

ASIR

PASIR

MANUAL DE USO

Pedro Peralta Guerrero
19 de junio de 2023

Índice

1. Manejo de índices	2
2. Patrones de índices	2
3. Discover	3
4. Dashboard	4
5. Visualizations	5

En este documento se explicará el uso básico del panel de OpenSearch, es decir, manejo de índices, creación de patrones de índices, creación de dashboard y creación de visualizaciones.

1. Manejo de índices

Si nos dirigimos al apartado **Index Management** > **Índices** podremos ver todos los índices, ver el estado de salud y realizar ciertas operaciones con ellos:

- Crear un nuevo índice: Puedes crear un nuevo índice proporcionando un nombre y una configuración específica. Esto te permite organizar y almacenar tus datos de manera adecuada.
- Listar los índices existentes: OpenSearch Dashboards te muestra una lista de todos los índices disponibles en tu clúster. Puedes ver información como el nombre, tamaño y número de documentos en cada índice.
- Ver estadísticas del índice: Puedes acceder a estadísticas detalladas de un índice en particular, como el número de documentos indexados, tamaño del índice, estadísticas de búsqueda y más.
- Actualizar la configuración del índice: Puedes modificar la configuración de un índice existente, como los análisis de texto, los campos indexados o las configuraciones de retención de datos.
- Eliminar un índice: Si ya no necesitas un índice, puedes eliminarlo para liberar espacio y recursos en tu clúster. Sin embargo, debes tener cuidado al hacerlo, ya que esto resultará en la pérdida permanente de los datos almacenados en ese índice.
- Administrar políticas de ciclo de vida (Lifecycle Policies): Puedes configurar políticas de ciclo de vida para tus índices. Estas políticas definen acciones automáticas, como la eliminación o el archivado de datos después de cierto tiempo o tamaño. Esto te permite administrar el crecimiento y el mantenimiento de los índices de manera eficiente.

Index	Health	Managed by policy	Status	Total size	Size of primaries	Total documents	Deleted documents	Primaries	Replicas
system-logs-2023.06.18	Green	No	Open	39.1mb	39.1mb	119816	0	1	1
security-auditlog-2023.06.18	Green	No	Open	491.3kb	491.3kb	165	0	1	1
security-auditlog-2023.06.13	Green	No	Open	780.8kb	780.8kb	766	0	1	1
.opensearch-observability	Green	No	Open	6kb	6kb	1	0	1	1
.opensearch-notifications-config	Green	No	Open	208b	208b	0	0	1	1
.opendistro_security	Green	No	Open	71.7kb	71.7kb	10	0	1	1
.opendistro-reports-instances	Green	No	Open	6.1kb	6.1kb	1	0	1	1

Figura 1: Anexo B: Manejo de índices

2. Patrones de índices

Para crear un “Index Pattern” en OpenSearch Dashboards debmos de seguir estos pasos:

- Nos dirigimos a la sección “Stack Management” en el menú lateral.
- Hacer clic en el botón “Create index pattern” (Crear patrón de índice).
- En el campo “Index pattern” (Patrón de índice), ingresa el nombre o patrón que quieres utilizar para identificar múltiples índices. El patrón puede contener comodines como asteriscos para que coincida con varios índices con nombres similares. Por ejemplo, si existen índices con nombres como "logs-2023-01-01", "logs-2023-01-02", etc., se puede ingresar "logs- como patrón.

- En el campo “Time Filter field name” (Nombre del campo de filtro de tiempo), selecciona el campo de fecha o timestamp que se utilizará para filtrar y visualizar datos en un rango de tiempo específico. Este campo debe existir en los índices que coinciden con el patrón.
- Haz clic en el botón “Create index pattern” (Crear patrón de índice) para crear el patrón de índice.

El “Index Pattern”(Patrón de índice) se utiliza en OpenSearch Dashboards para definir cómo se accede y visualiza la información de los índices relacionados. Proporciona una forma de agrupar y consultar datos de múltiples índices de manera eficiente.

Al crear un “Index Pattern”, OpenSearch Dashboards va a realizar las siguientes tareas:

- Identifica y registra los índices que coinciden con el patrón proporcionado.
- Extrae información sobre los campos y tipos de datos disponibles en los índices.
- Configura la visualización de datos, lo que permite utilizar herramientas como gráficos, tablas y visualizaciones personalizadas para explorar y analizar los datos contenidos en los índices.
- Habilita la funcionalidad de búsqueda y filtrado de datos utilizando el campo de filtro de tiempo especificado.

