

Elasticsearch

For Developer



logstash

Software Requirement

JDK 1.8

Elasticsearch 2.1.1

Kibana 4.3.1

Installation

<https://www.elastic.co/downloads/elasticsearch>

installation

1



Download and unzip the latest Elasticsearch distribution

2



**Run *bin/elasticsearch* on Unix,
or *bin/elasticsearch.bat* on Windows**

3



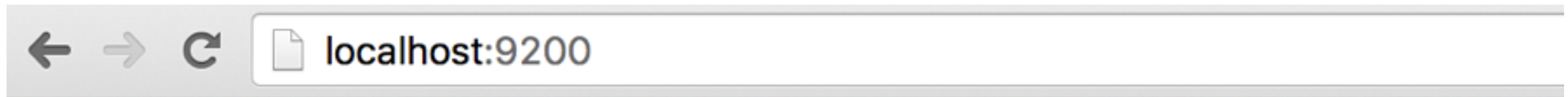
Run *curl -X GET http://localhost:9200/*

Starting

\$bin/elasticsearch

```
[2016-01-12 19:46:42,335][INFO ][node
:55Z] [Derrick Slegers Speed] version[2.1.1], pid[16245],
[2016-01-12 19:46:42,339][INFO ][node
] [Derrick Slegers Speed] initializing ...
[2016-01-12 19:46:42,479][INFO ][plugins
] [Derrick Slegers Speed] loaded [], sites []
[2016-01-12 19:46:42,540][INFO ][env
] [Derrick Slegers Speed] using [1] data paths, mount:
e_space [39.6gb], net total_space [232.6gb], spins? [unknown], types [hfs]
[2016-01-12 19:46:45,388][INFO ][node
] [Derrick Slegers Speed] initialized
[2016-01-12 19:46:45,391][INFO ][node
] [Derrick Slegers Speed] starting ...
[2016-01-12 19:46:45,511][INFO ][transport
] [Derrick Slegers Speed] publish_address {127.0.0.1:9
.1:9300}, {[fe80::1]:9300}, {[::1]:9300}
[2016-01-12 19:46:45,521][INFO ][discovery
] [Derrick Slegers Speed] elasticsearch/2XB02Bx0R66Gk
[2016-01-12 19:46:48,552][INFO ][cluster.service
] [Derrick Slegers Speed] new_master {Derrick Slegers
{127.0.0.1}{127.0.0.1:9300}, reason: zen-disco-join(elected_as_master, [0] joins received)
[2016-01-12 19:46:48,564][INFO ][http
] [Derrick Slegers Speed] publish_address {127.0.0.1:9
.1:9200}, {[fe80::1]:9200}, {[::1]:9200}
[2016-01-12 19:46:48,564][INFO ][node
] [Derrick Slegers Speed] started
[2016-01-12 19:46:48,597][INFO ][gateway
] [Derrick Slegers Speed] recovered [0] indices into
```

