Resources available

Learning ElasticSearch 5.0

Ethan Anthony

Packt Udemy

Learning ElasticSearch 5.0

Ethan Anthony

Video 1.1

The Course Overview

About Me

- I am a San Francisco-based software developer, specializing in distributed data-centric technologies
- I am the Founder of Xresults
- I have over 10 years of experience in cloud based technologies such as Amazon web services and OpenStack, as well as Hadoop, Mahout, Spark, and Elastic Search
- I began using ElasticSearch in 2012 and has since delivered solutions based on the Elastic Stack to a broad range of clientele
- I have consulted globally with firms in a cross-section of industry verticals, from the US to the Fareast

In this Video, we are going to take a look at...

- What is ElasticSearch?
- Installation
- Goal of ElasticSearch
- What's new in version 5.0

elasticsearch

Apache Lucene

Distributed

Analytics Engine

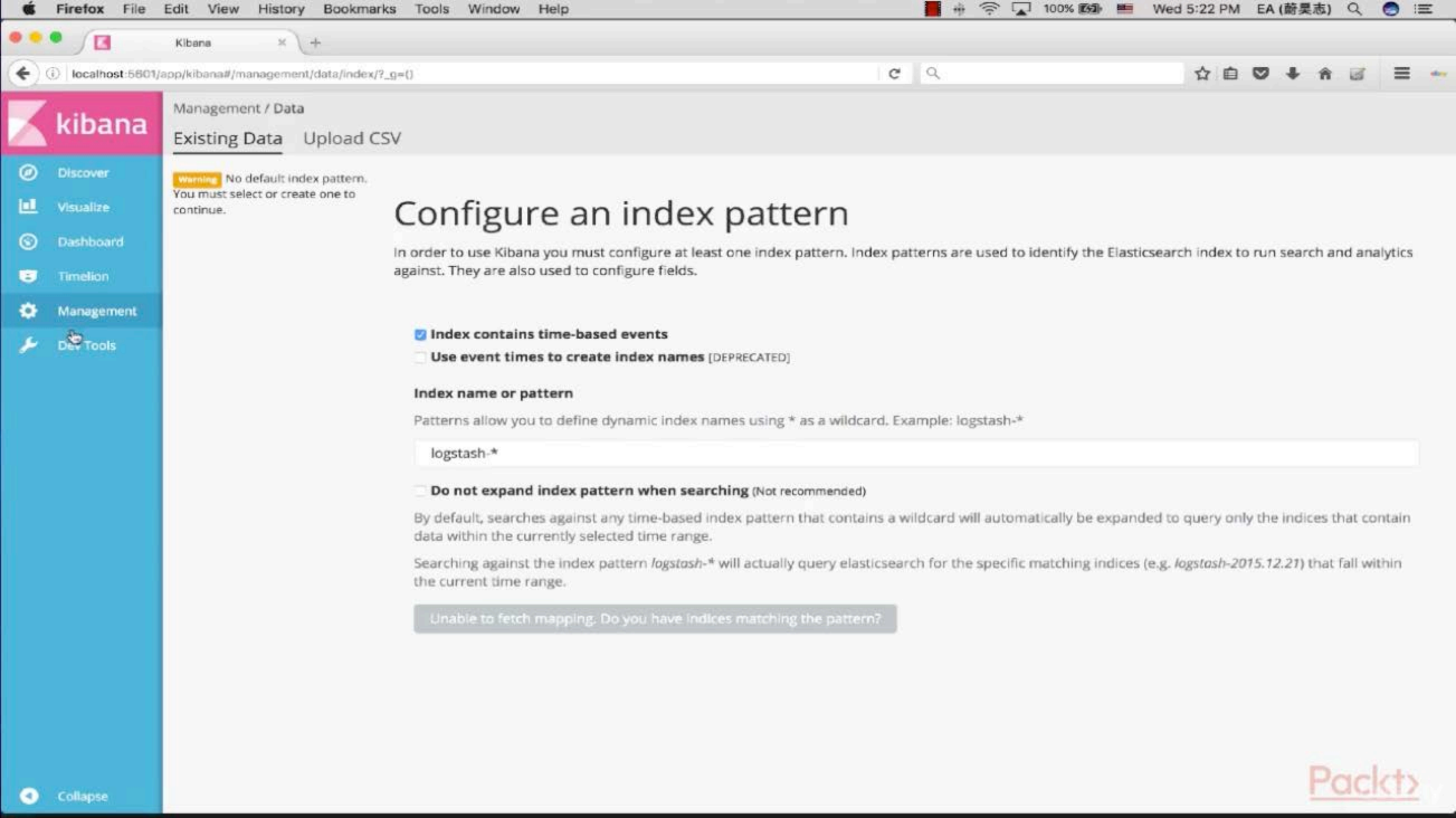
Horizontal Document Store

Lightning fast search

Open Source (free)

