Opensearch indesxer :- in new version we use opensearch indexer instead of wazuh indexer.

Opensearch Dashboard :- in new version we use opensearch dashboard instead of wazuh dashboard.

1.cluster :- collection of nodes

2.node :- instance

3.index :- understand like a table in sql

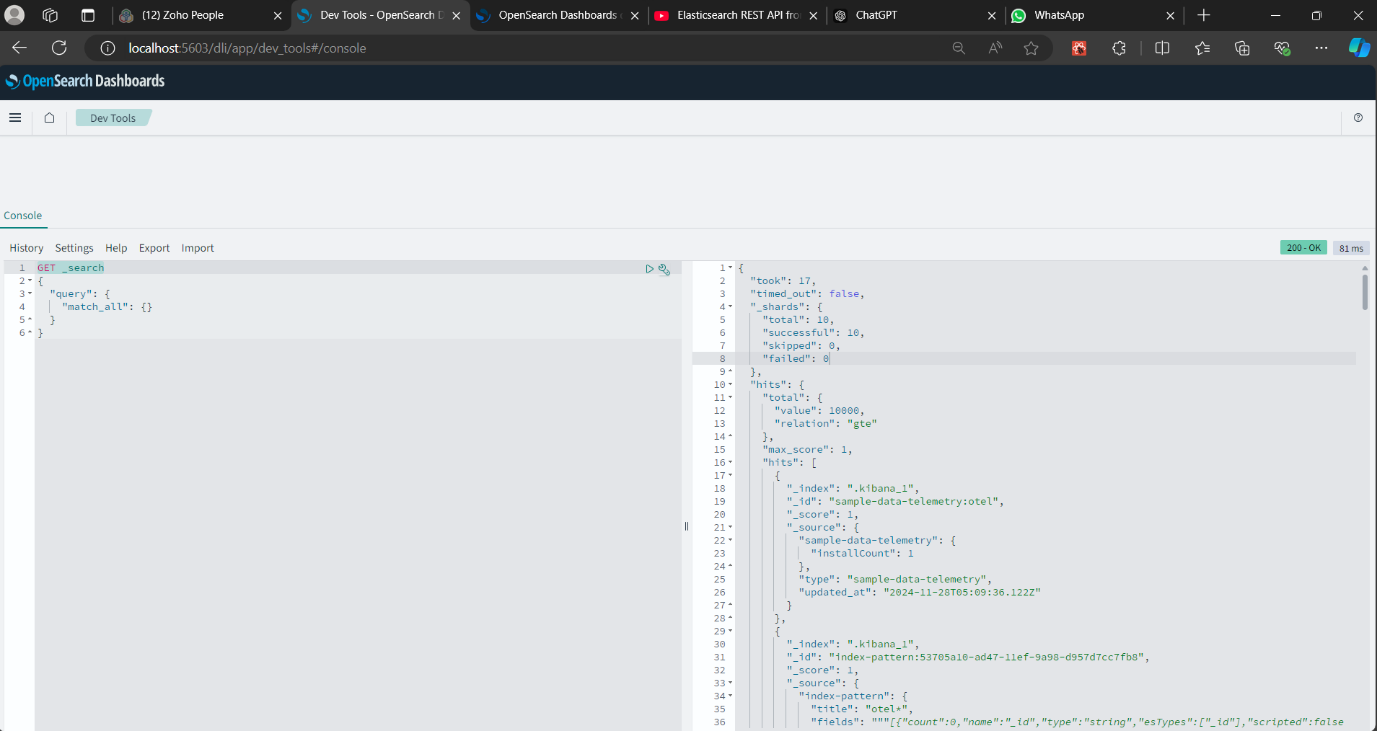
4.field:- columns

5.document:- rows

It is also collection of meta data and json data

**Dev tool**

1. GET \_search :- gives all data and all indexes

