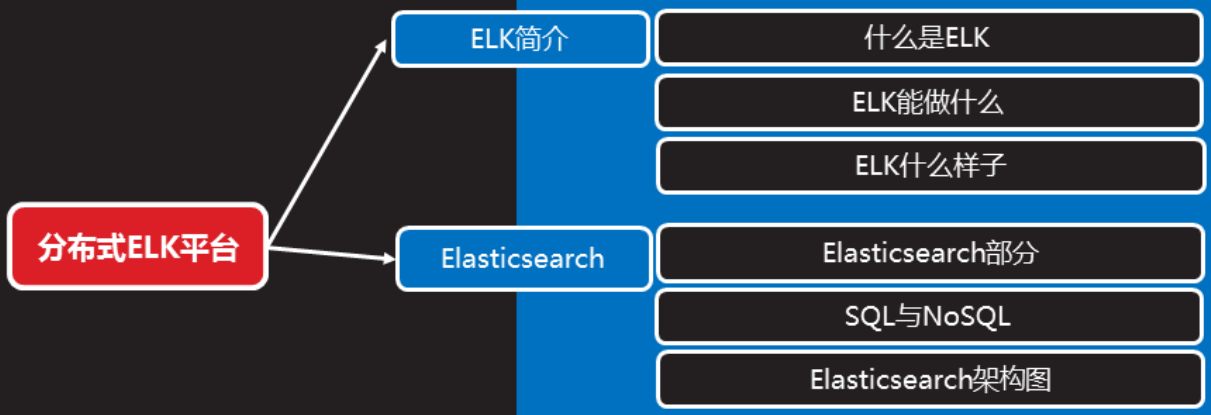
ARCHITECTURE DAY03

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	分布式ELK平台
	10:30 ~ 11:20	ES集群安装
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	扩展插件
	15:00 ~ 15:50	
	16:10 ~ 17:10	Kibana安装
	17:20 ~ 18:00	总结和答疑

分布式ELK平台



ELK简介

什么是ELK

知识讲解

- 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
  - 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

