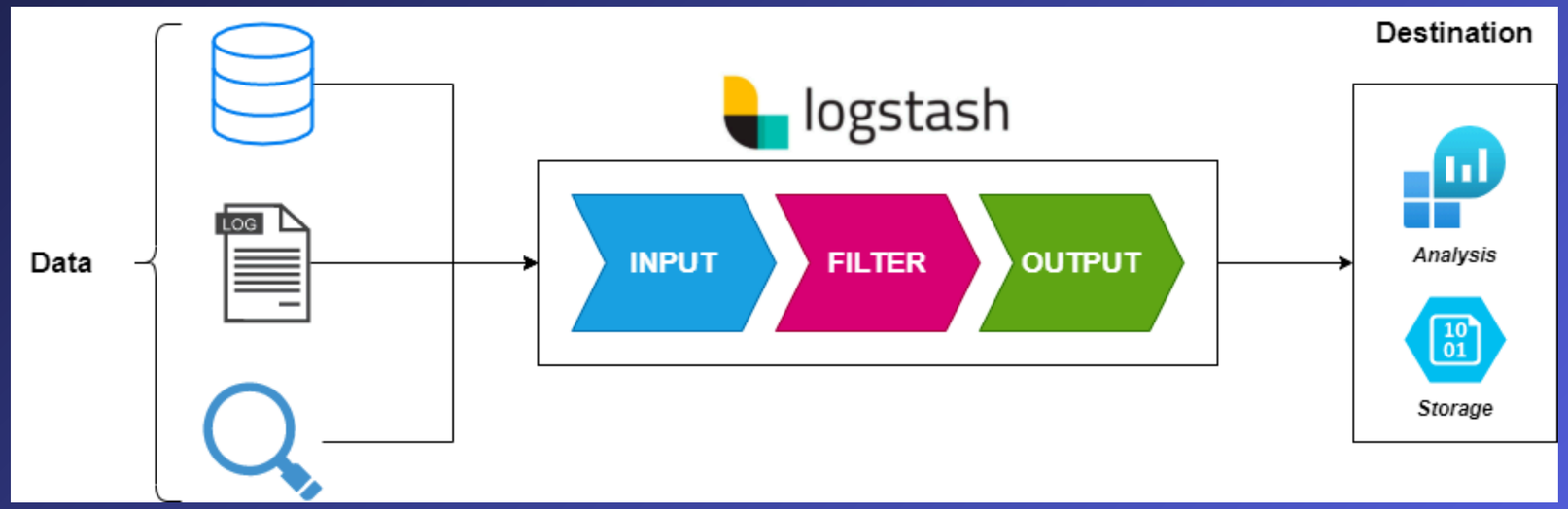
LOGSTASH

Es una herramienta de procesamiento de datos en tiempo real

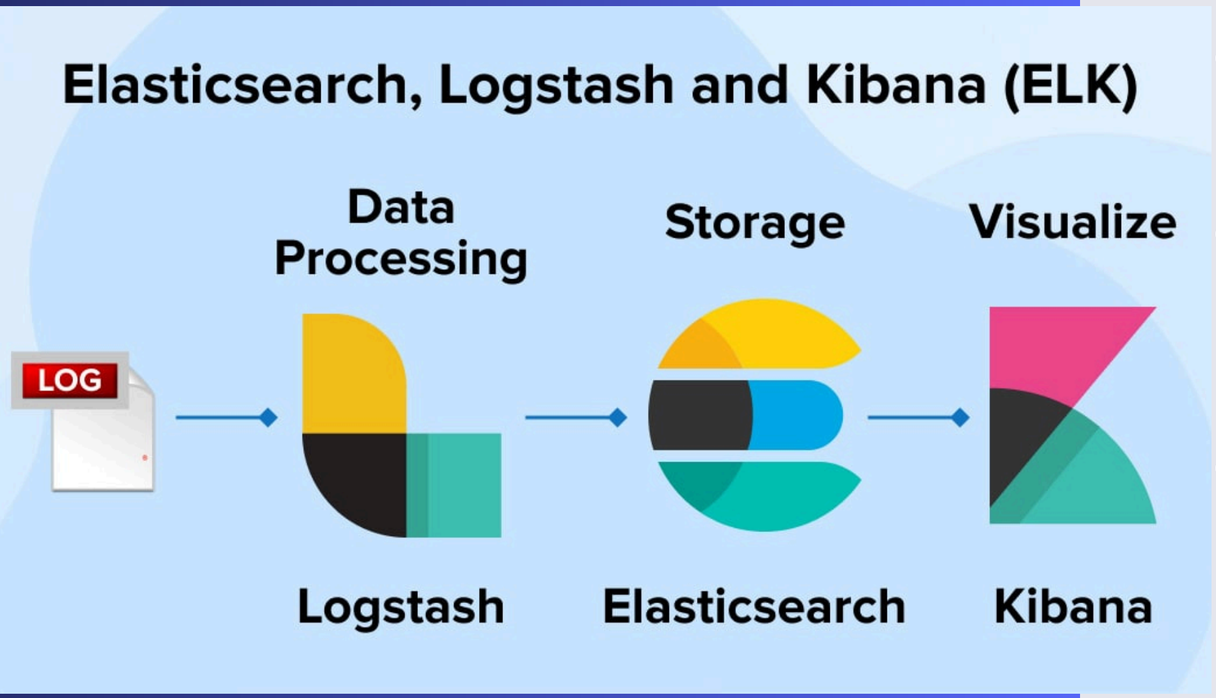
Fue creada para recolectar, procesar y transformar datos de diversas fuentes, y luego enviarlos a un almacenamiento como Elasticsearch o una base de datos para su análisis y visualización.

Caracteristicas principales:

- Ingesta de datos desde múltiples fuentes
- Transformación de datos
- Envío a múltiples destinos



COMO SE INTEGRA



- Entrada: Logstash ingesta datos desde múltiples fuentes, aplicando filtros y transformaciones.
- Indexación: Los datos procesados se envían a Elasticsearch, donde se almacenan e indexan para búsquedas rápidas.
- Visualización: Kibana accede a los datos en Elasticsearch y permite la creación de gráficos y dashboards que facilitan el análisis.

FUNCIONALIDADES

ELASTICSEARCH: ALMACENAMIENTO Y BÚSQUEDA DE DATOS

- **Indexación y Almacenamiento**: Permite almacenar y organizar datos de forma estructurada.
- **Búsqueda Compleja:** Usa un motor de búsqueda basado en Apache Lucene.
- **Escalabilidad:** Elasticsearch puede manejar grandes volúmenes de datos en un sistema distribuido.
- **Análisis y Agregación de Datos**: Ofrece herramientas para analizar datos en tiempo real,

LOGSTASH: INGESTA Y PROCESAMIENTO DE DATOS

- **Ingesta de Múltiples Fuentes:** puede recopilar datos de diferentes fuentes.
- **Transformación de Datos:** Permite aplicar filtros, transformar datos y realizar ajustes de formato antes de enviarlos a Elasticsearch.
- **Enriquecimiento de Datos:** Puede agregar metadatos.
- **Salida Configurable:** puede enviar datos a múltiples destinos, como bases de datos, archivos y otras aplicaciones.

KIBANA: VISUALIZACIÓN Y ANÁLISIS DE DATOS

- **Dashboards y Visualizaciones:** permite crear visualizaciones y dashboards interactivos para monitorear y analizar datos.
- **Búsqueda y Filtrado:** Ofrece una interfaz para realizar búsquedas sobre los datos indexados.
- **Análisis en Tiempo Real:** Permite el monitoreo en tiempo real.
- **Herramientas Adicionales:** incluye aplicaciones adicionales.