Easy to setup

Language agnostic

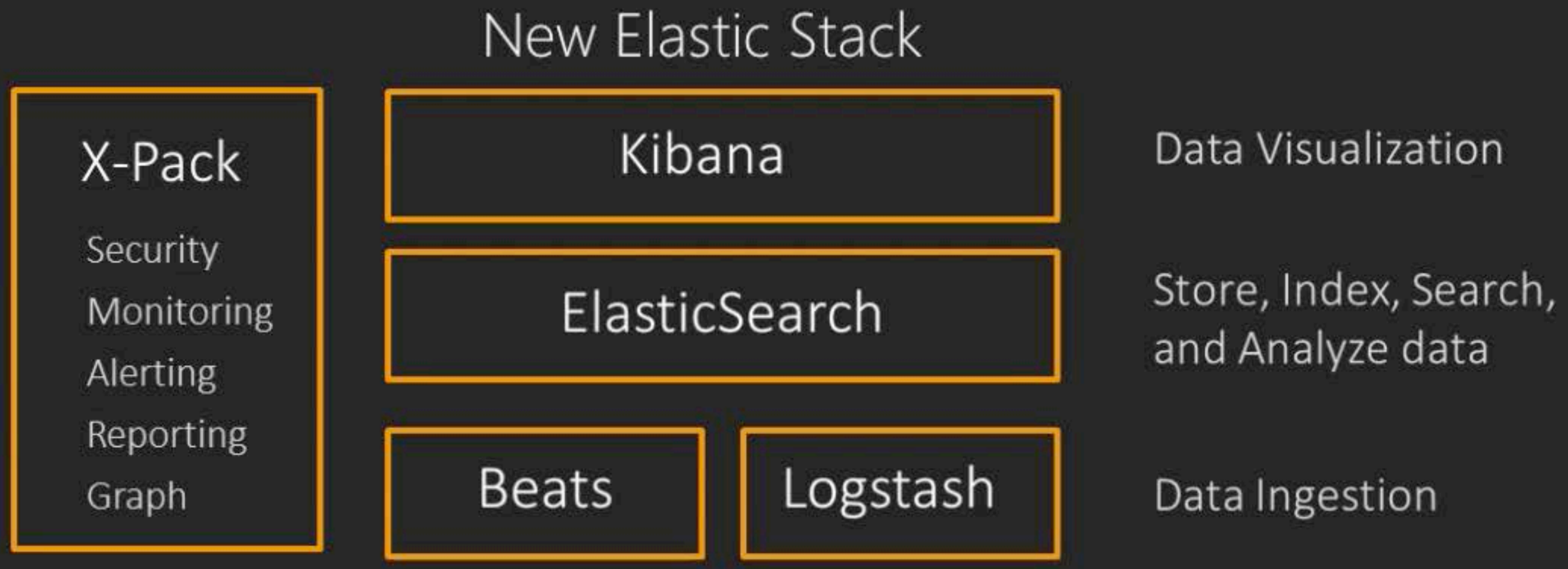

Firefox File Edit View History Bookmarks Tools Window Help
100% Wed 5:22 PM EA (蔚昊志)
Kibana
localhost:5601/app/kibana#/management/data/index/?_g=()
kibana
Discover
Visualize
Dashboard
Timelion
Management
Dev Tools
Collapse
Management / Data
Existing Data
Upload CSV
Warning No default index pattern. You must select or create one to continue.
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-*
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.
Unable to fetch mapping. Do you have indices matching the pattern?
Packt

