

大型架构及配置技术

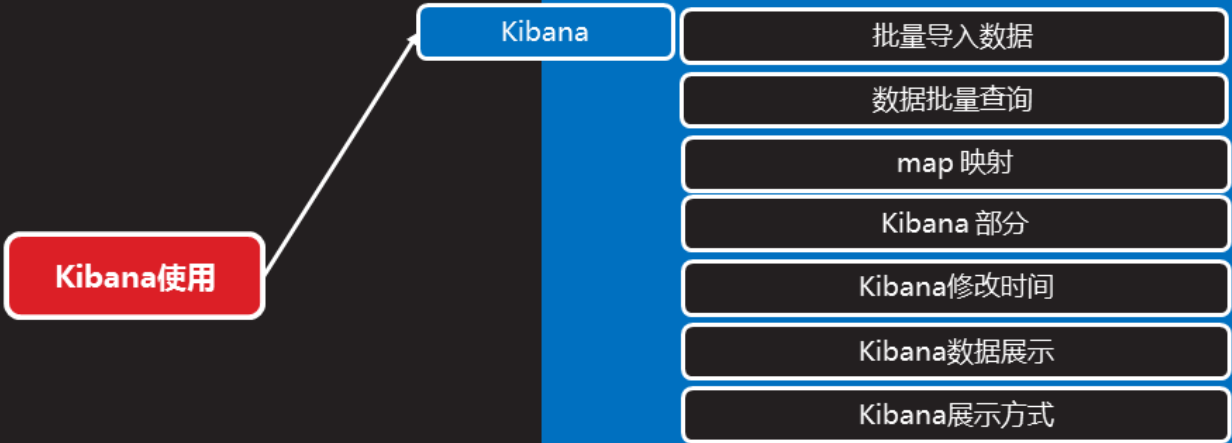
NSD ARCHITECTURE **DAY04**

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	Kibana使用
	10:30 ~ 11:20	
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	Logstash配置 扩展插件
	15:00 ~ 15:50	
	16:10 ~ 17:10	
	17:20 ~ 18:00	总结和答疑



Kibana使用



Kibana

批量导入数据

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

```
# gzip -d logs.jsonl.gz
# curl -XPOST 'http://192.168.4.14:9200/_bulk' --data-binary @logs.jsonl

# gzip -d shakespeare.json.gz
# curl -XPOST 'http://192.168.4.14:9200/_bulk' --data-binary @shakespeare.json
```

批量导入数据（续1）

知识讲解

- 使用_bulk批量导入数据
 - 导入没有index配置的json文件
 - 我们需要在ur里面制定index和type

```
# gzip -d accounts.json.gz
# curl -XPOST
'http://192.168.4.14:9200/accounts/act/_bulk?pretty' --data-binary @accounts.json
```



数据批量查询

知识讲解

- 数据批量查询使用GET

```
# curl -XGET 'http://192.168.4.11:9200/_mget?pretty' -d '{
  "docs":[
    {
      "_index": "accounts",
      "_type": "act",
      "_id": 1
    },
    {
      "_index": "accounts",
      "_type": "act",
      "_id": 2
    }
  ]
}
```



数据批量查询（续1）

- 数据批量查询使用GET

- 续上一页

```
{
  "_index": "shakespeare",
  "_type": "scene",
  "_id": 1
}
```

知识讲解



map 映射

- mapping :
 - 映射：创建索引的时候，可以预先定义字段的类型及相关属性
 - 作用：这样会让索引建立得更加细致和完善
 - 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

知识讲解



案例1：导入数据

1. 批量导入数据并查看

课堂练习



Kibana 部分

- 数据导入以后查看logs是否导入成功

logstash-2015.05.20

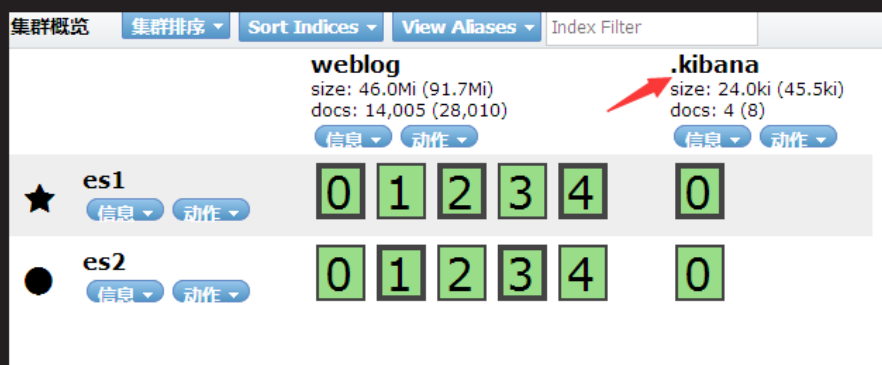
logstash-2015.05.19

logstash-2015.05.18

Kibana 部分（续1）

- 修改Kibana的配置文件后启动Kibana，然后查看ES集群，如果出现.kibana Index表示Kibana与ES集群连接成功

知识讲解



Kibana 部分（续2）

- Kibana里选择日志
 - 支持通配符 *
 - 我们这里选择logstash-*
 - 在下面的Time-field选择@timestamp作为索引
 - 然后点create按钮

知识讲解



Kibana 部分 (续3)

知识讲解

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☒ Index contains time-based events

☐ Use event times to create index names [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

☐ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern `logstash-*` will actually query elasticsearch for the specific matching indices (e.g. `logstash-2015.12.21`) that fall within the current time range.