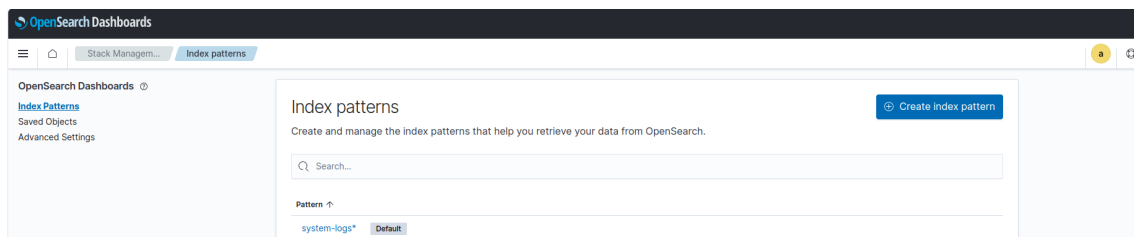


Figura 2: Anexo B: Patrones de índices

3. Discover

El apartado “Discover” en OpenSearch Dashboards proporciona una interfaz para explorar y buscar datos en los índices. Accederemos desde el menú lateral pulsado en la pestaña “Discover”. El uso de esta interfaz es la siguiente:

- Selección del índice: En la parte superior de la página, existe un desplegable donde puedes seleccionar el índice o el patrón de índice que desees explorar. Puedes elegir entre los patrones de índice que hayas creado previamente o seleccionar un índice específico
- Vista de documentos: En la parte central de la página, verás una tabla que muestra los documentos de los índices seleccionados. Cada fila representa un documento individual y cada columna corresponde a un campo dentro del documento.
- Búsqueda y filtrado: En la parte superior de la página, encontraremos una barra de búsqueda que permite buscar datos específicos en los documentos. Se puede ingresar consultas de búsqueda para filtrar los resultados en función de los valores de los campos. También podemos aplicar filtros adicionales para refinar aún más los resultados.

- Guardado de búsquedas: Si se desea conservar una búsqueda específica para referencia futura, nos permite guardarla haciendo clic en el botón “Save” (Guardar) en la barra de herramientas superior. Esto te permite acceder rápidamente a la búsqueda guardada en cualquier momento.

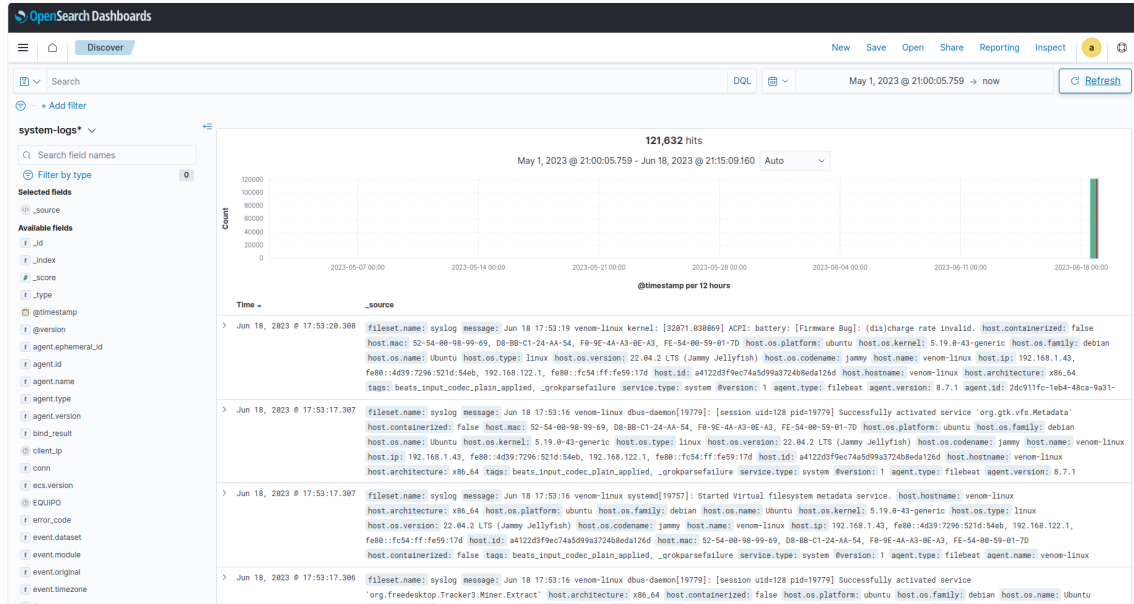


Figura 3: Anexo B: Discover

4. Dashboard

OpenSearch Dashboards es una sección que nos permite crear paneles de control personalizados para visualizar y analizar los datos de manera visual y práctica. El funcionamiento es el siguiente:

- Acceso a Dashboard: En el menú lateral de OpenSearch Dashboards, haz clic en la pestaña “Dashboard” para acceder a esta herramienta.
- Creación de un nuevo panel: Puedes comenzar creando un nuevo panel haciendo clic en el botón “Create dashboard” (Crear panel) o seleccionando uno existente si ya existe uno.
- Diseño del panel: Una vez en el panel, se puede diseñar la apariencia y contenido. Podemos agregar elementos como gráficos, visualizaciones, tablas, métricas, filtros y otros componentes interactivos. Estos elementos se conocen como "visualizaciones" permiten representar tus datos de diversas formas.
- Configuración de las visualizaciones: Cada visualización en el panel se puede configurar para mostrar datos específicos de los índices. Podemos elegir el índice, definir consultas de búsqueda y aplicar filtros para limitar los datos que se muestran en cada visualización.
- Organización del panel: Es posible organizar las visualizaciones en el panel según las necesidades. Se puede mover y redimensionar las visualizaciones, crear múltiples páginas o pestañas dentro del panel y establecer filtros interactivos para que los datos se actualicen automáticamente.
- Guardado y compartición del panel: Una vez que el panel esté diseñado es posible guardarlo para acceder a él posteriormente. También se puede compartir con otros usuarios para que puedan ver el mismo panel de control y beneficiarse de la visualización de datos.
- Personalización y configuración adicional: OpenSearch Dashboards ofrece varias opciones de personalización y configuración para los paneles. Podemos ajustar la apariencia visual, configurar paneles en modo de pantalla completa, establecer opciones de actualización automática y más.