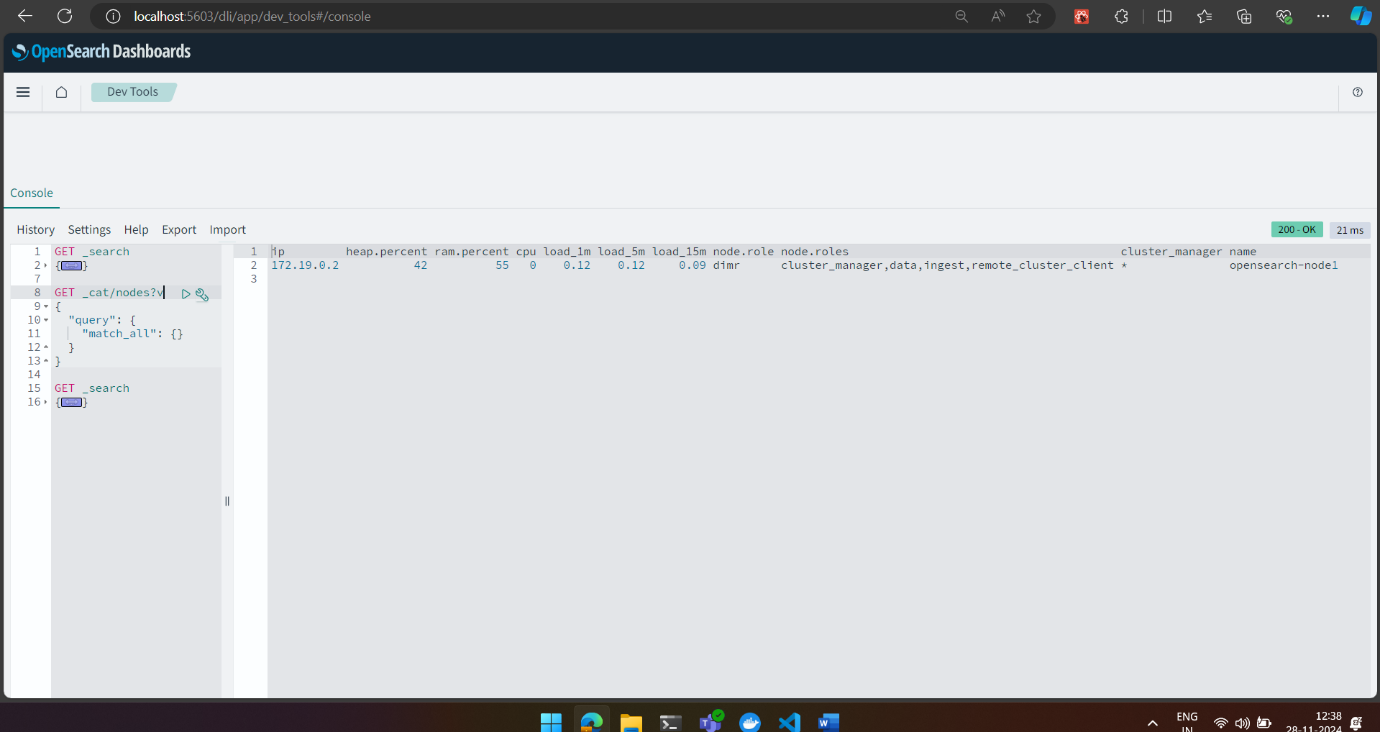


2.GET \_cat/nodes?v :-

cat = view data in human redable format

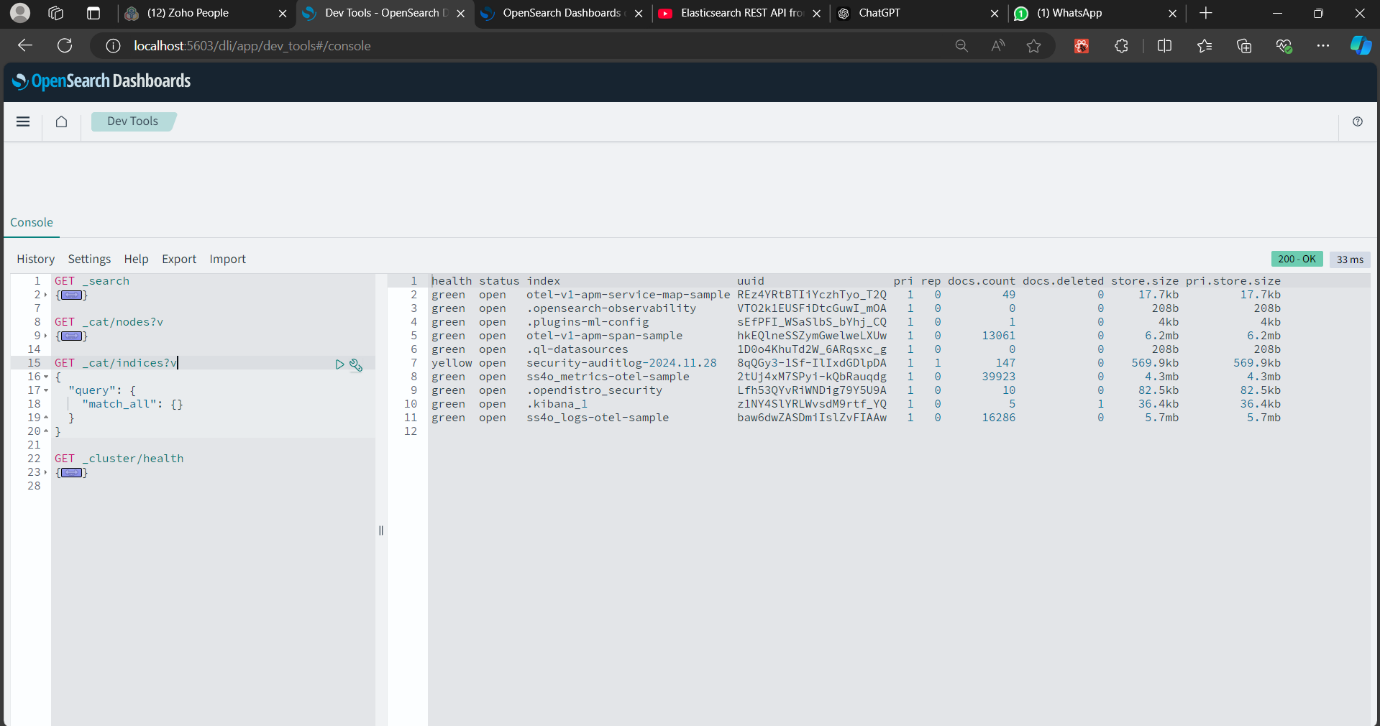
V = gives header

Node = number of nodes



3. \_cat/indices?v

Indices :- details of indices