Near Real-Time

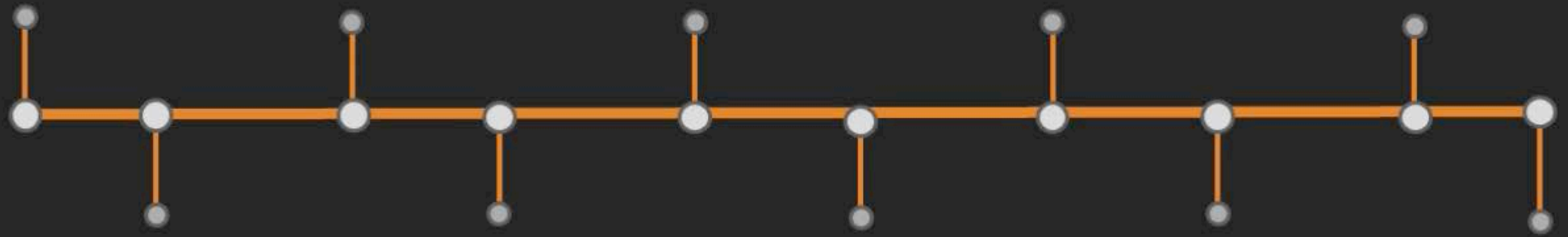
Document added

Inverted Index

Available for search


New Elastic Stack
X-Pack
Security
Monitoring
Alerting
Reporting
Graph
Kibana
ElasticSearch
Beats
Logstash
Data Visualization
Store, Index, Search, and Analyze data
Data Ingestion

The Road Map



Section 1
Getting Started with ElasticSearch

Section 2
Dichotomy of Elastic Search

Section 3
Getting Going with Documents and Indices

Section 4
Querying with RESTful API

Section 5
Power to Your Search with DSL

Section 6
What ElasticSearch Is Not?

Section 7
Getting More with the Elastic Stack

Section 8
Apache Log Analysis

Section 9
Advanced ElasticSearch Queries

Section 10
ElasticSearch Versus Apache Solr

Developer Friendly Nature

- Open Source
  - Free and well documented
- Quick setup
- Easy to use
- Language agnostic

Shards, a Closer Look (5 Primary Shards)

Single Node cluster

Node1

[P0 P1 P2 P3 P4]