Welcome to Elasticsearch



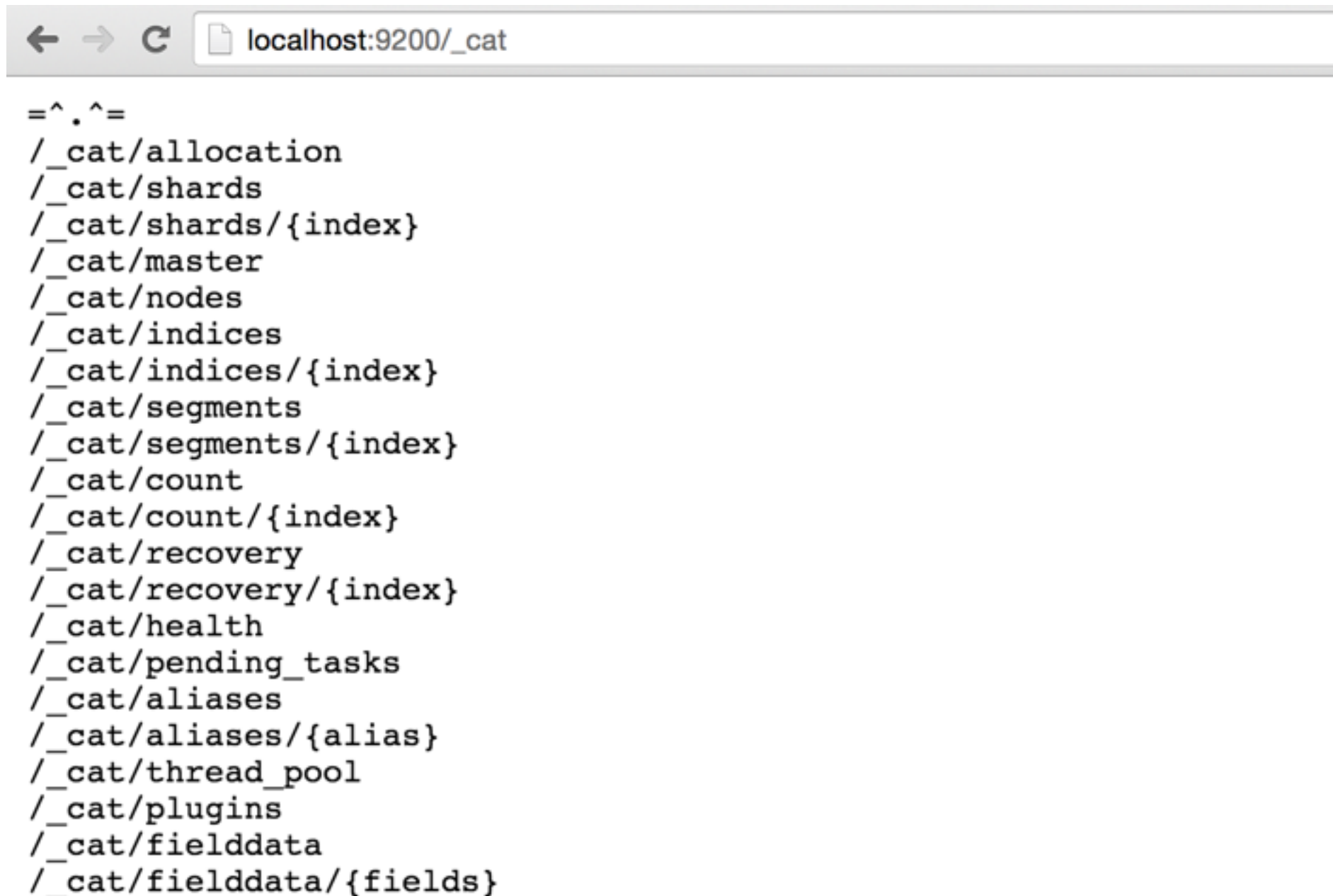
```
{
  name: "Derrick Slegers Speed",
  cluster_name: "elasticsearch",
- version: {
    number: "2.1.1",
    build_hash: "40e2c53a6b6c2972b3d13846e450e66f4375bd71",
    build_timestamp: "2015-12-15T13:05:55Z",
    build_snapshot: false,
    lucene_version: "5.3.1"
  },
  tagline: "You Know, for Search"
}
```


Starting with parameter

`$elasticsearch --cluster.name <your cluster>`
`--node.name <your node>`

```
[2016-01-13 08:26:57,870][INFO ][node                ] [somkiat] version[2.1.1], pid[16479], build[40e2c53]
[2016-01-13 08:26:57,870][INFO ][node                ] [somkiat] initializing ...
[2016-01-13 08:26:57,959][INFO ][plugins             ] [somkiat] loaded [], sites []
[2016-01-13 08:26:57,997][INFO ][env                 ] [somkiat] using [1] data paths, mounts [[/ (/dev/di
b), net total_space [232.6gb], spins? [unknown], types [hfs]
[2016-01-13 08:27:00,447][INFO ][node                ] [somkiat] initialized
[2016-01-13 08:27:00,448][INFO ][node                ] [somkiat] starting ...
[2016-01-13 08:27:00,562][INFO ][transport           ] [somkiat] publish_address {127.0.0.1:9300}, bound_a
80::1}:9300}, {[::1]:9300}
[2016-01-13 08:27:00,594][INFO ][discovery           ] [somkiat] somkiat/x5nCOWuMS6-pHMuQqAV83g
[2016-01-13 08:27:03,631][INFO ][cluster.service     ] [somkiat] new_master {somkiat}{x5nCOWuMS6-pHMuQqAV8
reason: zen-disco-join(elected_as_master, [0] joins received)
[2016-01-13 08:27:03,642][INFO ][http                ] [somkiat] publish_address {127.0.0.1:9200}, bound_a
80::1}:9200}, {[::1]:9200}
[2016-01-13 08:27:03,643][INFO ][node                ] [somkiat] started
[2016-01-13 08:27:03,670][INFO ][gateway             ] [somkiat] recovered [0] indices into cluster_state
```

