

ELASTICSEARCH: FOR SEARCH AND BEYOND

Shaunak Kashyap • @shaunak • Developer Advocate at Elastic

WHY USE ELASTICSEARCH?

Full text search

Polski

Wolna encyklopedia

1 106 000+ haseł

Português

A enciclopédia livre

871 000+ artigos

javascri



English



JavaScript

JavaScriptCore

JavaScript library

JavaScript engine

uage:



Structured search

 meteor / meteor

 Watch 1,558

 Star 25,851

 Fork


Issues

Pull requests

Labels

Milestones

Filters ▾

 is:open is:pr author:glasser

New pull request

 Clear current search query, filters, and sorts

 1 Open ✓ 12 Closed

Author ▾

Labels ▾

Milestones ▾

Assignee ▾

Sort ▾

 Fix packages on Object prototype extension  Project:JS Environment

Faceted navigation

Times

Take-off **San Francisco (SFO)**
Mon 12:00a - Tue 12:00a



Take-off **London (LON)**
Thu 6:00a - 11:00p



Show landing times ▼

Airports

☐ Depart/Return same

San Francisco

- ☒ OAK: Oakland \$2059
- ☒ SFO: San Francisco \$1120
- ☒ SJC: San Jose \$2054

London

- ☒ LCY: London City ... \$1701
- ☒ LGW: Gatwick \$1392
- ☒ LHR: Heathrow \$1120
- ☒ SOU: Eastleigh \$2193

