

1 如何批量导入数据

参考答案

使用_bulk批量导入数据

使用POST方式批量导入数据，数据格式为json，url 编码使用data-binary导入含有index配置的json文件

```
01. [ root@room9pc01 ~] # scp /var/ftp/elk/*.gz 192.168.1.66: /root/
02. [ root@kibana ~] # gzip -d logs.jsonl.gz
03. [ root@kibana ~] # gzip -d accounts.json.gz
04. [ root@kibana ~] # gzip -d shakespeare.json.gz
05. [ root@kibana ~] # curl -X POST "http://192.168.1.61:9200/_bulk" \
06. --data-binary @shakespeare.json
07. [ root@kibana ~] # curl -X POST "http://192.168.1.61:9200/xixi/haha/_bulk" \
08. --data-binary @accounts.json
09. //索引是xixi，类型是haha，必须导入索引和类型，没有索引，要加上
10. [ root@kibana ~] # curl -X POST "http://192.168.1.61:9200/_bulk" \
11. --data-binary @logs.jsonl
```

2 如何实现数据批量查询

参考答案

```
01. [ root@kibana ~] # curl -XGET 'http://192.168.1.61:9200/_mget?pretty' -d '{
02.   "docs":[
03.     {
04.       "_index": "shakespeare",
05.       "_type": "act",
06.       "_id": 0
07.     },
08.     {
09.       "_index": "shakespeare",
10.       "_type": "line",
11.       "_id": 0
12.     },
13.     {
```

```
14.         "_index": "xixi",
15.         "_type": "haha",
16.         "_id": 25
17.     }
18. ]
19. }'
20. {      //查询的结果
21.     "docs": [ {
22.         "_index" : "shakespeare",
23.         "_type" : "act",
24.         "_id" : "O",
25.         "_version" : 1,
26.         "found" : true,
27.         ...
28.         ...
29.         "employer" : "Filody ne",
30.         "email" : "virginiaay ala@filody ne.com",
31.         "city" : "Nicholson",
32.         "state" : "PA "
33.     }
34.     ]
35. }
```

3 map映射的作用及分类是什么

参考答案

作用：这样会让索引建立得更加的细致和完善

分类：静态映射和动态映射

动态映射：自动根据数据进行相应的映射

静态映射：自定义字段映射数据类型

4 Logstash插件有哪些

参考答案

codec类插件、file插件、tcp和udp插件、syslog插件、filter grok插件