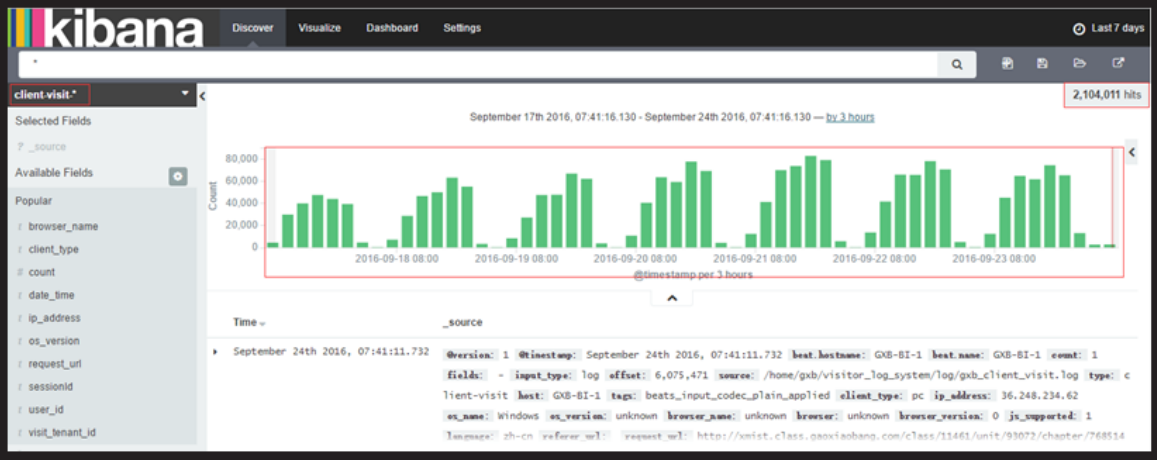
ELK能做什么

知识讲解

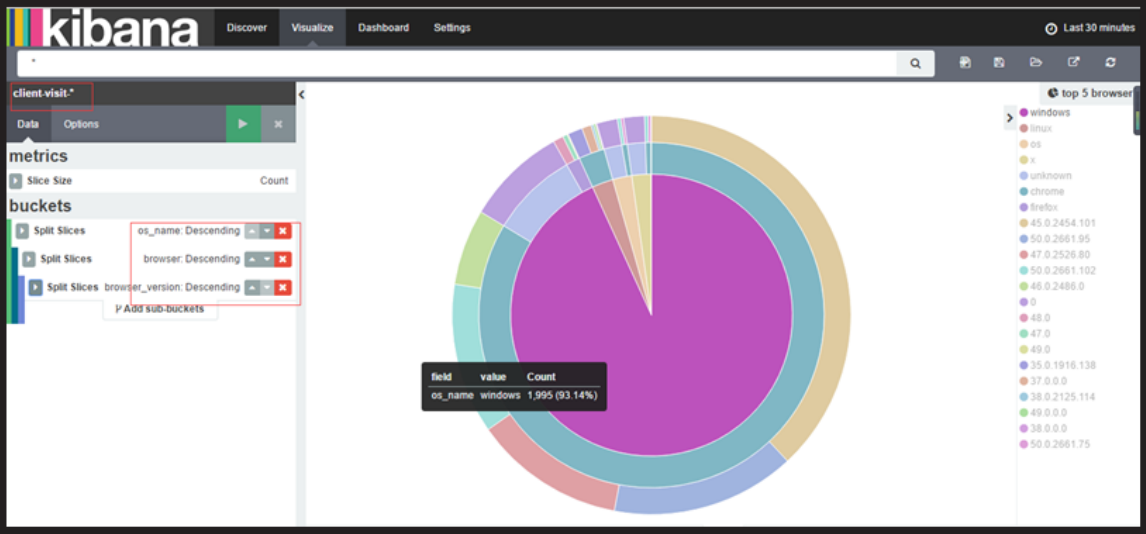
- ELK组件在海量日志系统的运维中，可用于解决
  - 分布式日志数据集中式查询和管理
  - 系统监控，包含系统硬件和应用各个组件的监控
  - 故障排查
  - 安全信息和事件管理
  - 报表功能

ELK什么样子

知识讲解

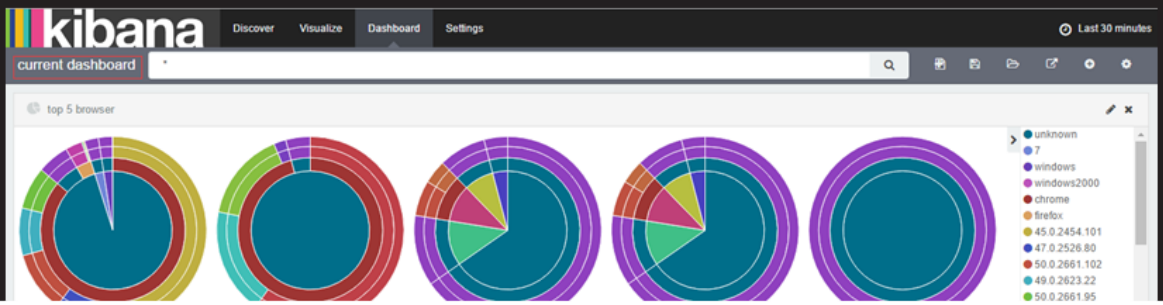


ELK什么样子（续1）



知识讲解

ELK什么样子（续2）



知识讲解

Elasticsearch

Elasticsearch部分

知识讲解

- ElasticSearch是一个基于Lucene的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful API的Web接口
- Elasticsearch是用Java开发的，并作为Apache许可条款下的开放源码发布，是当前流行的企业级搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便

Elasticsearch部分（续1）

Tedu.cn 达内教育

知识讲解

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

Elasticsearch部分（续2）

Tedu.cn 达内教育

知识讲解

- ES没有什么
  - Elasticsearch没有典型意义的事务
  - Elasticsearch是一种面向文档的数据库
  - Elasticsearch没有提供授权和认证特性

Elasticsearch部分（续3）

Tedu.cn 达内教育

知识讲解

- 相关概念
  - Node： 装有一个ES服务器的节点
  - Cluster： 有多个Node组成的集群
  - Document： 一个可被搜索的基础信息单元
  - Index： 拥有相似特征的文档的集合
  - Type： 一个索引中可以定义一种或多种类型
  - Filed： 是ES的最小单位，相当于数据的某一列
  - Shards： 索引的分片，每一个分片就是一个Shard
  - Replicas： 索引的拷贝

SQL与NoSQL

Tedu.cn 达内教育

知识讲解

- ES与关系型数据库的对比
  - 在ES中，文档归属于一种 类型（type），而这些类型存在于索引（index）中，类比传统关系型数据库
  - DB -> Databases -> Tables -> Rows -> Columns
  - 关系型 数据库 表 行 列
  - ES -> Indices -> Types -> Documents -> Fields
  - ES 索引 类型 文档 域（字段）