CAT API



https://www.elastic.co/guide/en/elasticsearch/guide/current/_cat_api.html

มันทำงานอย่างไร

bin/

elasticsearch
plugin

config/

elasticsearch.yml
logging.yml

lib/

data/

Default port

9300

Internal communication

9200

HTTP REST

เปลี่ยนชื่อ Node

config/elasticsearch.yml

node.name=Somkiat

```
← → ↻ localhost:9200
{
  "status" : 200,
  "name" : "Somkiat",
  "version" : {
    "number" : "1.3.4",
    "build_hash" : "a70f3ccb52200f8f2c87e9c370c6597448eb3e45",
    "build_timestamp" : "2014-09-30T09:07:17Z",
    "build_snapshot" : false,
    "lucene_version" : "4.9"
  },
  "tagline" : "You Know, for Search"
}
```

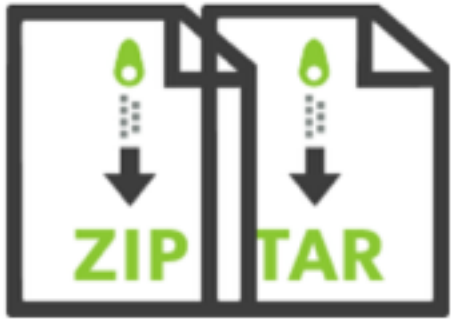
<https://github.com/elastic/elasticsearch>

การติดตั้ง Kibana

Installation

<https://www.elastic.co/downloads/kibana>

Installation Steps



Download and unzip Kibana 4

*Note: Kibana 4.3.1 requires
Elasticsearch 2.1.*



- Extract your archive
- Open `config/kibana.yml` in an editor
- Set the `elasticsearch.url` to point at your Elasticsearch instance
- Run `./bin/kibana` (or `bin\kibana.bat` on Windows)



- Point your browser at `http://yourhost.com:5601`
- Check out the [README.md](#)

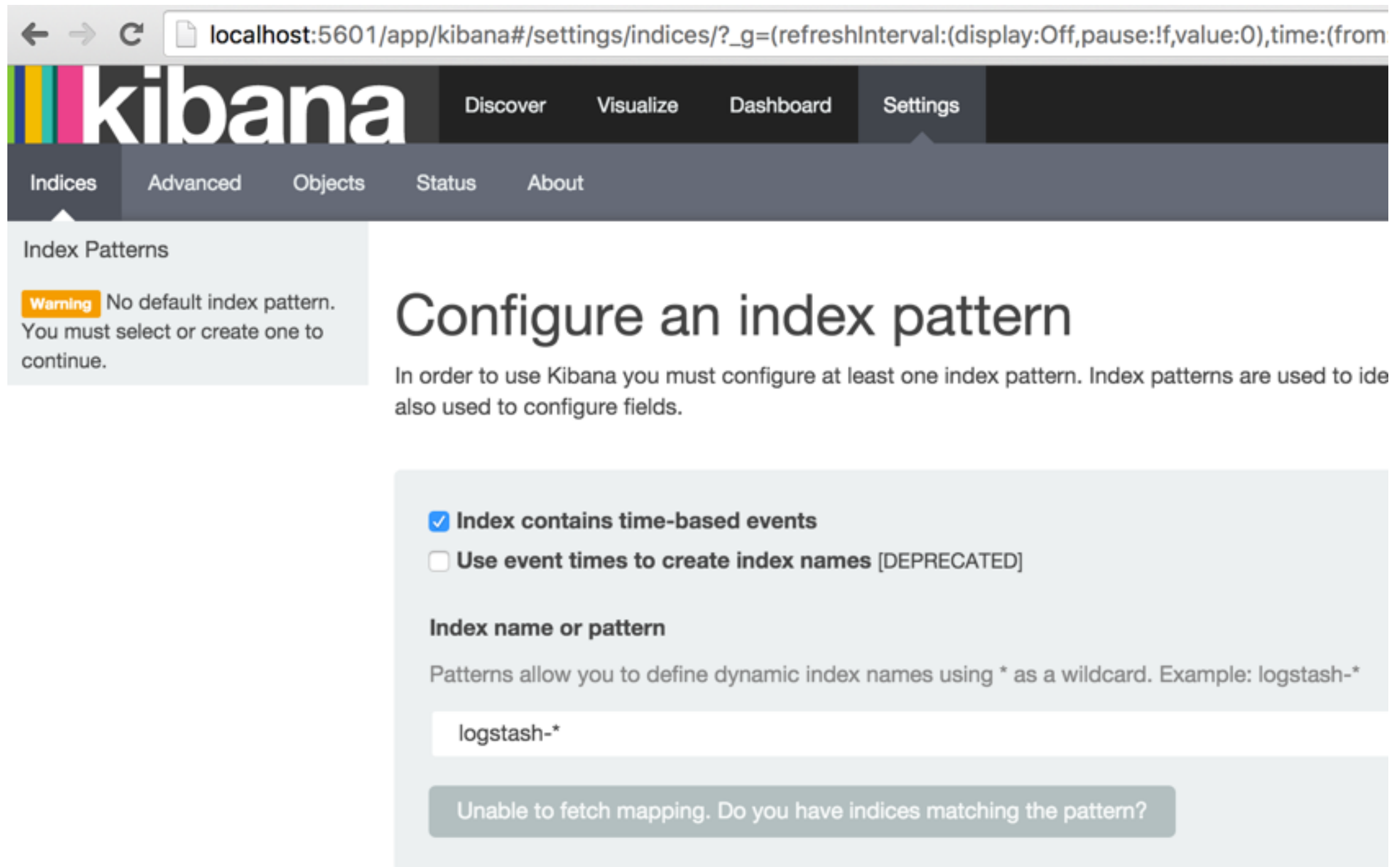
ต้อง Start elasticsearch ก่อนนะ !!