Airlines

Carrier | Alliance

- ☒ Aer Lingus \$1392
- ☒ Aeroflot \$1120

\$1120
KAY

Select

\$1392
Aer L

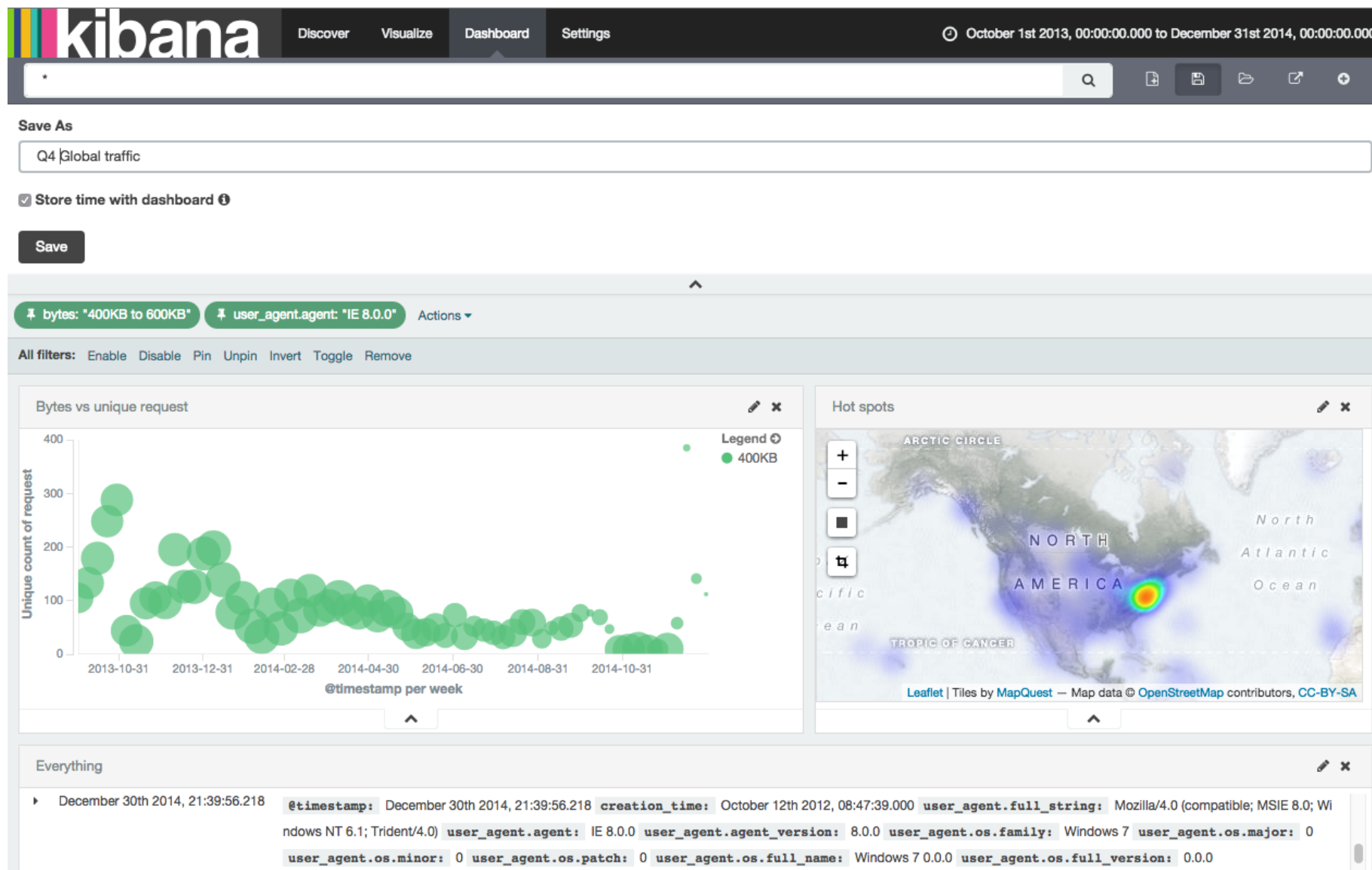
Select

\$1392
Aer L

Select

\$1120

Analytics



BUT... WHAT IS IT?

Elasticsearch is a distributed, open source search and analytics engine, designed for horizontal scalability, reliability, and easy management

SOME CONCEPTS

Document

The unit of data fed into Elasticsearch, in JSON format

```
{  
  "from": "tony@stark.com",  
  "to": [ "thor@avengers.org", "natasha@avengers.org" ],  
  "subject": "Infinity Stones",  
  "body": "..."  
}
```

Index

A collection of documents stored in Elasticsearch

Type

The category of the document within an index





DevOps Borat
@DEVOPS_BORAT



Following

In startup we are practice Outage Driven Infrastructure.

RETWEETS

455

FAVORITES

196



9:38 PM - 11 Mar 2013



MORE CONCEPTS

Shard

A part of an index, consisting of a subset of documents in that index

Node

A running Elasticsearch process

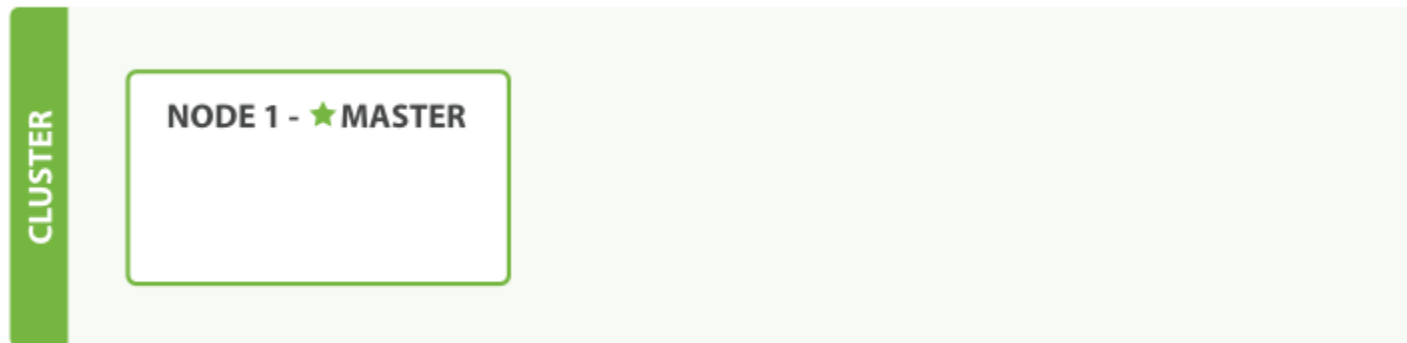
Cluster

A collection of nodes that can communicate with each other *and* share the same `cluster.name`