SQL与NoSQL（续1）

Tedu.cn 达内教育

知识讲解

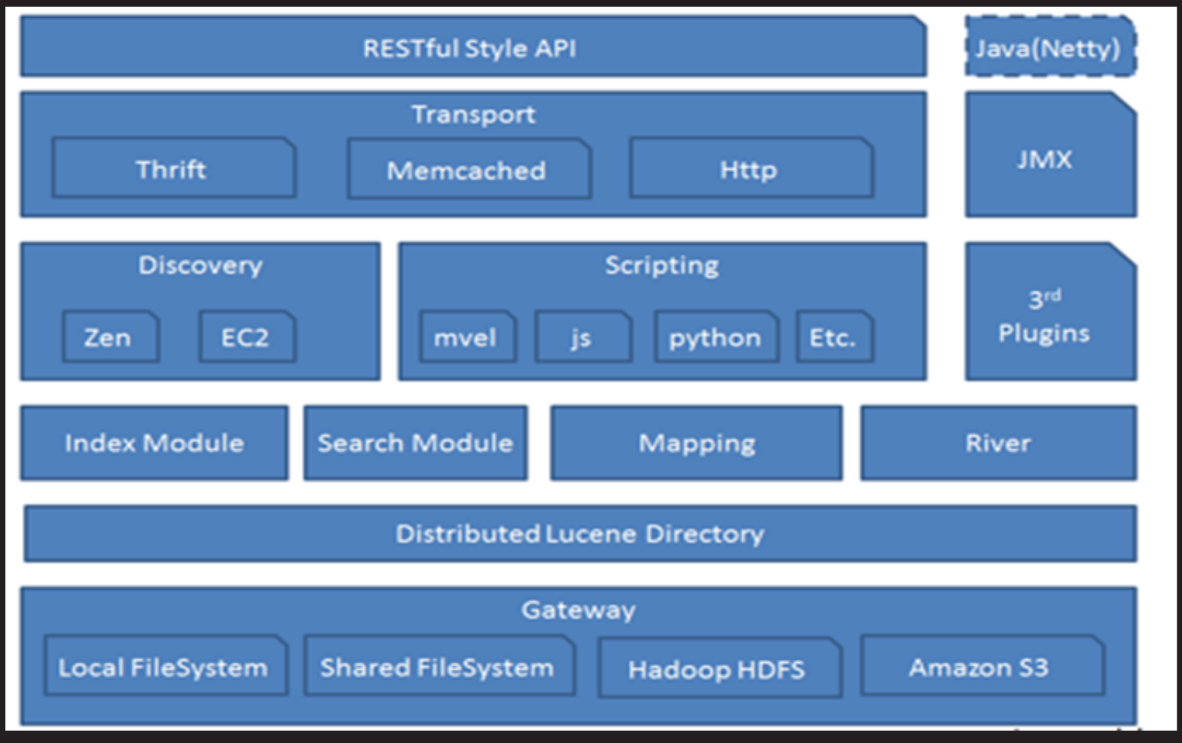
- ES与关系型数据库的对比

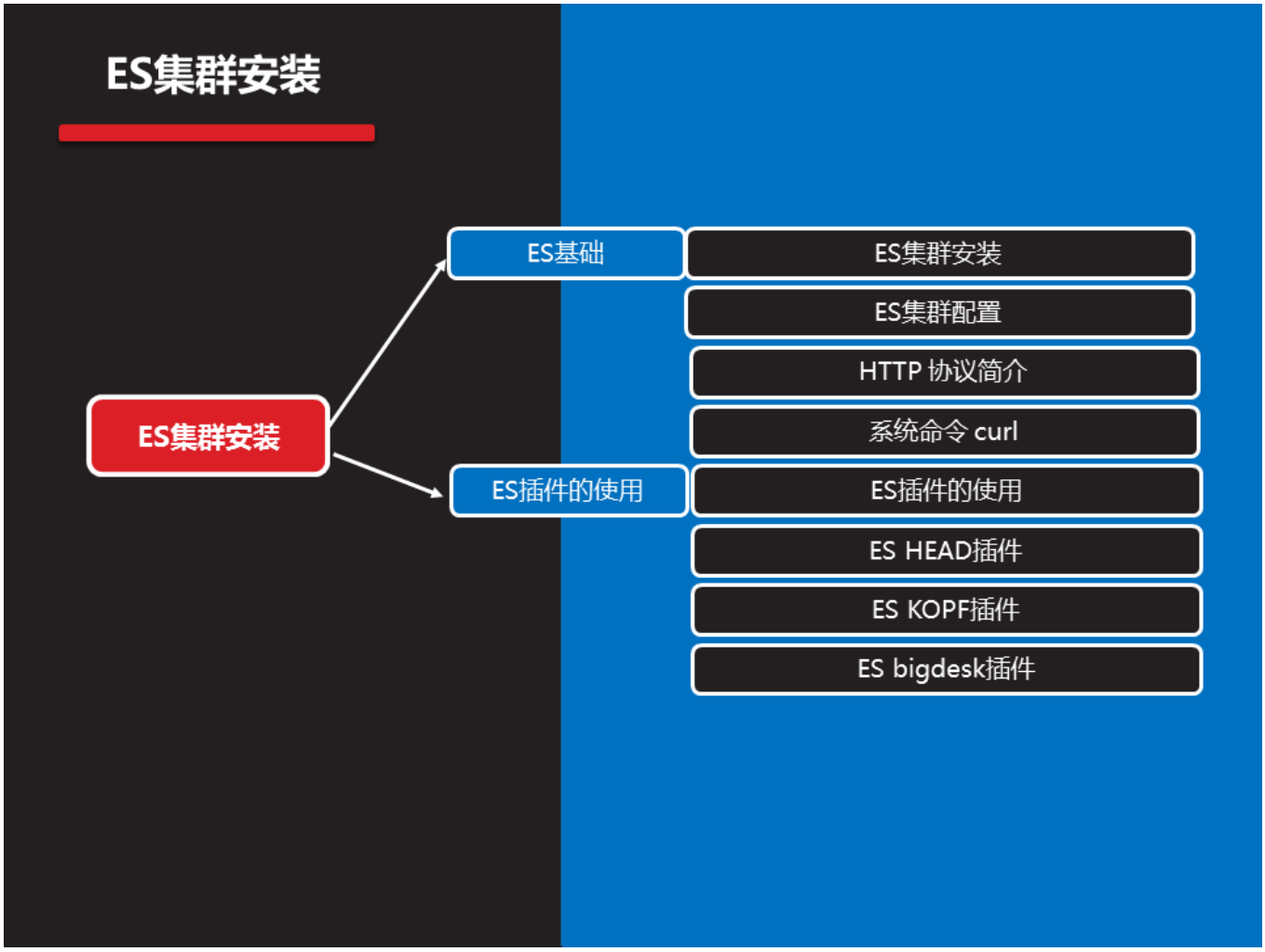
Relational database	Elasticsearch
Database	Index
Table	Type
Row	Document
Column	Field
Schema	Mapping
Index	Everything is indexed
SQL	Query DSL
SELECT * FROM table...	GET http://...
UPDATE table SET	PUT http://...