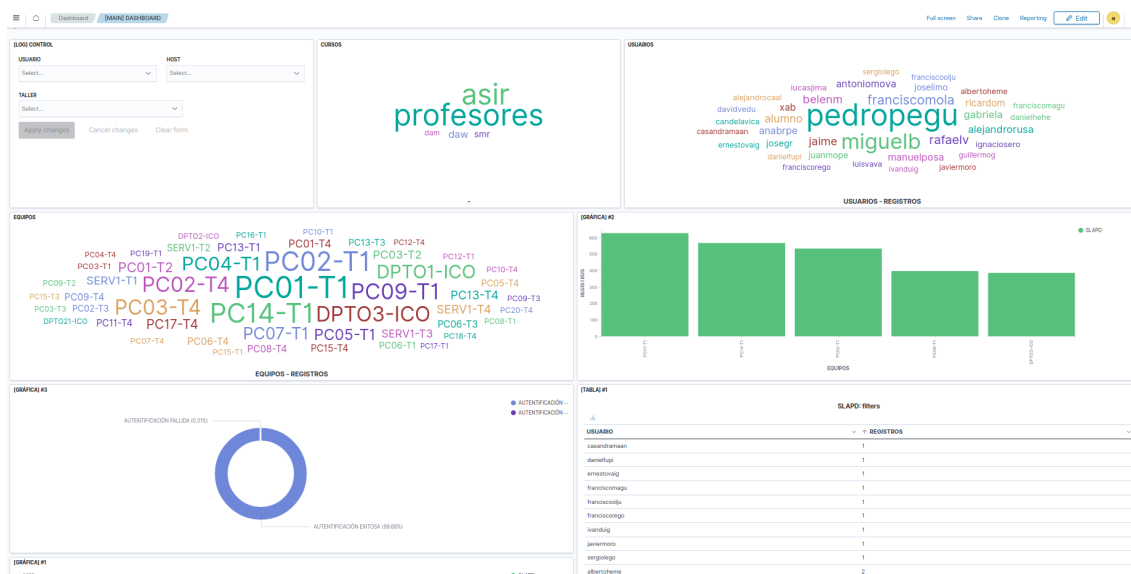


Figura 4: Anexo B: Dashboard

5. Visualizations

El apartado “Visualizations” en OpenSearch Dashboards es una sección que permite crear y personalizar visualizaciones de datos para mostrar información de manera gráfica y comprensible.

- **Acceso a Visualizations:** En el menú lateral de OpenSearch Dashboards, hacer clic en la pestaña “Visualizations” para acceder a esta herramienta.
- **Creación de una nueva visualización:** Creamos una nueva visualización haciendo clic en el botón “Create visualization” (Crear visualización) o seleccionando una visualización existente si ya existe alguna creada.
- **Selección del tipo de visualización:** OpenSearch Dashboards ofrece una variedad de tipos de visualizaciones, como gráficos de barras, gráficos de líneas, tablas, gráficos circulares y más. Podemos seleccionar el tipo de visualización que mejor se adapte a tus datos y objetivos.
- **Configuración de la fuente de datos:** Para cada visualización, se debe configurar la fuente de datos, es decir, el índice o patrón de índice que contiene los datos que deseas visualizar. Puedes definir consultas de búsqueda y filtros para limitar los datos que se mostrarán en la visualización.
- **Configuración de los campos y métricas:** Puedes seleccionar los campos específicos que se desea visualizar y definir las métricas o agregaciones que se aplicarán a esos campos. Por ejemplo, puedes mostrar la suma, el promedio o el recuento de los valores de un campo en particular.
- **Personalización de la apariencia visual:** Es posible personalizar la apariencia visual de la visualización, como el color, el tamaño, los ejes, las etiquetas y otros elementos visuales. Esto te permite adaptar la visualización a tus preferencias y requisitos específicos.
- **Guardado de la visualización:** Una vez que se haya configurado y personalizado la visualización, podemos guardarla para acceder a ella posteriormente y reutilizarla en diferentes paneles o dashboards.
- **Compartición de la visualización:** OpenSearch Dashboards permite compartir visualizaciones con otros usuarios, lo que les permite ver y utilizar las mismas visualizaciones en sus propios paneles y dashboards.