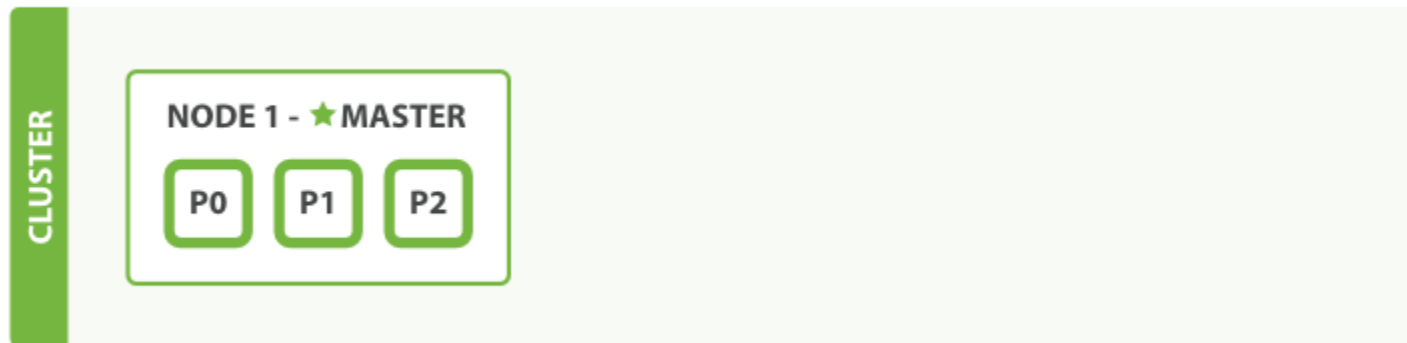
A CLUSTER OF ONE NODE

```
C:\elasticsearch-1.7.0> bin\elasticsearch
```



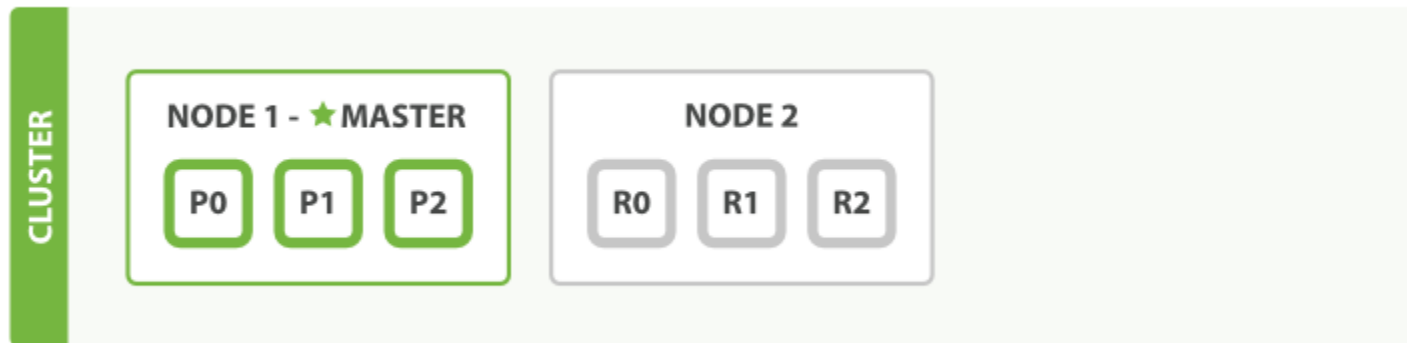
CREATING AN INDEX

```
PUT /twitter
{
  "settings": {
    "number_of_shards": 3,
    "number_of_replicas": 1
  }
}
```