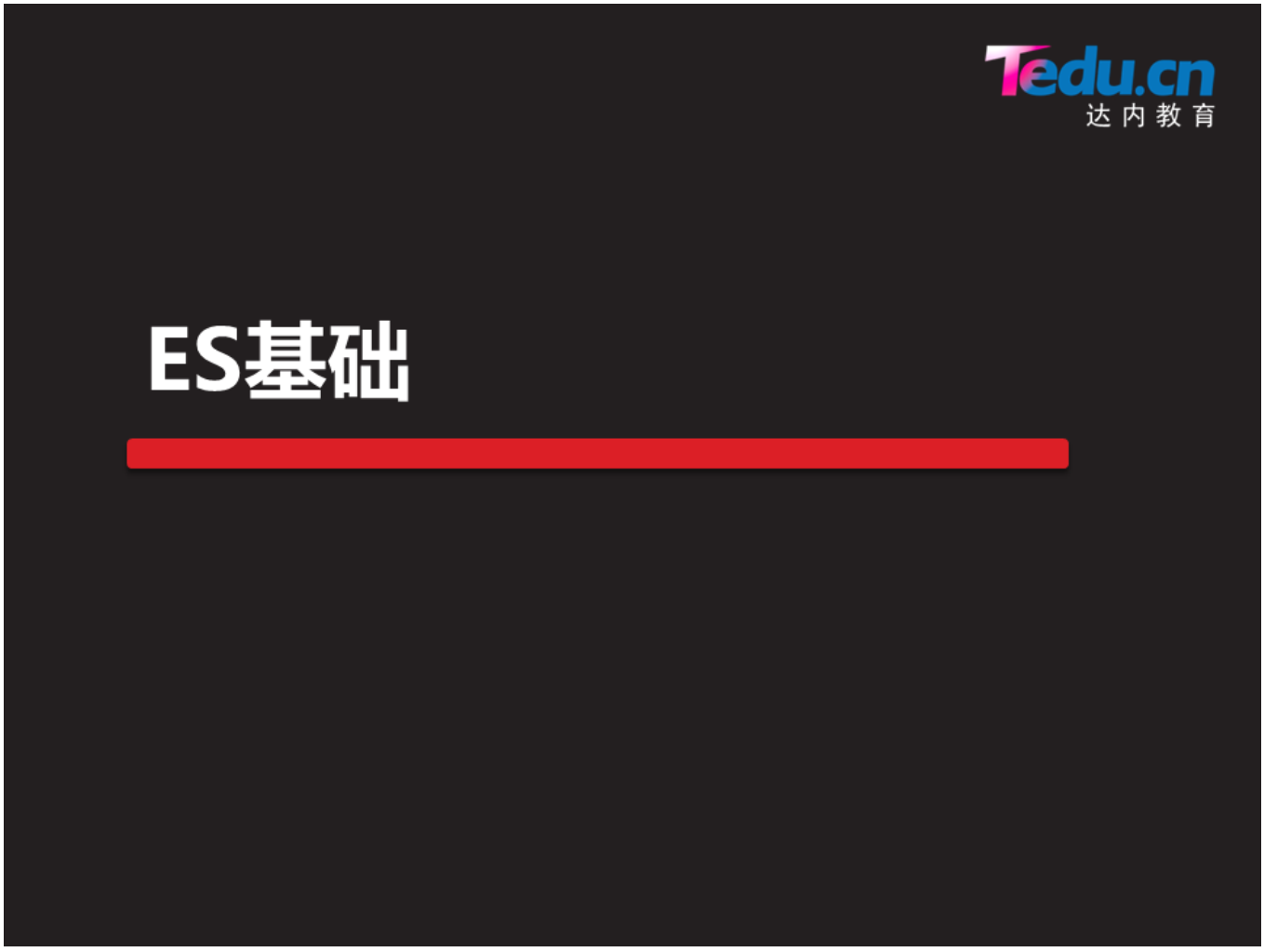
Elasticsearch架构图

Tedu.cn 达内教育

知识讲解




ES集群安装
ES集群安装
ES基础
ES插件的使用
ES集群安装
ES集群配置
HTTP 协议简介
系统命令 curl
ES插件的使用
ES HEAD插件
ES KOPF插件
ES bigdesk插件


Tedu.cn
达内教育
ES基础

ES集群安装

Tedu.cn 达内教育

知识讲解

- 安装第一台ES服务器
  - 设置主机名称和ip对应关系
  - 解决依赖关系
  - 安装软件包
  - 修改配置文件
  - 启动服务
  - 检查服务

ES集群安装（续2）

Tedu.cn 达内教育

知识讲解

- 安装ES

  rpm -ivh elasticsearch-2.3.4-1.noarch

- 修改配置文件
  - elasticsearch.yml

    network.host: 0.0.0.0

ES集群安装（续3）

Tedu.cn 达内教育

知识讲解

- 启动服务
  - 启动服务并设开机自启

    systemctl enable elasticsearch

    systemctl start elasticsearch

  - 验证：

    netstat –ltunp

  - 能够看到9200，9300被监听

ES集群安装（续4）

知识讲解

- 通过浏览器或curl访问9200端口

```
curl http://192.168.4.11:9200/
{
  "name" : "node1",
  "cluster_name" : "my-es",
  "version" : {
    "number" : "2.3.4",
    ..... ..... .....
    "build_snapshot" : false,
    "lucene_version" : "5.5.0"
  },
  "tagline" : "You Know, for Search"
}
```

案例1：ES集群安装

课堂练习

1. 准备1台虚拟机
2. 部署elasticsearch第一个节点
3. 访问9200端口查看是否安装成功

ES集群配置

Tedu.cn 达内教育

知识讲解

- ES集群配置
  - ES集群配置也很简单，只需要对配置文件做少量的修改即可，其他步骤和单机完全一致
  - ES集群配置文件

```
cluster.name: my-es
node.name: node1
network.host: 0.0.0.0
discovery.zen.ping.unicast.hosts: ["node1", "node2", "node3"]
```