Elasticsearch

Queries

Sobre los índices de la forma “log-generator-”

1. Realizar una query que retorne todos los documentos que contengan “Ingreso” en el campo “responseText”
2. Realizar una query que retorne todos los documentos que contengan “User” en alguno de los siguientes campos [“stacktrace”, “action”]
3. Realizar una query que retorne todos los documentos que contengan exactamente “DELETE USER” en el campo “action”
4. Ejecutar una query que retorne todos los documentos que contengan en el campo “action” alguno de los siguientes valores “DELETE USER” o “SEND EMAIL”.
5. Retornar todos los nombres de usuario que contengan el sufijo “man”.
6. Ejecutar un query que retorne todos los documentos que cumplan las siguientes condiciones simultáneamente:
    a. Su nombre de usuario sea “IronMan”
    b. El tipo de log no sea "LOGIN"
    c. Que cumpla por lo menos una de estas condiciones: La duración esté entre 1 y 2 o la acción sea “DELETE USER”
7. Separar los documentos en buckets según el “logtype” al que correspondan.
8. Obtener el promedio de duración entre el total de los documentos.
9. Obtener la cantidad de registros de cada ‘level’.
10. Obtener los “stats” sobre la duración del total de documentos.

Sobre los índices de la forma curso-*

11. Crear índice cuyo nombre tenga la forma **curso-nombre_alumno**
12. Utilizando la BULK API cargar sobre el índice **curso-nombre_alumno** los documentos que se encuentran en el archivo accounts.json
    Ayuda: para crear un índice con el contenido podrán utilizar el siguiente comando

    ```
    POST /curso-nombre_alumno/_bulk
    <documentos-formato-json>
    ```

    Siendo documentos-formato-json el contenido del archivo a cargar.
13. Eliminar el documento utilizando al DELETE API y el campo “_id”.
14. Eliminar todos los documentos de cuentas pertenecientes al estado de Illinois (state: IL) , y luego comprobar si efectivamente los eliminaron.

15. Actualizar un documento por su "_id".
16. Actualizar todos los documentos que tengan un balance menor a 10000 agregando el campo plus con el valor 2000.

Index Template

1. Generar un index template para los documentos teniendo en cuenta los siguientes puntos:
    a. Evitar la generación de campos full text sobre los que no se va a realizar búsquedas full text.
    b. Asegurar que los campos correspondientes al filtro geoip sean del tipo correspondiente.