DESCRIPCIÓN DEL PROYECTO

Crear un entorno de análisis y visualización de datos utilizando Elastic Stack y Kibana. Configurar la recolección y análisis de grandes volúmenes de datos estructurados y no estructurados usando datasets de fuente abierta, por ejemplo, de Kaggle. Desarrollar dashboards interactivos para la toma de decisiones basadas en datos.

IMPLEMENTACIÓN

```
input {
  # Usar entrada desde stdin (para ingresar datos manualmente)
  stdin {
    codec => "json"   # Puedes cambiar esto si usas un formato diferente
  }
}

filter {
  # Este paso es opcional; se puede agregar lógica de filtrado aquí si necesitas procesar los datos
}

output {
  # Enviar los datos a Elasticsearch
  elasticsearch {
    hosts => ["https://192.168.200.3:9200"]  # Dirección de Elasticsearch
    ssl_certificate_verification => false
    user => "elastic"
    password => "aW9fVQP5vHx_WEdjxVbP"
    index => "manual_data"              # Nombre del índice donde se almacenarán los datos
    document_id => "%{some_unique_field}"
  }

  # Mostrar en consola (esto es opcional, solo para verificar)
  stdout {
    codec => rubydebug
  }
}
```

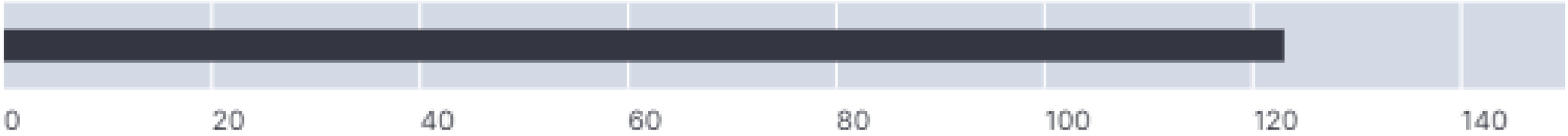
PRUEBAS

```
vagrant@servidorParcial:/etc/logstash/conf.d$ sudo /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/test.conf
```

```
The stdin plugin is now waiting for input:
{"name": "test", "value": 123}
{
      "@version" => "1",
          "name" => "test",
         "event" => {
        "original" => "{\"name\": \"test\", \"value\": 123}\n"
    },
         "value" => 123,
    "@timestamp" => 2024-11-06T17:49:01.195689171Z,
          "host" => {
        "hostname" => "servidorParcial"
    }
}
```

Median of value

123



Median of value

123

@timestamp per 30 seconds	Median of value
14:25:00	-
14:25:30	-
14:26:00	-
14:26:30	-
14:27:00	-
14:27:30	123
14:28:00	-
14:28:30	-
14:29:00	-
14:29:30	-

elastic

Find apps, content, and more. ^/

D Dashboards Editing DASHBOARD_LAPTOPS

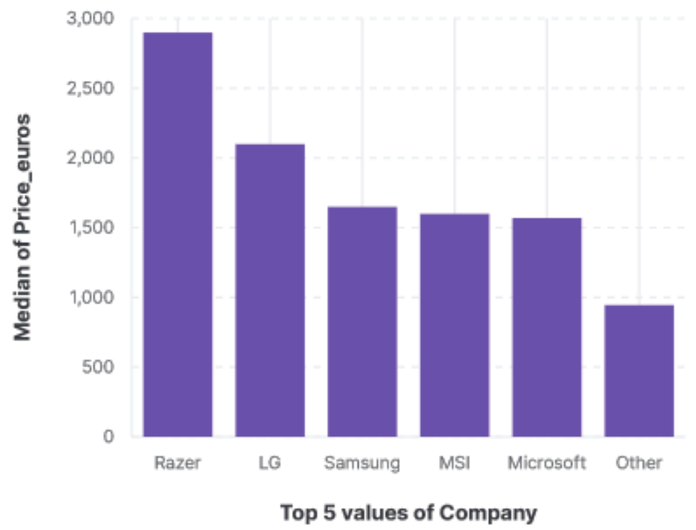
Settings Share Save as Switch to view mode Reset Save