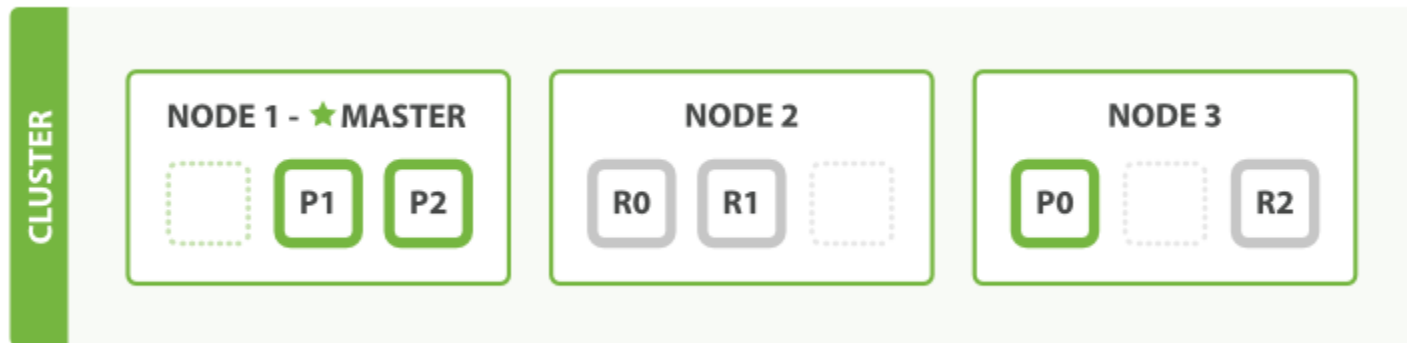
ADD ANOTHER NODE

```
C:\elasticsearch-1.7.0> bin\elasticsearch
```



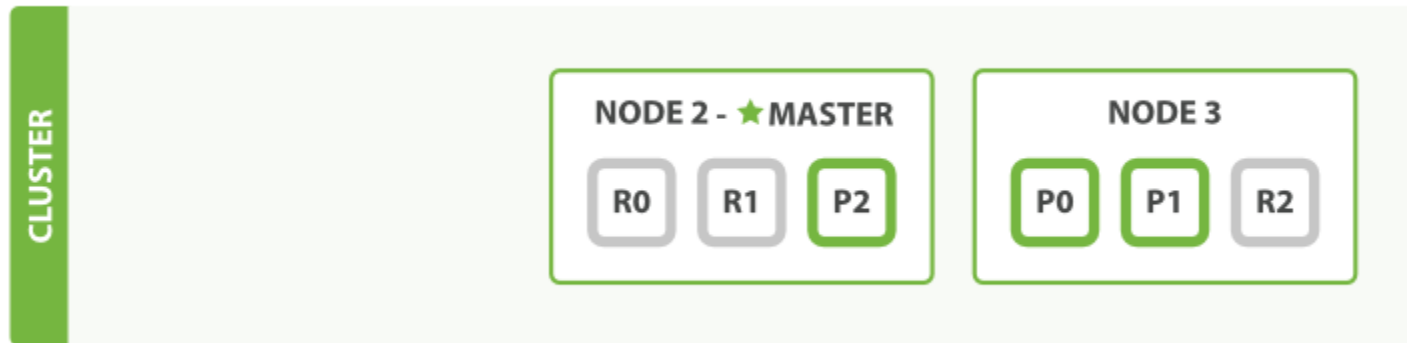
SCALING HORIZONTALLY

```
C:\elasticsearch-1.7.0> bin\elasticsearch
```



