# 第1章 课程介绍

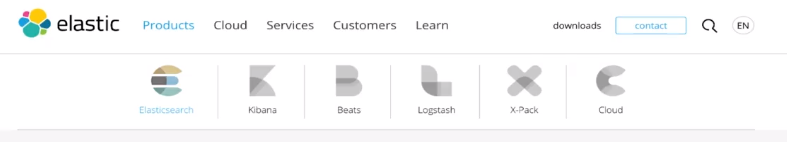


# 第2章 Elastic Search和Kibana入门

## 2-1 Elasticsearch安装与演示



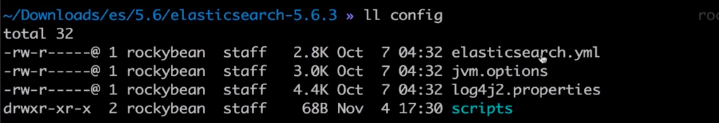


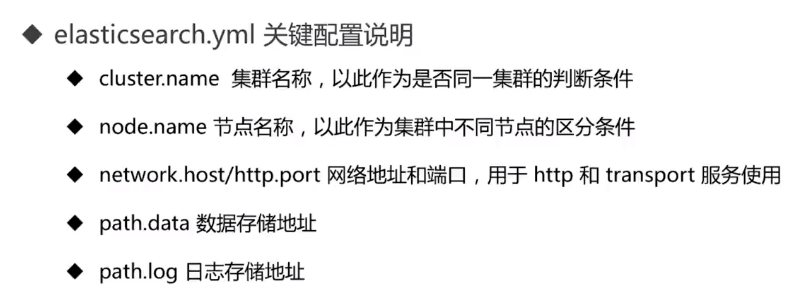


下载zip包或者tar包解压安装，访问127.0.0.1:9200

## 2-2 Elasticsearch配置详解







Node.name 不指定随机指定一个

cluster.name: bigdata\_es

node.name: ${HOSTNAME}

node.master: true

node.data: true

path.data: /export/elasticsearch/data

path.logs: /export/elasticsearch/logs

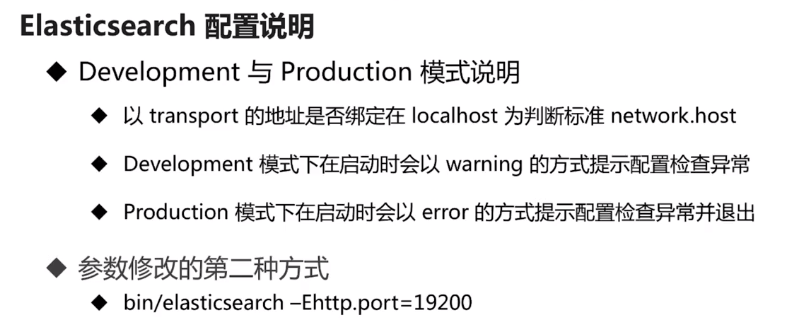
network.host: ${HOSTNAME}

discovery.zen.minimum\_master\_nodes: 1

discovery.zen.ping.unicast.hosts: [10.15.40.44]