Multi-Node cluster

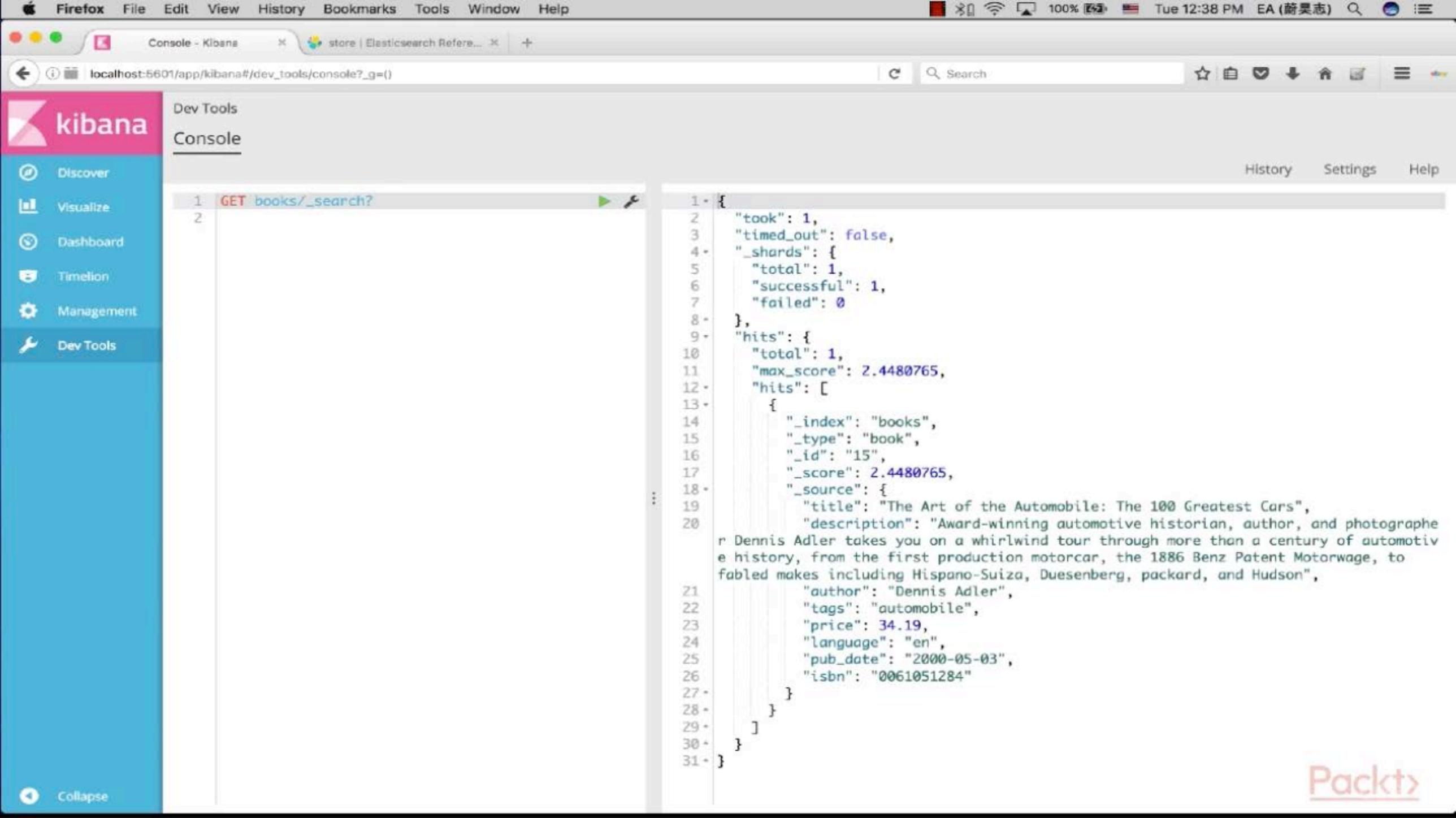
Node1

[P0 P1 P3]

Node2

[P2 P4]

* P = Primary shard


Firefox File Edit View History Bookmarks Tools Window Help
Tue 12:38 PM EA (蔚昊志)
Console - Kibana
store | Elasticsearch Refere...
localhost:5601/app/kibana#/dev_tools/console?_g=()
Search
kibana
Discover
Visualize
Dashboard
Timelion
Management
Dev Tools
Collapse
Dev Tools
Console
History
Settings
Help
1 GET books/_search?
2
1 {
2 "took": 1,
3 "timed_out": false,
4 "_shards": {
5 "total": 1,
6 "successful": 1,
7 "failed": 0
8 },
9 "hits": {
10 "total": 1,
11 "max_score": 2.4480765,
12 "hits": [
13 {
14 "_index": "books",
15 "_type": "book",
16 "_id": "15",
17 "_score": 2.4480765,
18 "_source": {
19 "title": "The Art of the Automobile: The 100 Greatest Cars",
20 "description": "Award-winning automotive historian, author, and photographe
r Dennis Adler takes you on a whirlwind tour through more than a century of automotiv
e history, from the first production motorcar, the 1886 Benz Patent Motorwage, to
fabled makes including Hispano-Suiza, Duesenberg, packard, and Hudson",
21 "author": "Dennis Adler",
22 "tags": "automobile",
23 "price": 34.19,
24 "language": "en",
25 "pub_date": "2000-05-03",
26 "isbn": "0061051284"
27 }
28 }
29]
30 }
31 }
Packt>

ElasticSearch, an "In Addition to"

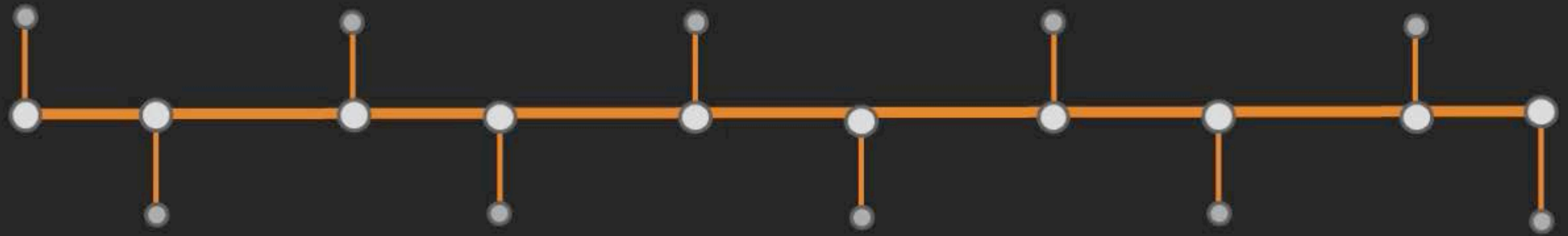
- Transactions: Sequence of operations done as a single logical unit of work

~~TRANSACTIONS~~ = SPEED!!!