**Create one employee index**

POST .kibana/\_doc/index-pattern-log-pattern

{

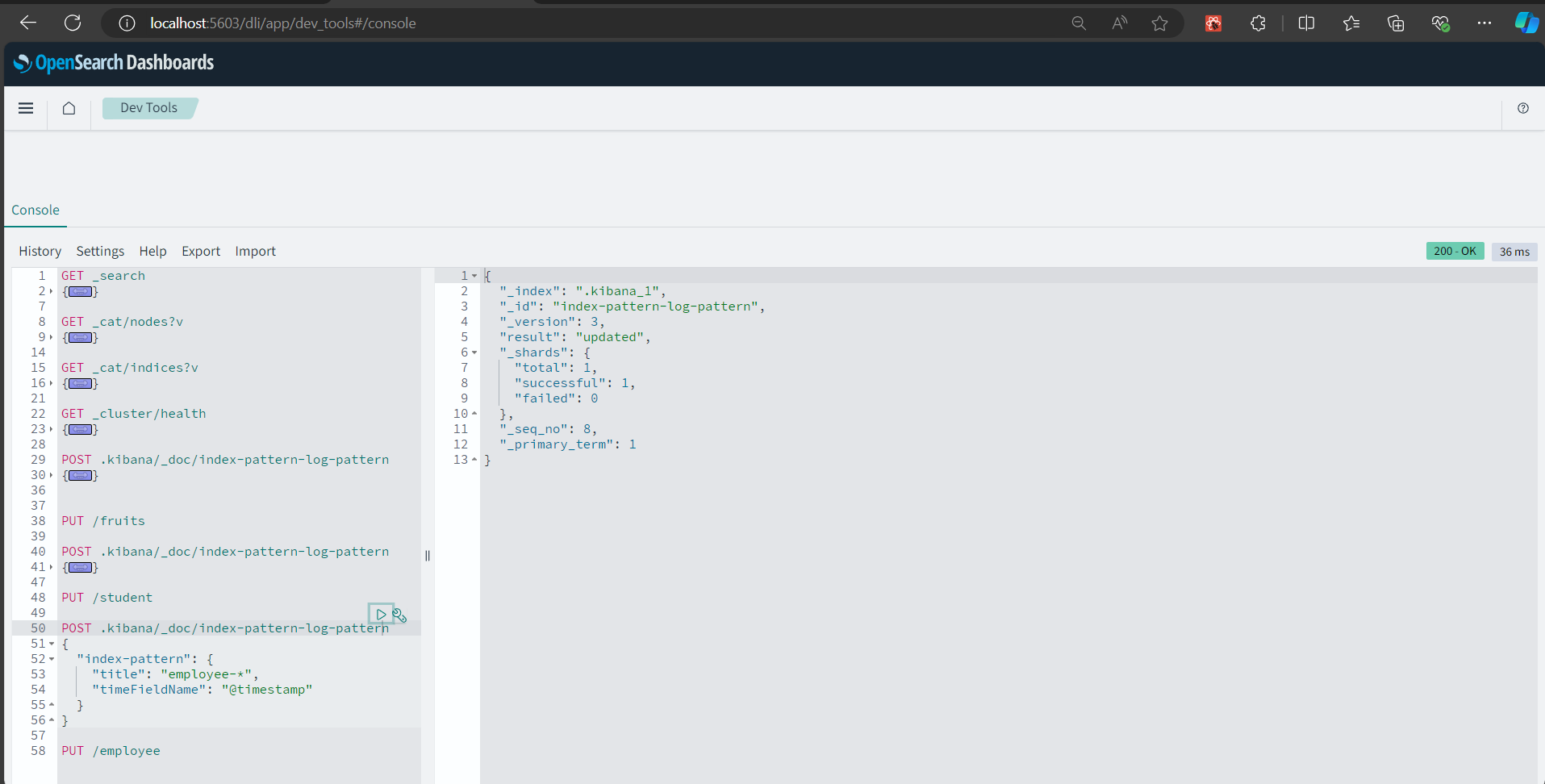
"index-pattern": {

"title": "employee-\*",

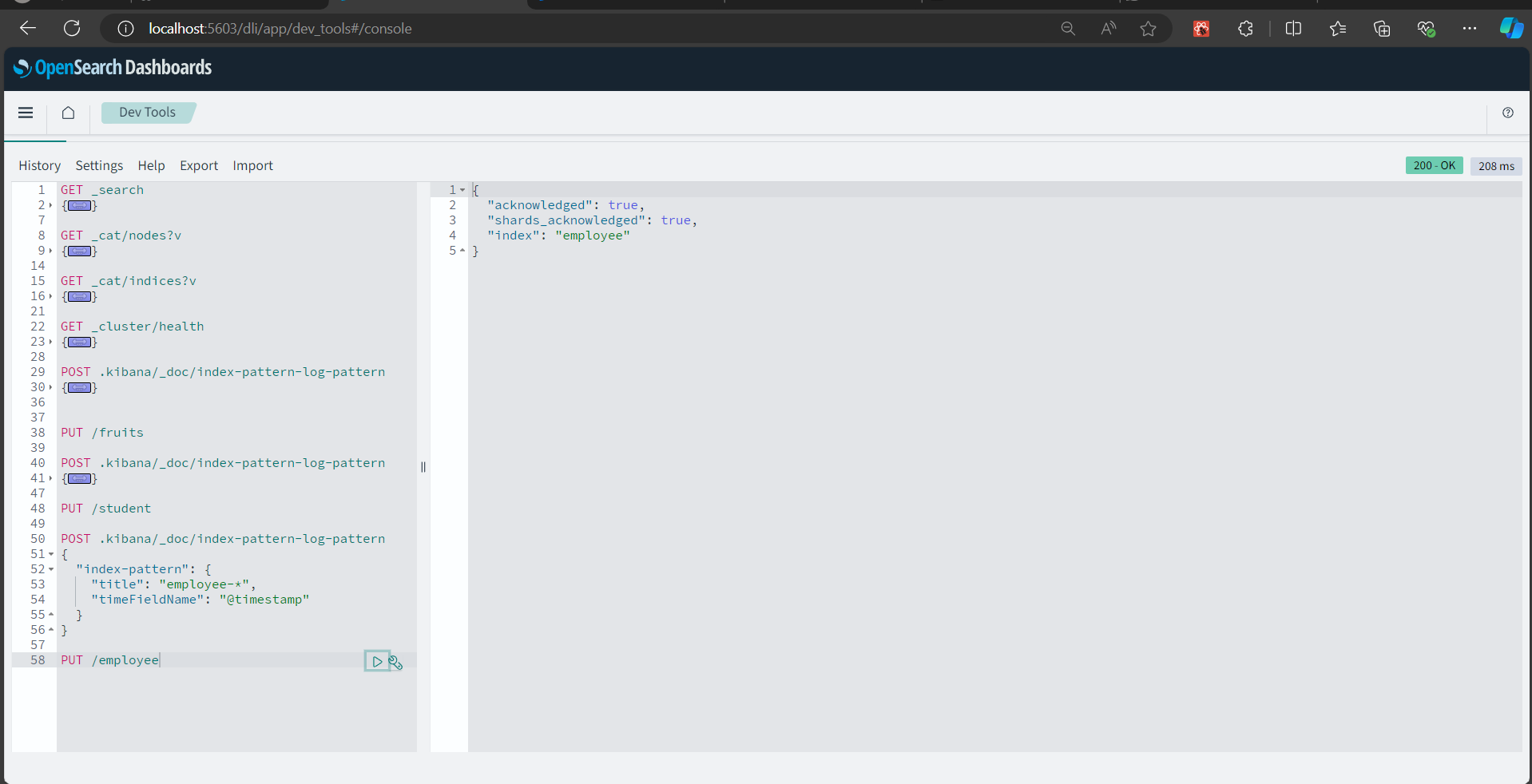
"timeFieldName": "@timestamp"