xpack.security.enabled: false

配置文件和命令行两个方式修改



## 2-3 Elasticsearch本地快速搭建集群

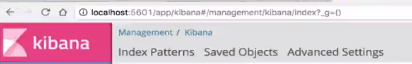


## 2-4 Kibana 安装与演示

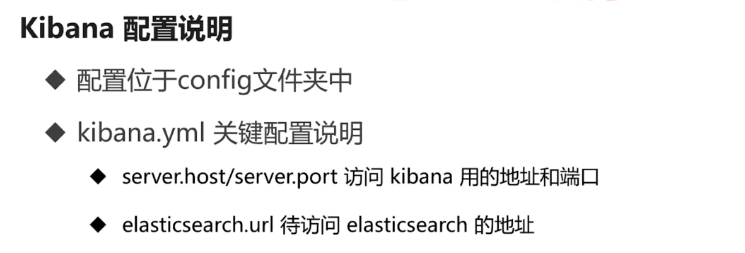
官网下载安装，根据不同平台（js开发的）

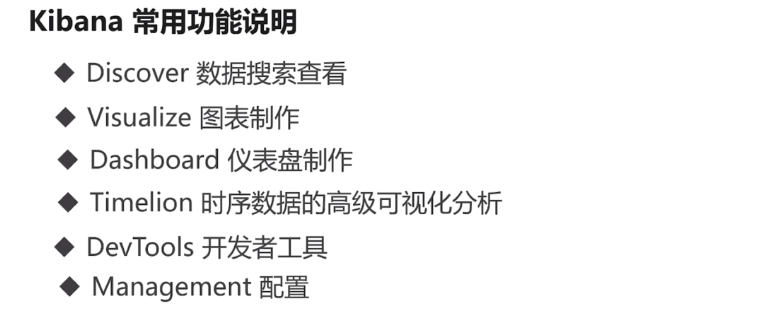
修改配置



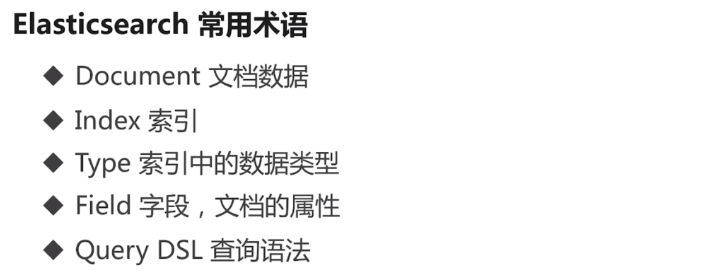


## 2-5 Kibana 配置详解

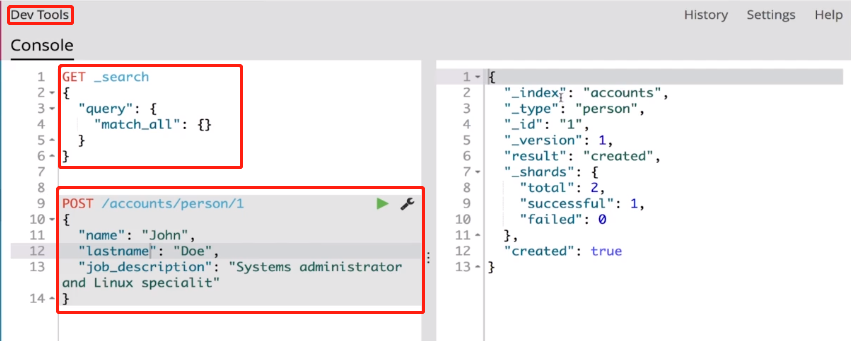




## 2-6 Elasticsearch 术语介绍与CRUD实际操作



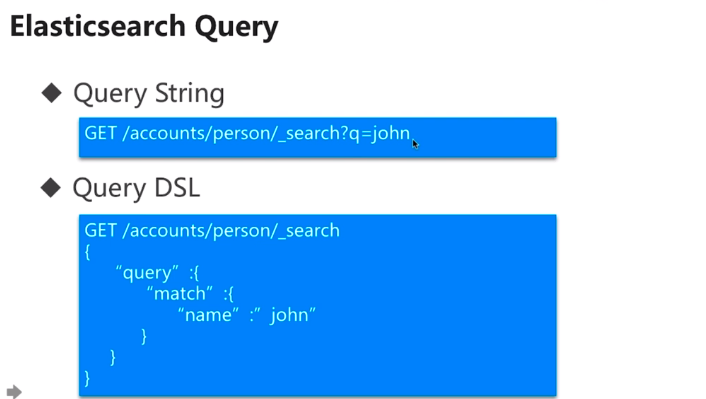




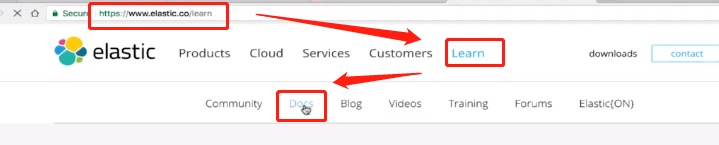
## 2-7 Elasticsearch 查询简介

两种方式：

1. String : url 参数中指定
2. DSL



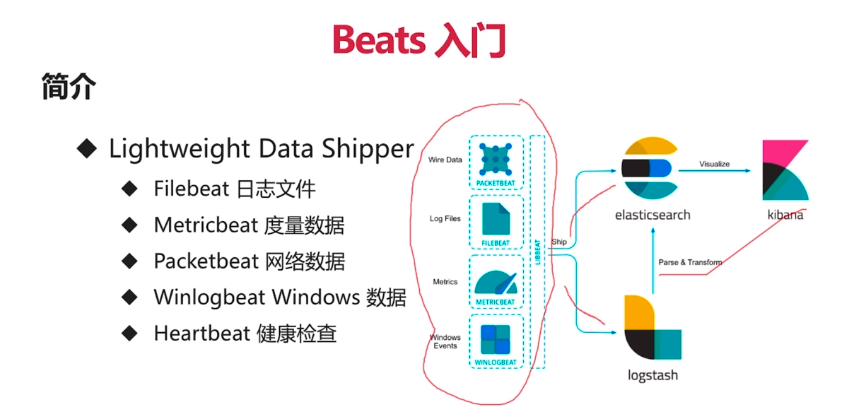
更多查询语法请参见官网：[www.elastic.co](http://www.elastic.co)



