# 除了文字形式介绍，视频介绍如下

ES SearchUI.wmv

# 1：索引管理

## 1）创建索引

1. elasticsearch服务中创建索引结构（类似与创建表结构）

# 打开：<http://127.0.0.1:5601/app/dev_tools#/console>

执行如下类似命令：

PUT /calllogs

{

"settings": {

"number\_of\_replicas": 1 --副本数1个

, "number\_of\_shards": 5 --5个分片

},

"mappings": { --索引结构，类似与表结构

"properties": {

"SerialNo":{"type": "integer"},

"RequestId":{"type": "keyword"},

"StartDt":{"type": "date"},

"EndDt":{"type": "date"},

"MessageInfo":{"type": "text","analyzer": "standard","search\_analyzer": "standard"},

"MessageResponse":{"type": "text","analyzer": "standard","search\_analyzer": "standard"}

}

}

}

1. kibana中创建对应的索引模式（只是为了匹配到kibana后面功能的需要）

打开：<http://127.0.0.1:5601/app/management/data/index_management/indices>

如下如点击创建索引模式后选择你上面创建的索引，指定时间字段，next,next即可，之后你再到searchui页面就能看到配置好的索引模式可以开始查询 了



1. 写数据到索引中

写数据到索引，目前咱们用的是logstash结构化解析工具先将数据结构化好后再写入es中的，logstash如何接入数据源并写入es中参考：“logstash培训.pptx”

## 2）删除、清空、刷新索引

打开：<http://127.0.0.1:5601/app/management/data/index_management/indices>



# 2：ES SearchUI客户终端配置项

打开：http://127.0.0.1:5601/app/management/kibana/settings

## 1）指定导出字段

找到配置iis的那个searchui文件夹，找到searchui.html

找到58行：const \_id = value.\_id ? value.\_id : '';

将这里的\_id 变为\_source.你需要的字段名称

保存即可，刷新浏览器页面，清缓存即可

## 2）指定可导出的最大行数

上面页面，找到搜索“Number of rows”所在行，默认是500，你可以在这里指定，之后保存即可

## 3）修改默认时间条件

搜索“Hide 'Time' column”，可以关闭searchui 页面的时间过滤项

搜索“Time filter defaults”，可以指定默认搜索的时间范围

## 4）修改显示的索引模式给索引添加的字段范围

搜索” Meta fields”，删除你不想显示的字段

# 3：启动关闭服务

## 1）启动关闭集群所有elasticsearch服务

在window service中找到elasticsearch对应服务操作

## 2）启动关闭logstash解析化工具

目前还没有变为window service，只需在启动的名称窗口中只需ctrl+c，关闭此服务，待下次修改好对应配置文件后再执行相同代码运行

## 3）启动kibana服务

在window service中找到elasticsearch对应服务操作

# 4：快照操作

打开：<http://127.0.0.1:5601/app/management/data/snapshot_restore/snapshots>

1）注册快照仓库

快照仓库的配置需要开发人员来操作，有些客户环境不能做共享目录还做不了快照操作

大致过程：先在每个elasticsearch节点配置path.repo: //172.19.74.26/snapshots指定一个共享目录每个节点都能访问到的路径，之后重启每个节点服务-》点击存储库-》注册存储库-》

2）创建策略

点击创建策略，选择上面创建的存储库，选择你想处理的索引，选择时间策略，之后next,next即可，elasticsearch会根据你的策略自动生成快照备份，同样你也可以对指定快照恢复，需要注意的是：恢复快照，之前的索引名称需要改或者删除才能恢复快照成功，跟数据库备份还原很类似