Time-field name ⓘ refresh fields



Kibana 部分 (续4)

知识讲解



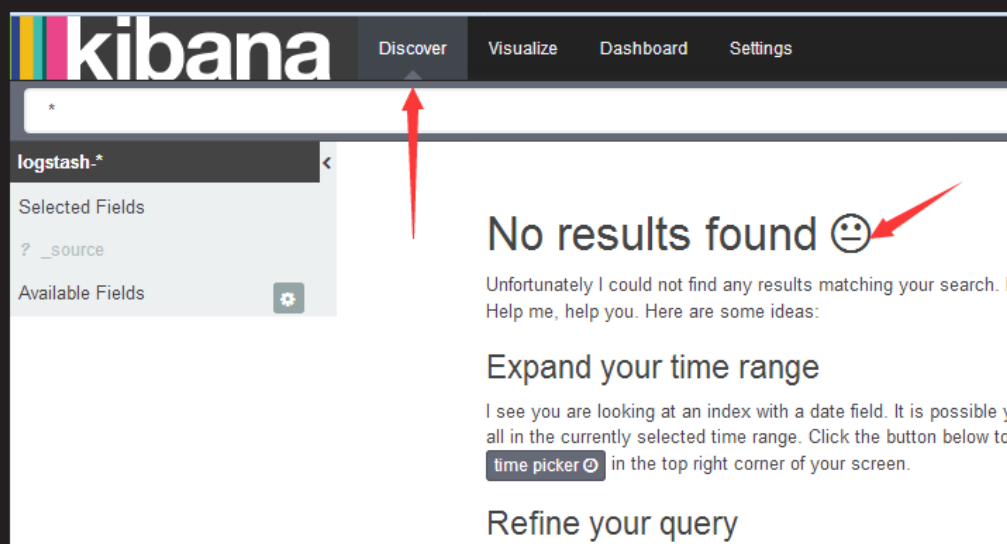
The screenshot shows the Kibana interface with the 'Indices' tab selected. Under 'Index Patterns', the 'logstash-*' pattern is highlighted. The main content area displays the fields for this index pattern. A table lists the fields and their types:

name	type
relatedContent.og:type	string
headings.raw	string
relatedContent.twitter:image	string
utc_time	date
geo.coordinates.lon	number



Kibana 部分（续5）

- 导入成功以后选择Discover



Kibana 部分（续6）

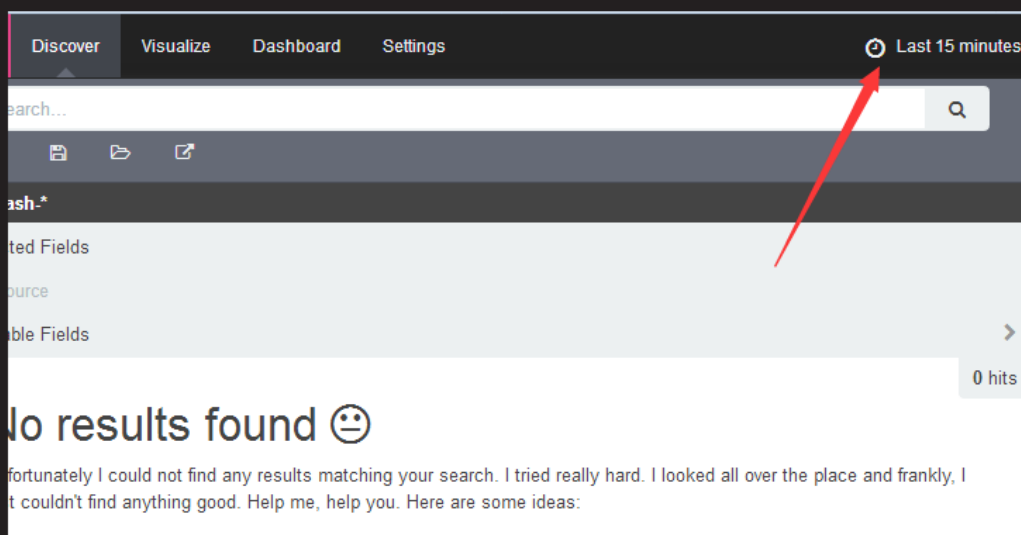
- 这里没有数据的原因是我们导入的日志是2015-05-10至2015-05-20的时间段，默认配置是最近15分钟，在这可以修改一下时间来显示



Kibana修改时间

- 修改时间

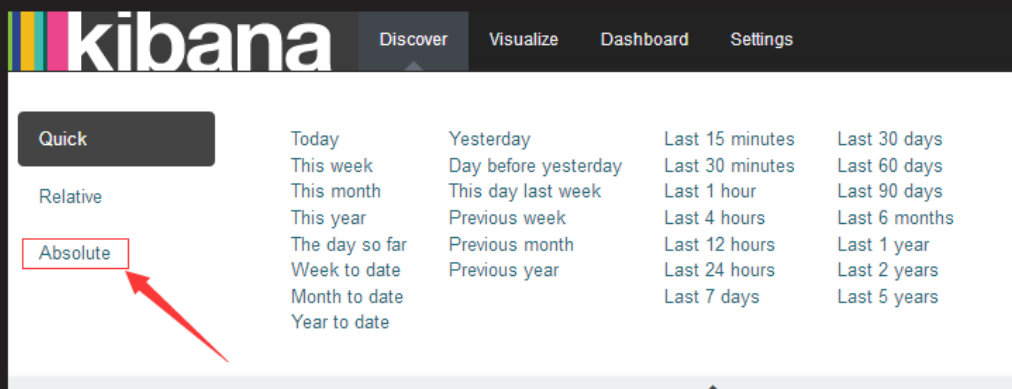
知识讲解



Kibana修改时间（续1）

- 修改时间

知识讲解





Kibana展示方式（续1）

- 饼图与列表，多种维度自定义统计分析

知识讲解