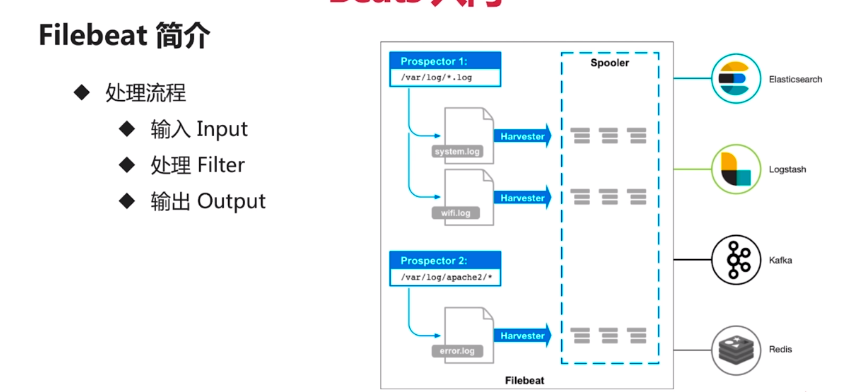
# 第3章 Beats、Filebea入门

## 3-1 Beats 入门

轻量级数据传送者。



## 3-2 Filebeat 简介



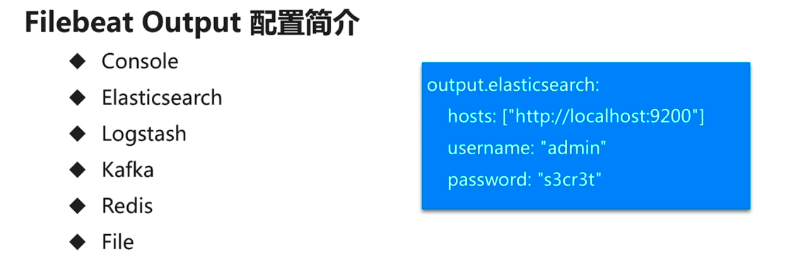
Prospector： 观察者

Harvester: 收割者

一个Filebeat可以有多个Prospector，一个Harvester针对一个日志文件

## 3-3 Filebeat 配置简介

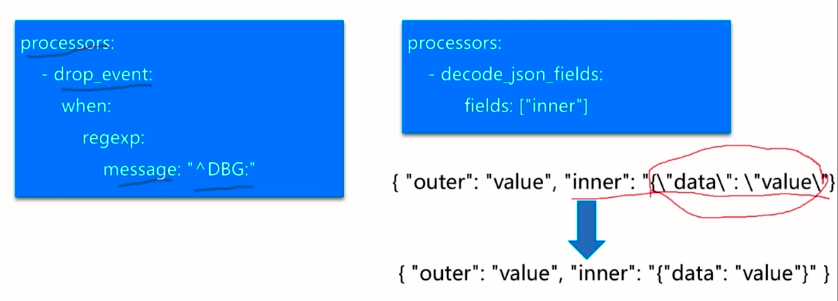




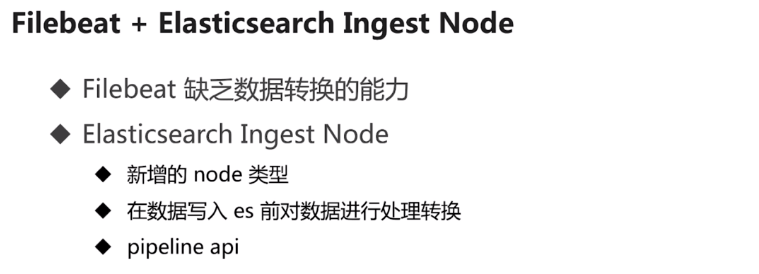