- Denormalization: Process of adding redundant data, for the purpose of improving read performance

~~Denormalization~~ = SPEED!!!

The Road Map



Section 1
Getting Started with ElasticSearch

Section 2
Dichotomy of Elastic Search

Section 3
Getting Going with Documents and Indices

Section 4
Querying with RESTful API

Section 5
Power to Your Search with DSL

Section 6
What ElasticSearch Is Not?

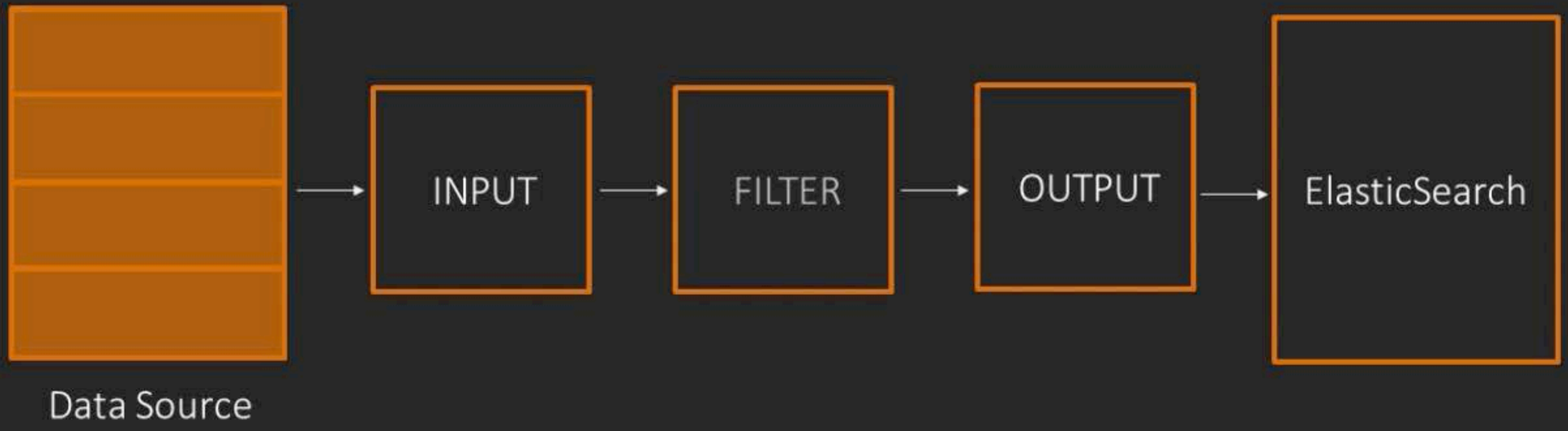
Section 7
Getting More with the Elastic Stack