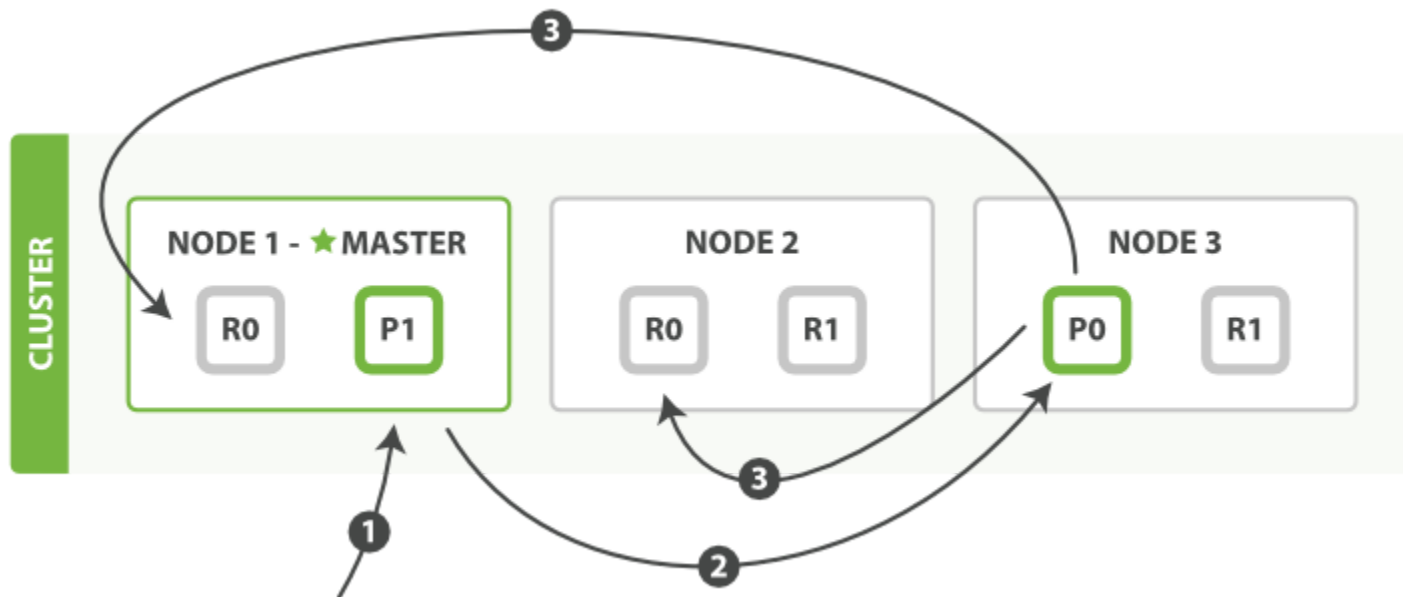
LOSE A NODE

```
C:\elasticsearch-1.7.0> bin\elasticsearch  
...  
Ctrl-C
```



INDEXING A DOCUMENT

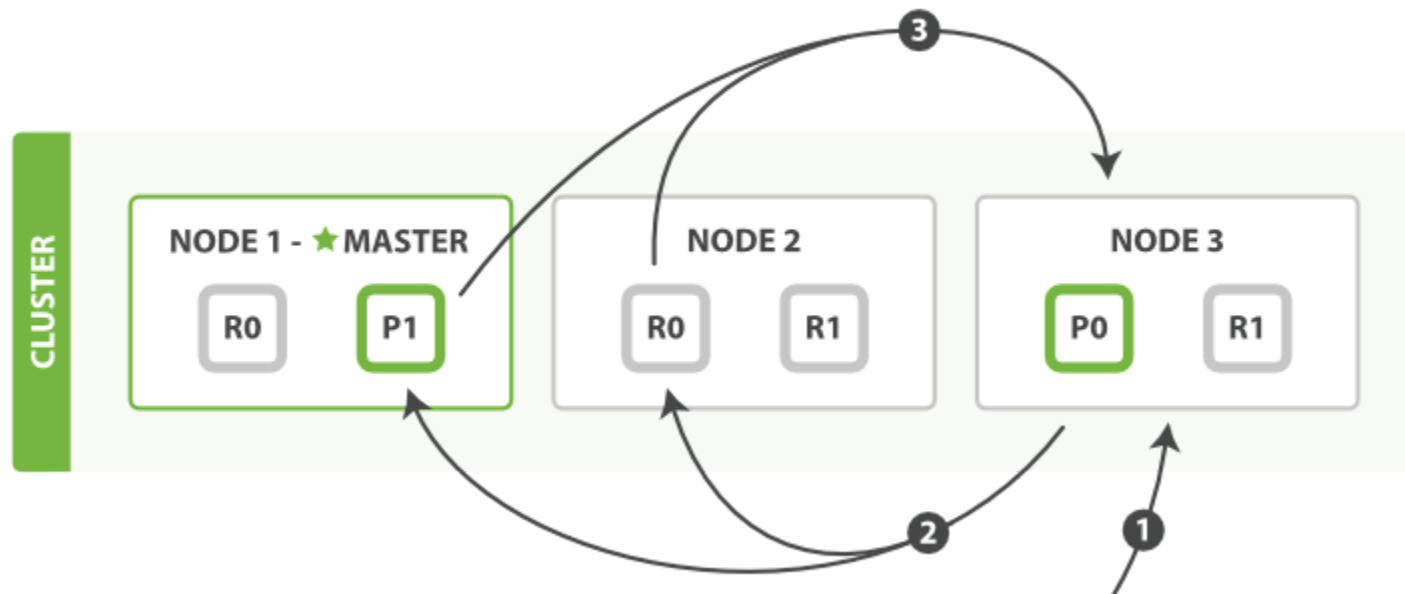
```
PUT /twitter/tweet/311335361169195009
{
  "message": "In startup we are practice Outage Driven Infrastructure.",
  "@timestamp": "2013-03-12T04:38:29.000Z"
}
```