内容处理：处理能力较弱

通过关键字过滤行，json处理等。





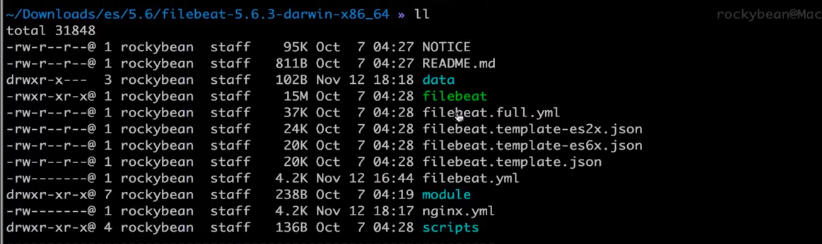
## 3-4 Filebeat 高级使用简介

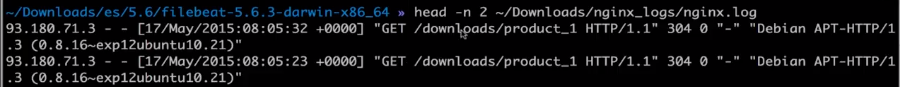




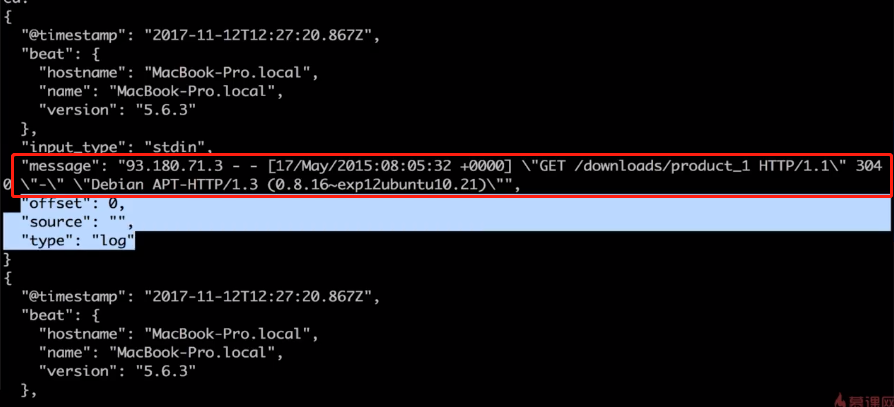
3-5 Filebeat 演示

官网下载beats---filebeat---解压配置 分平台

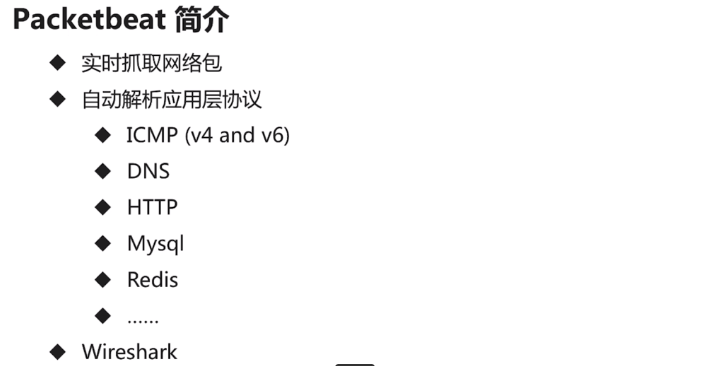




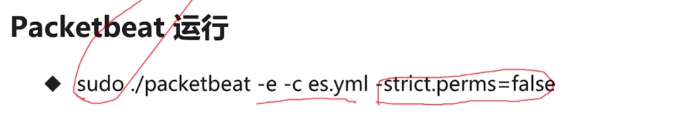