}

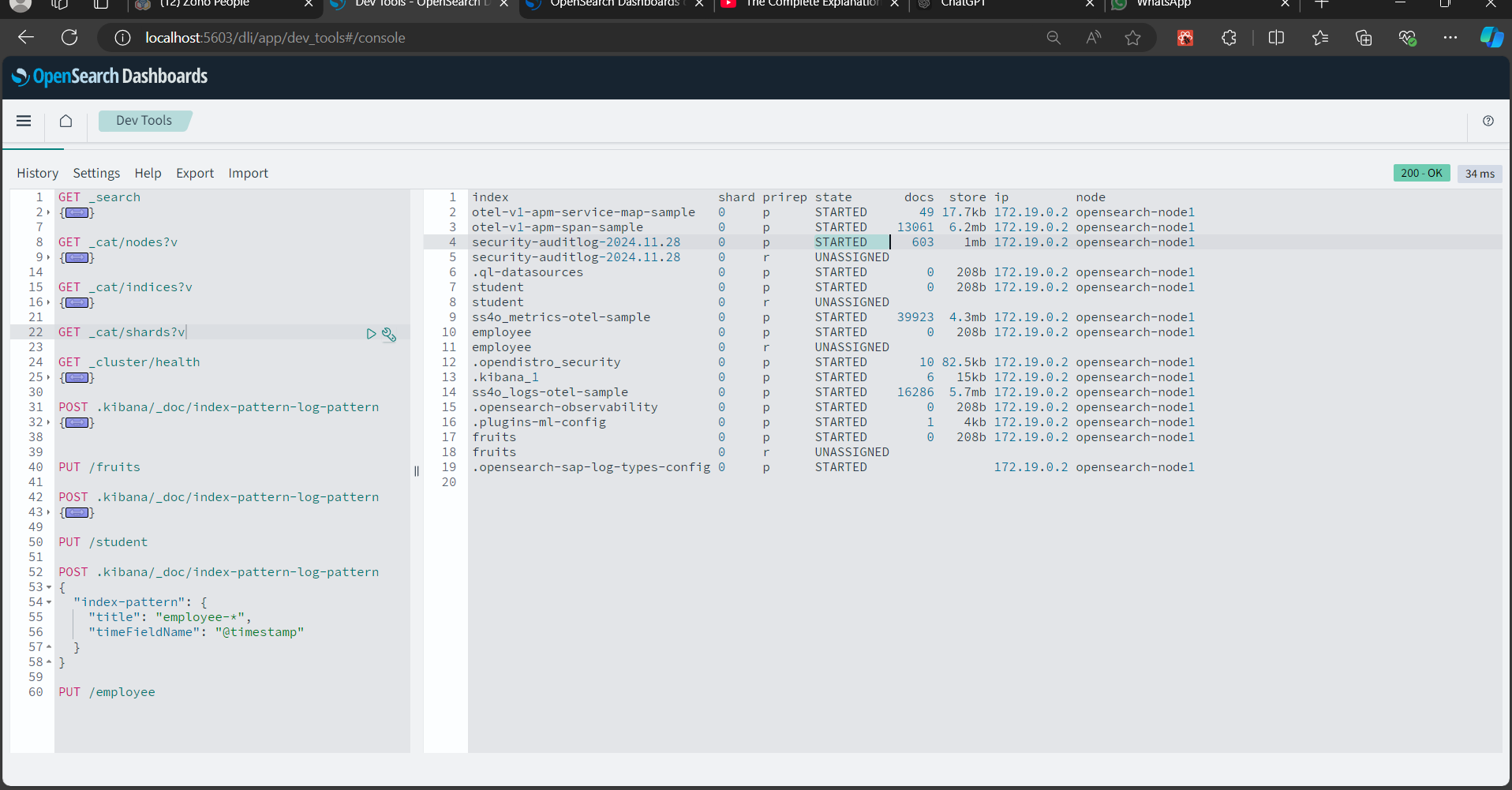
}

****

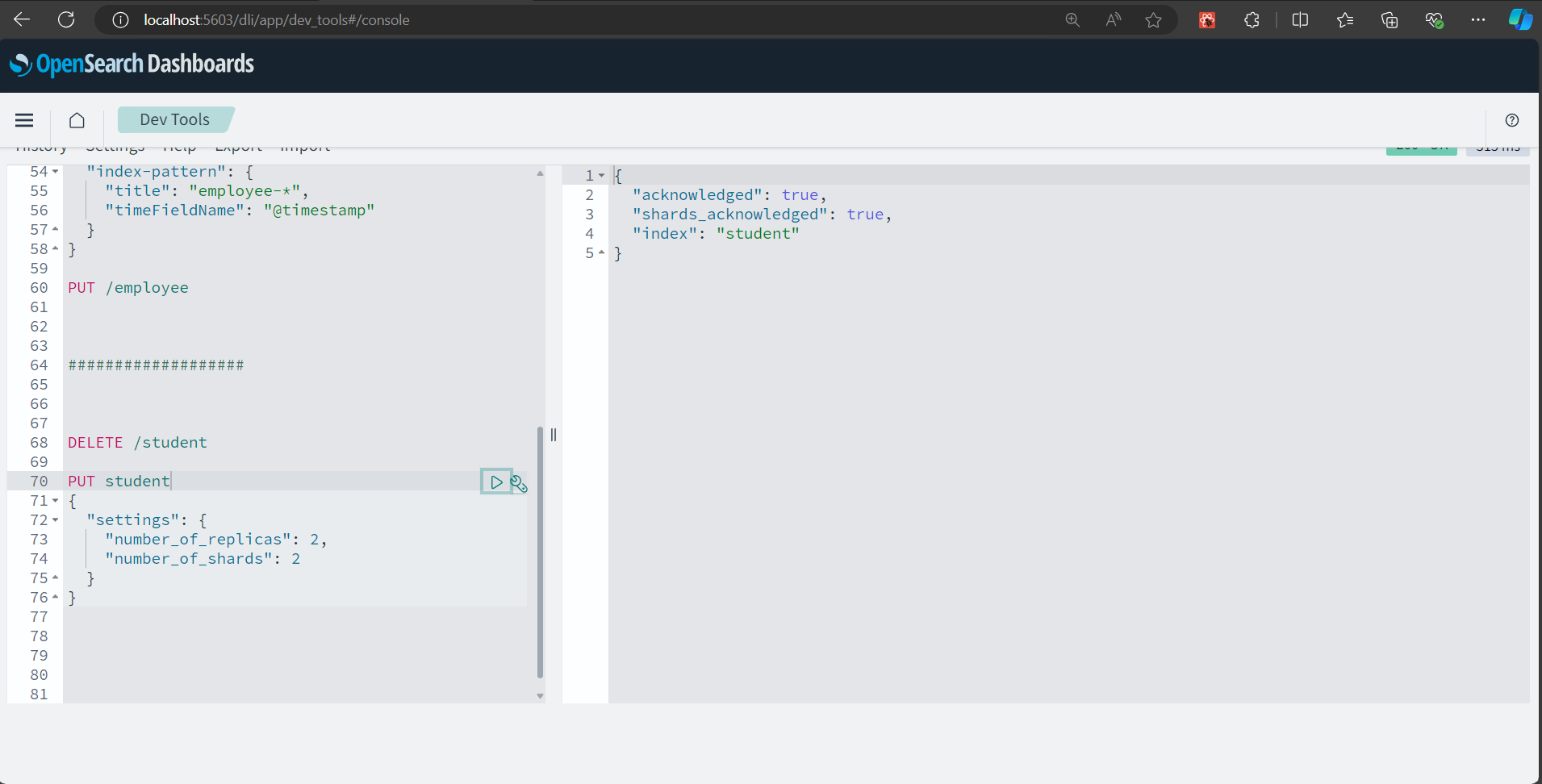