Filter your data using KQL syntax

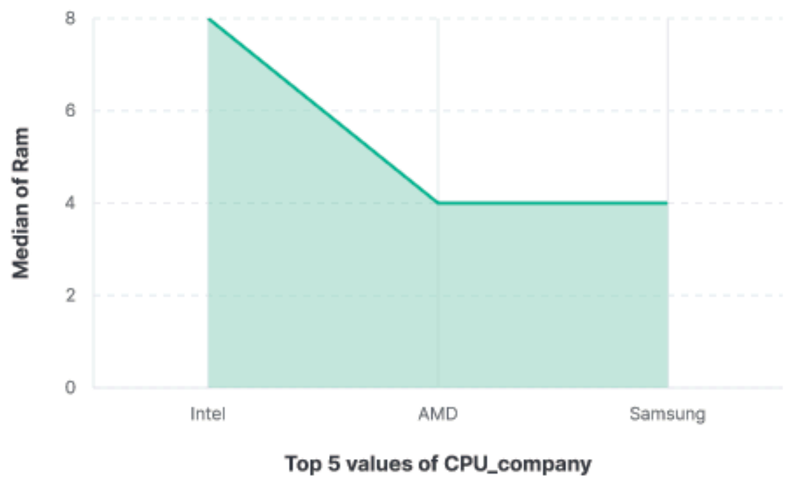
Last 15 minutes

Create visualization Add panel Add from library Controls

Precio Euros



RAM



PESO

Top 5 values of Company	Median of Weight
MSI	2.515
Acer	2.2
Asus	2.2
Fujitsu	2.2
Dell	2.18
Other	1.89

DEMOSTRACIÓN

CONCLUSIONES

- Kibana nos facilita la búsqueda de archivos de registros representando datos de manera intuitiva, facilitando el análisis de tendencias y patrones en tiempo real mediante gráficos y dashboards personalizables.

- Logstash es esencial para la ingesta de datos recopila, procesa y transforma datos de diversas fuentes, preparándolos para ser almacenados en Elasticsearch.

- Eficiencia en la recopilación hasta la visualización de datos, permitiendo el monitoreo y análisis en tiempo real en un solo entorno, lo que optimiza tanto la gestión como el análisis de grandes volúmenes de información.

REFERENCIAS

- BMC, "Logstash: Using Data Pipeline," BMC Blogs. [Enlace]. Disponible en: https://www.bmc.com/blogs/logstash-using-data-pipeline/. [Accedido: 30-Oct-2024].
- Tatvasoft, "Data Analytics with Elasticsearch, Logstash & Kibana (ELK)," Tatvasoft Blogs. [Enlace]. Disponible en: https://www.tatvasoft.com/blog/data-analytics-elasticsearch-logstash-kibana-elk/. [Accedido: 30-Oct-2024].
- Elastic, "Kibana Dashboard," Elastic. [Enlace]. Disponible en: https://www.elastic.co/es/kibana/kibana-dashboard. [Accedido: 30-Oct-2024].
- Simplifying Tech Code, "How to Install and Configure Elasticsearch, Kibana & Logstash 8.12 Version on Ubuntu Linux 2024," Simplifying Tech Code, 15-Mar-2024. [Enlace]. Disponible en: https://simplifyingtechcode.wordpress.com/2024/03/15/how-to-install-and-configure-elasticsearch-kibana-logstash-8-12-version-on-ubuntu-linux-2024/. [Accedido: 30-Oct-2024].
- Elastic, "Elasticsearch," Elastic. [Enlace]. Disponible en: https://www.elastic.co/es/elasticsearch. [Accedido: 30-Oct-2024].
- Simplifying Tech, "How to Install Elasticsearch, Kibana & Logstash | Tutorial | Simplifying Tech," YouTube, 2024. [Enlace]. Disponible en: https://www.youtube.com/watch?v=y0VH131_r84&ab_channel=SimplifyingTech. [Accedido: 30-Oct-2024].