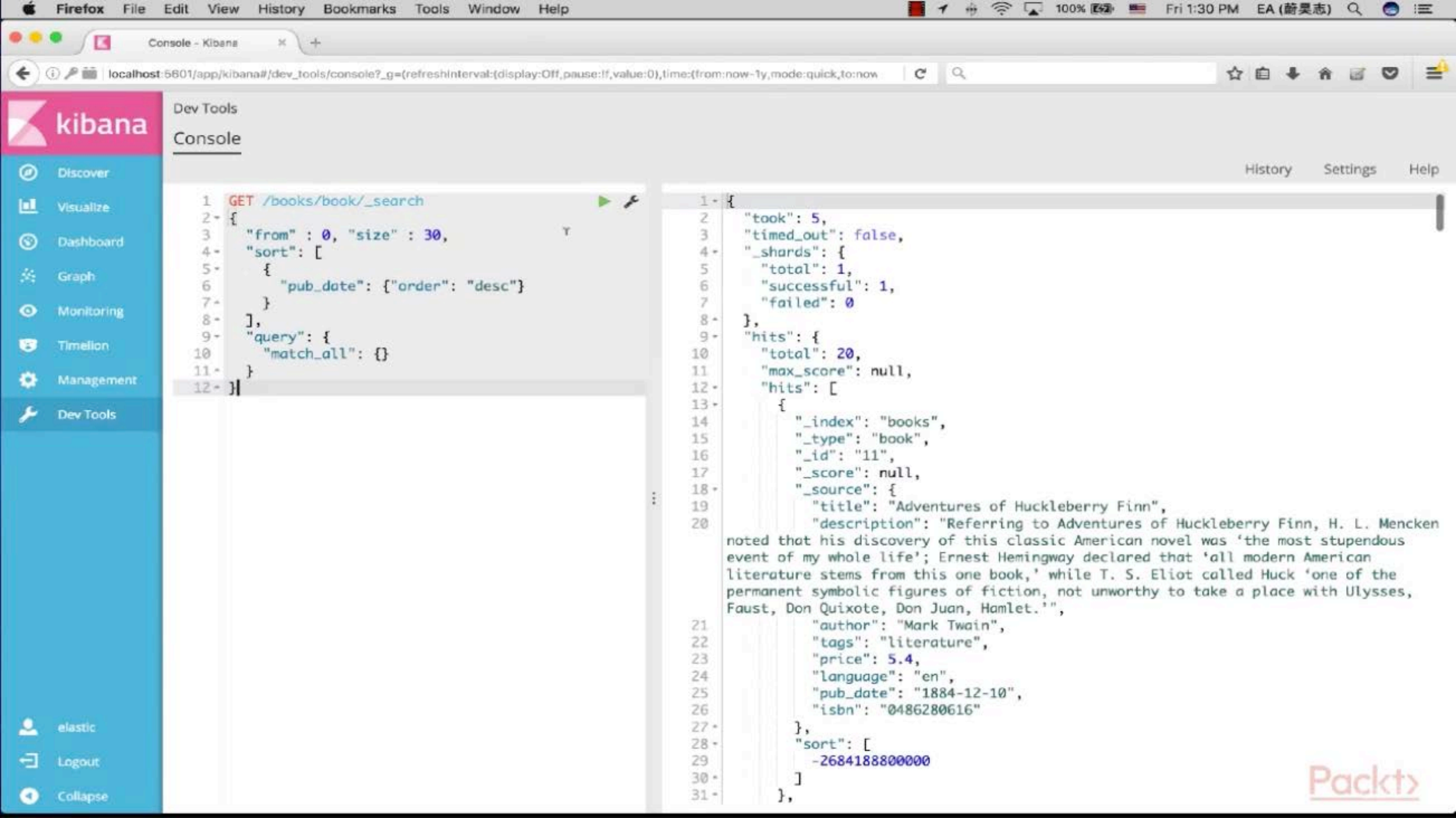
Section 8
Apache Log Analysis

Section 9
Advanced ElasticSearch Queries

Section 10
ElasticSearch Versus Apache Solr

Logstash Pipeline in Action




Firefox File Edit View History Bookmarks Tools Window Help
Fri 1:30 PM
Console - Kibana
localhost:5601/app/kibana#/dev_tools/console?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-1y,mode:quick,to:now
kibana
Discover
Visualize
Dashboard
Graph
Monitoring
Timelion
Management
Dev Tools
elastic
Logout
Collapse
Dev Tools
Console
History
Settings
Help
GET /books/book/_search
{
"from" : 0, "size" : 30,
"sort": [
{
"pub_date": {"order": "desc"}
}
],
"query": {
"match_all": {}
}
}
{
"took": 5,
"timed_out": false,
"_shards": {
"total": 1,
"successful": 1,
"failed": 0
},
"hits": {
"total": 20,
"max_score": null,
"hits": [
{
"_index": "books",
"_type": "book",
"_id": "11",
"_score": null,
"_source": {
"title": "Adventures of Huckleberry Finn",
"description": "Referring to Adventures of Huckleberry Finn, H. L. Mencken noted that his discovery of this classic American novel was 'the most stupendous event of my whole life'; Ernest Hemingway declared that 'all modern American literature stems from this one book,' while T. S. Eliot called Huck 'one of the permanent symbolic figures of fiction, not unworthy to take a place with Ulysses, Faust, Don Quixote, Don Juan, Hamlet.'",
"author": "Mark Twain",
"tags": "literature",
"price": 5.4,
"language": "en",
"pub_date": "1884-12-10",
"isbn": "0486280616"
},
"sort": [
-2684188800000
]
},
Packt>

What Is Apache Solr?

- An open source search platform based on Apache Lucene, designed to be distributed, fault tolerant, and scalable

The Goal of this Course Is

- Get the basics of ElasticSearch concepts, APIs and best use cases
- Create large-scale ElasticSearch clusters and build analytics using aggregation
- Implement ElasticSearch 5.0 in the cloud