## 3-5 Packetbeat 简介

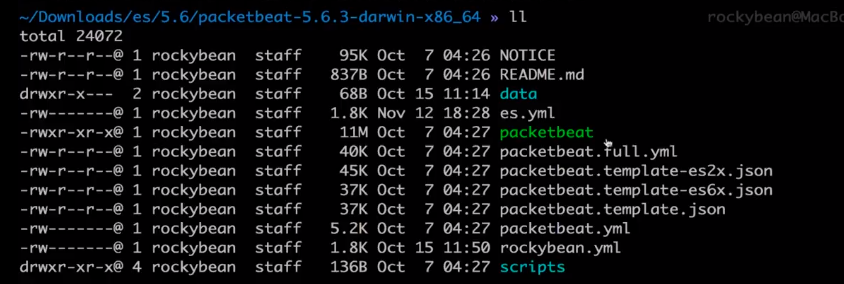




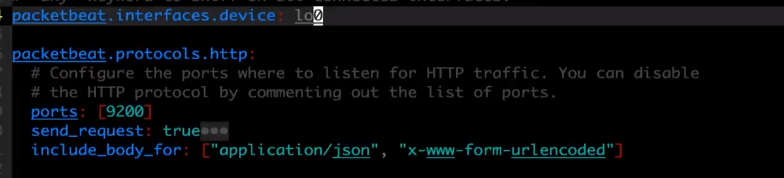


## 3-6 Packetbeat 演示

官网下载解压安装



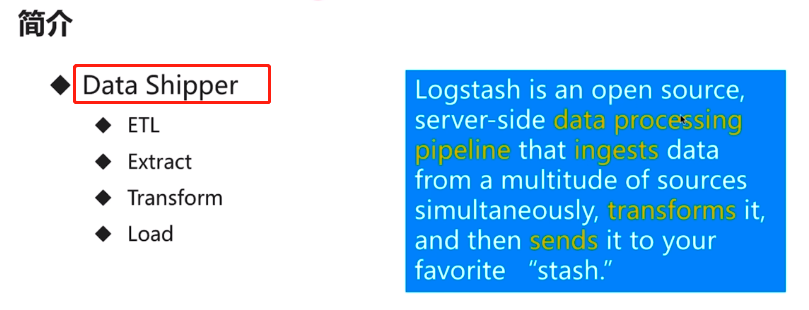
es.yml



# 第4章 Logstash入门

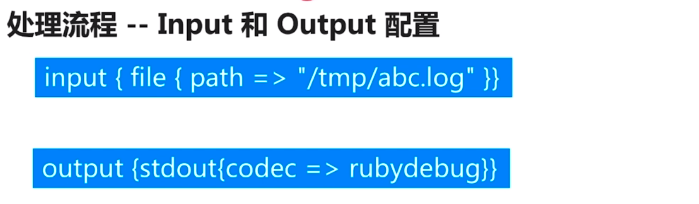
## 4-1 Logstash 简介

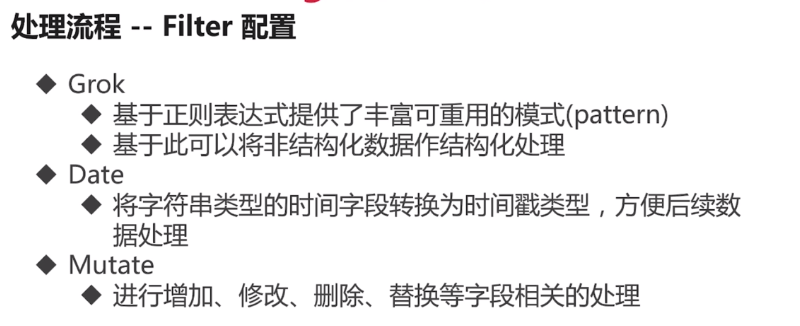
Logstash 不是轻量级，比Beats 占用更多资源，功能更强大

