

1 简述什么是ELK

参考答案

ELK是一整套解决方案，是三个软件产品的首字母缩写，很多公司都在使用，如：Sina、携程、华为、美团等

ELK分别代表的意思

Elasticsearch：负责日志检索和储存

Logstash：负责日志的收集和分析、处理

Kibana：负责日志的可视化

这三款软件都是开源软件，通常是配合使用，而且又先后归于Elastic.co公司名下，故被简称为ELK

2 ELK可以实现什么功能

参考答案

在海量日志系统的运维中，可用于解决分布式日志数据集中式查询和管理、系统监控，包含系统硬件和应用各个组件的监控、故障排查、安全信息和事件管理、报表功能

3 Elasticsearch主要特点

参考答案

- 1、实时分析
- 2、分布式实时文件存储，并将每一个字段都编入索引
- 3、文档导向，所有的对象全部是文档
- 4、高可用性，易扩展，支持集群（Cluster）、分片和复制（Shards 和 Replicas）
- 5、接口友好，支持JSON

4 如何插入，增加，删除和查询数据

参考答案

增加数据

01. [root@se5 ~] # locale
02. [root@se5 ~] # LANG=en_US.UTF-8 //设置编码

```
03. [ root@se5 ~] # curl -X PUT "http://192.168.1.65:9200/taindex/teacher/1" -d '{
04.   "职业": "诗人",
05.   "名字": "李白",
06.   "称号": "诗仙",
07.   "年代": "唐"
08. }'
09. { "_index": "taindex", "_type": "teacher", "_id": "1", "_version": 2, "_shards": { "total": 2, "s
```

修改数据

```
01. [ root@se5 ~] # curl -X PUT "http://192.168.1.65:9200/taindex/teacher/1" -d '{
02.   "doc": {
03.     "年代": "唐代"
04.   }
05. }'
06. { "_index": "taindex", "_type": "teacher", "_id": "1", "_version": 3, "_shards": { "total": 2, "s
```

查询数据

```
01. [ root@se5 ~] # curl -X GET "http://192.168.1.65:9200/taindex/teacher/3?pretty"
02. {
03.   "_index" : "taindex",
04.   "_type" : "teacher",
05.   "_id" : "3",
06.   "found" : false
07. }
```

删除数据

```
01. [ root@se5 ~] # curl -X DELETE "http://192.168.1.65:9200/taindex/teacher/3?pretty"
02. {
03.   "found" : false,
04.   "_index" : "taindex",
05.   "_type" : "teacher",
06.   "_id" : "3",
07.   "_version" : 1,
```

```
08.     "_shards" : {  
09.         "total" : 2,  
10.         "successful" : 2,  
11.         "failed" : 0  
12.     }  
13. }
```