**PUT /employee**

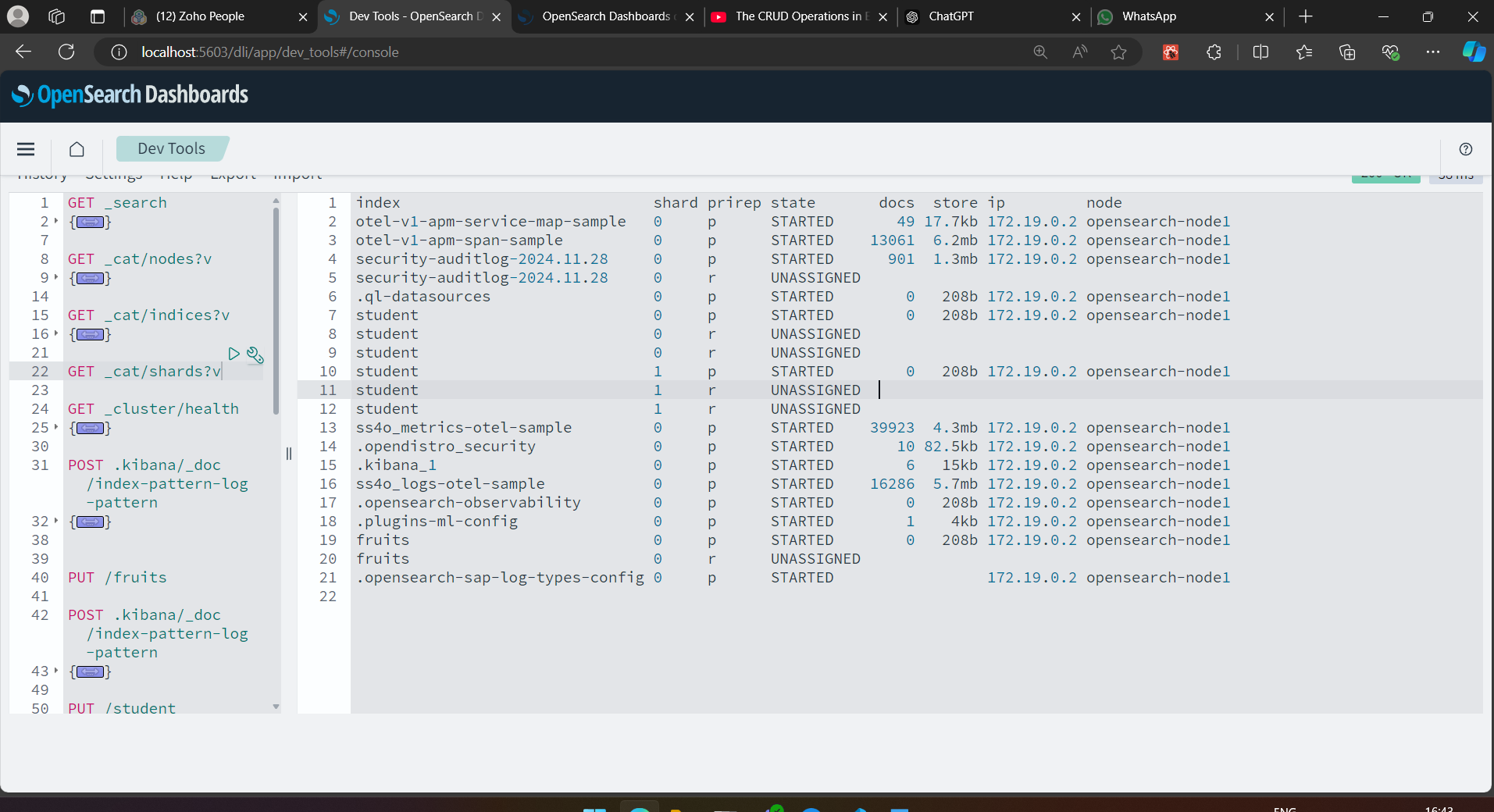
****

GET \_cat/shards?v

****

**Recreate shard and create 2 shard and 2 replicas**

****

****