Transferring SQL Server Database to Elastic Search Using Logstash & JDBC

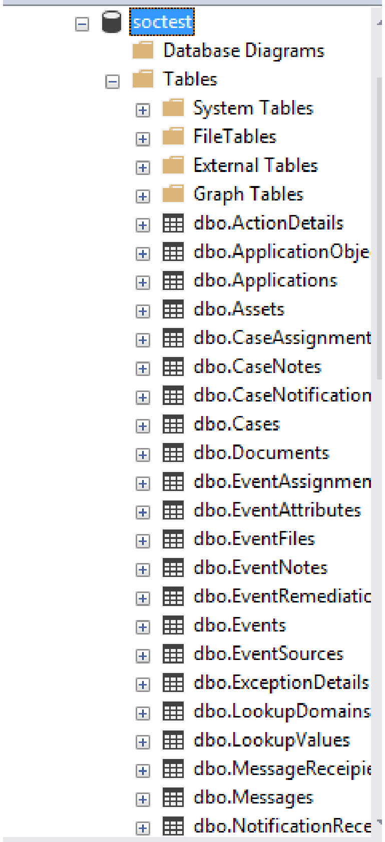
(JAVA DATABASE CONNECTOR)

-Anshuman Dey Kirty

Steps:

(Importing *soctest.bkp* on SQL Server)

1. Create Server using the *SQL Server Installation Centre* on the C:\SQLServer2017Media\Express_ENU\setup.exe
2. Click on *New SQL Server Stand-alone installation and add feature to an existing installation.*
3. Name instance.
4. Choose *SQL Authentication mode* under *Database Engine Configuration*.
5. After creation of server, open the *Microsoft SQL Server Management Studio*.
6. Database from .bkp file
   i) Create a database then right click on it
   Tasks ->Restore ->Database
   ii) Select the database .bkp file (soctest.bkp) and import it.



(Transfer process to Elasticsearch using Logstash)

7. Install and Run Elasticsearch.
8. Run Logstash using the command (`bin\logstash -f logstash.conf`) by creating the .conf (configure) file in the given method below.

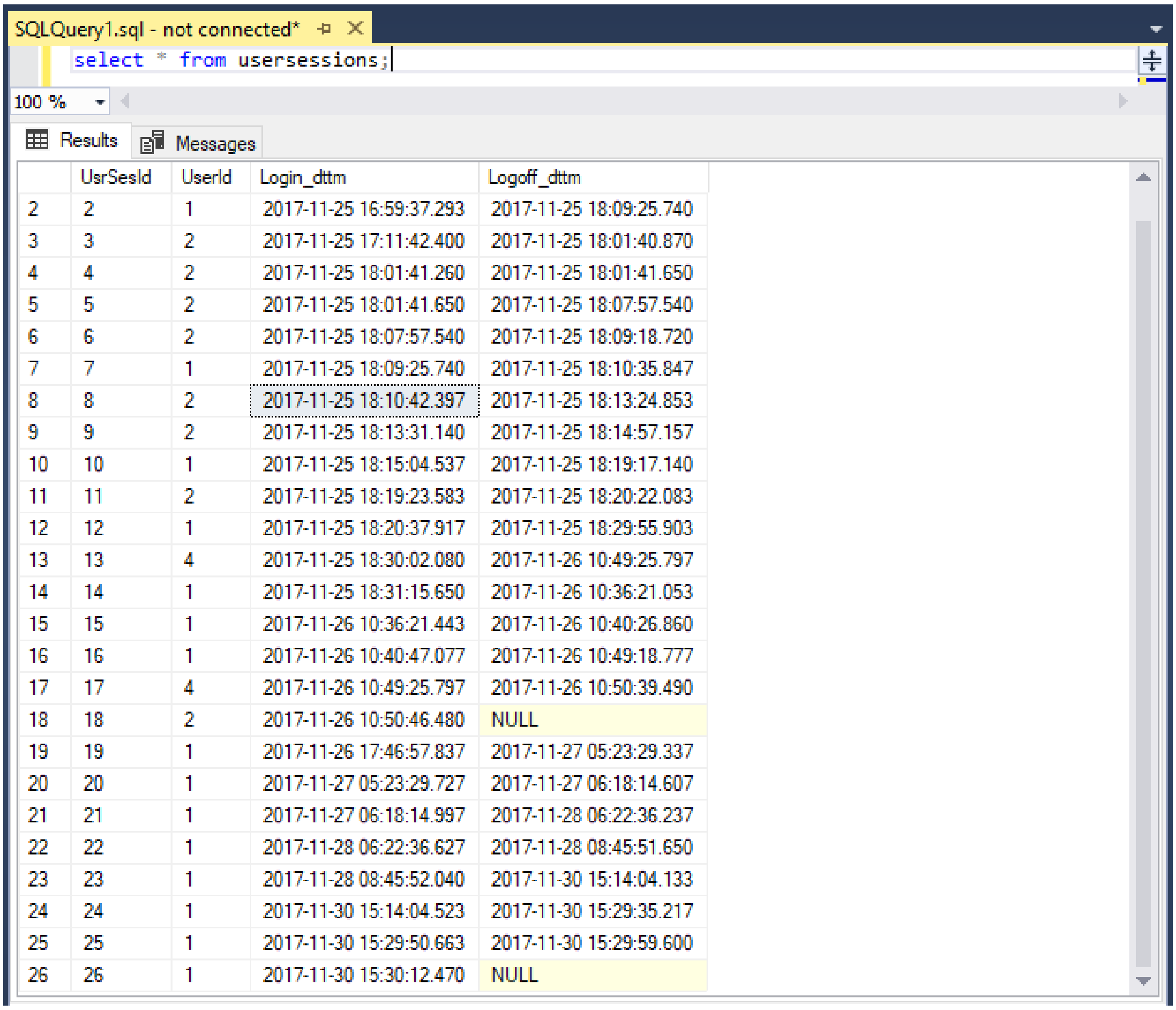
Code:

```
input {
      jdbc {
            jdbc_driver_library =>
            jdbc_driver_class =>
      jdbc_connection_string =>
 "jdbc:sqlserver://DB Name;user=username;password=pass;"
      jdbc_user => ""
      #our Query
      statement => "select * from [soctest].[dbo].[UserSessions]"

      }
}
output{
      stdout { codec => json_lines }
      elasticsearch{
      "hosts" => ["localhost:9200"]
      "index" => "soctest"
      "document_type" => "Tables"
      }
}
```