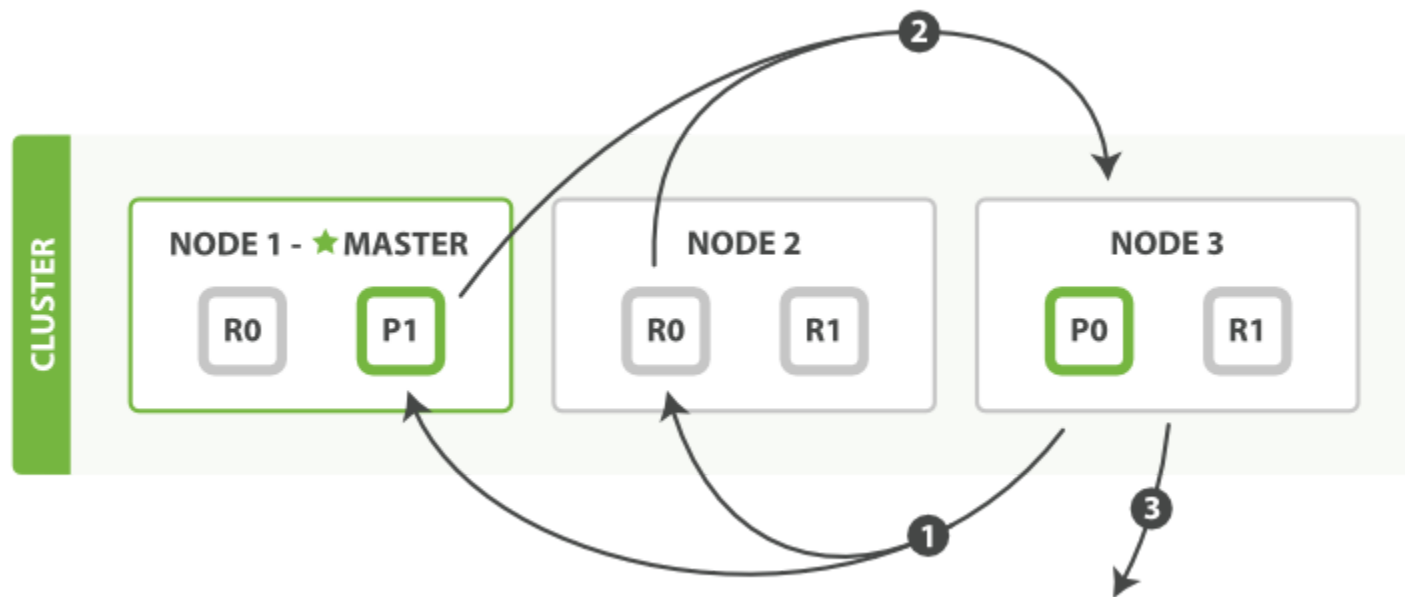
SEARCHING FOR DOCUMENTS

```
GET twitter/_search?q=devops
```

QUERY PHASE



FETCH PHASE



TODAY WE LEARNED

- Types of applications that can be built with Elasticsearch
- Key features of Elasticsearch
- Some sample index, search, and aggregations queries
- Key concepts
- How clusters work under the hood
- How indexing and searching work under the hood

THANK YOU

Shaunak Kashyap • Developer Advocate at Elastic • @shaunak

<https://discuss.elastic.co/>