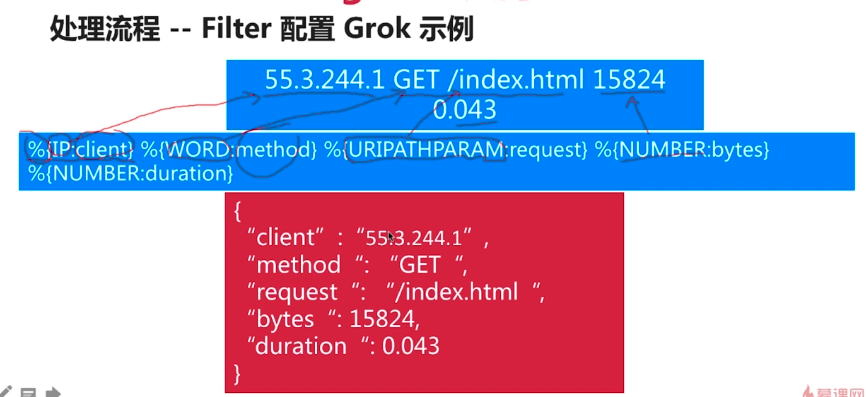




## 4-2 Logstash 配置简介





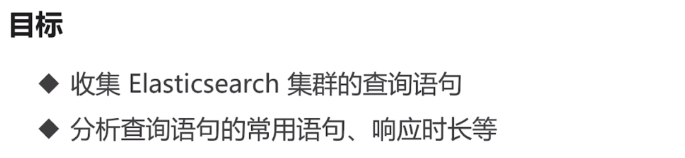


## 4-3 Logstash 演示

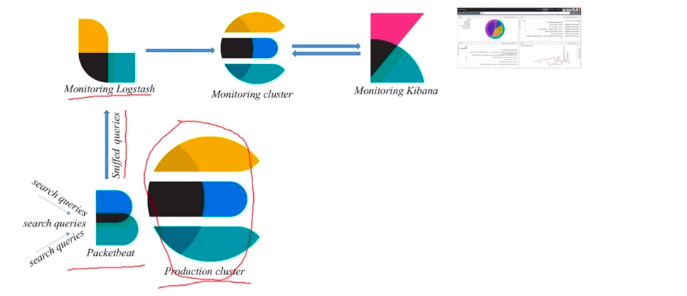
官网下载---基于jvm



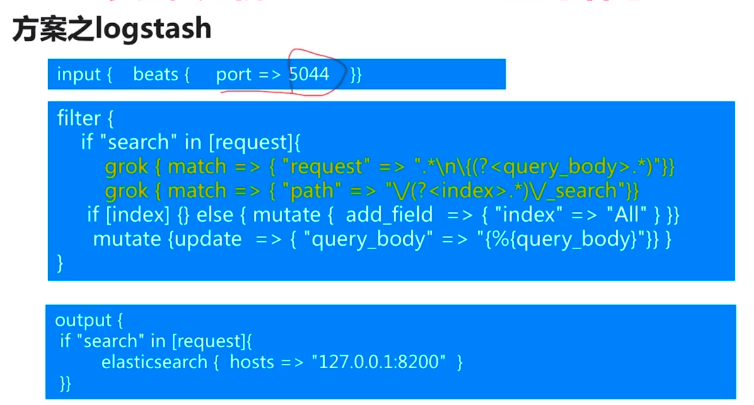
# 第5章 案例实战













启动生产环境es, kibana

启动监控集群es，kibana

启动packetbeat

Packetbeat 对于长连接抓包有些延迟