Output:

Table *Usersessions* with 26 Rows.

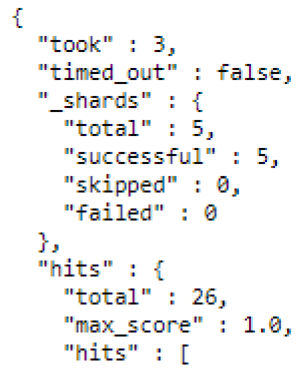


```
select * from usersessions;
```

	UsrSesId	UserId	Login_dttm	Logoff_dttm
2	2	1	2017-11-25 16:59:37.293	2017-11-25 18:09:25.740
3	3	2	2017-11-25 17:11:42.400	2017-11-25 18:01:40.870
4	4	2	2017-11-25 18:01:41.260	2017-11-25 18:01:41.650
5	5	2	2017-11-25 18:01:41.650	2017-11-25 18:07:57.540
6	6	2	2017-11-25 18:07:57.540	2017-11-25 18:09:18.720
7	7	1	2017-11-25 18:09:25.740	2017-11-25 18:10:35.847
8	8	2	2017-11-25 18:10:42.397	2017-11-25 18:13:24.853
9	9	2	2017-11-25 18:13:31.140	2017-11-25 18:14:57.157
10	10	1	2017-11-25 18:15:04.537	2017-11-25 18:19:17.140
11	11	2	2017-11-25 18:19:23.583	2017-11-25 18:20:22.083
12	12	1	2017-11-25 18:20:37.917	2017-11-25 18:29:55.903
13	13	4	2017-11-25 18:30:02.080	2017-11-26 10:49:25.797
14	14	1	2017-11-25 18:31:15.650	2017-11-26 10:36:21.053
15	15	1	2017-11-26 10:36:21.443	2017-11-26 10:40:26.860
16	16	1	2017-11-26 10:40:47.077	2017-11-26 10:49:18.777
17	17	4	2017-11-26 10:49:25.797	2017-11-26 10:50:39.490
18	18	2	2017-11-26 10:50:46.480	NULL
19	19	1	2017-11-26 17:46:57.837	2017-11-27 05:23:29.337
20	20	1	2017-11-27 05:23:29.727	2017-11-27 06:18:14.607
21	21	1	2017-11-27 06:18:14.997	2017-11-28 06:22:36.237
22	22	1	2017-11-28 06:22:36.627	2017-11-28 08:45:51.650
23	23	1	2017-11-28 08:45:52.040	2017-11-30 15:14:04.133
24	24	1	2017-11-30 15:14:04.523	2017-11-30 15:29:35.217
25	25	1	2017-11-30 15:29:50.663	2017-11-30 15:29:59.600
26	26	1	2017-11-30 15:30:12.470	NULL

From Elasticsearch:

Total Hits: 26



```
{
  "took" : 3,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 26,
    "max_score" : 1.0,
    "hits" : [
```

All the Data has been Transferred Successfully.