Starting

\$bin/kibana

```
MacBook-Pro-2:kibana-4.3.1-darwin-x64 somkiat$ bin/kibana
log [14:15:00.943] [info][status][plugin:kibana] Status changed from uninitialized
log [14:15:00.969] [info][status][plugin:elasticsearch] Status changed from uninitialized
Waiting for Elasticsearch
log [14:15:00.981] [info][status][plugin:kbn_vislib_vis_types] Status changed from uninitialized - Ready
log [14:15:00.985] [info][status][plugin:markdown_vis] Status changed from uninitialized
log [14:15:00.988] [info][status][plugin:metric_vis] Status changed from uninitialized
log [14:15:00.991] [info][status][plugin:spyModes] Status changed from uninitialized
log [14:15:00.994] [info][status][plugin:statusPage] Status changed from uninitialized
log [14:15:01.000] [info][status][plugin:table_vis] Status changed from uninitialized
log [14:15:01.018] [info][listening] Server running at http://0.0.0.0:5601
log [14:15:06.107] [info][status][plugin:elasticsearch] Status changed from yellow
sting Kibana index found
log [14:15:09.394] [info][status][plugin:elasticsearch] Status changed from yellow
index ready
```


Welcome to Kibana



The screenshot shows the Kibana web interface in a browser. The address bar displays `localhost:5601/app/kibana#/settings/indices/?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from`. The Kibana logo is on the left, and navigation tabs for Discover, Visualize, Dashboard, and Settings are on the right. Below these, sub-tabs for Indices, Advanced, Objects, Status, and About are visible. The 'Indices' sub-tab is active, showing 'Index Patterns'. A warning message states: 'Warning No default index pattern. You must select or create one to continue.' The main heading is 'Configure an index pattern'. Below it, explanatory text says: 'In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify data and also used to configure fields.' A configuration box contains two checkboxes: 'Index contains time-based events' (checked) and 'Use event times to create index names [DEPRECATED]' (unchecked). Below is a section titled 'Index name or pattern' with a text input field containing 'logstash-*'. A note explains: 'Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*'. At the bottom, a message box says: 'Unable to fetch mapping. Do you have indices matching the pattern?'.

localhost:5601/app/kibana#/settings/indices/?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from

kibana

Discover Visualize Dashboard Settings

Indices Advanced Objects Status About

Index Patterns

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 data and 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-*

Unable to fetch mapping. Do you have indices matching the pattern?

การติดตั้ง Sense app ใน Kibana

<https://www.elastic.co/guide/en/sense/current/index.html>

ติดตั้ง sense แบบ online

```
$cd kibana-4.3.1
```

```
$/bin/kibana plugin --install elastic/sense
```

```
Installing sense
```

```
Attempting to extract from https://download.elastic.co/ela
```

```
Downloading 318236 bytes.....
```

```
Extraction complete
```

```
Optimizing and caching browser bundles...
```

```
Plugin installation complete
```

ติดตั้ง sense แบบ offline

Download file

<https://download.elasticsearch.org/elastic/sense/sense-latest.tar.gz>

```
$/bin/kibana plugin -i sense -u file:///<path of file>
```

```
Installing sense
```

```
Attempting to extract from file:///Users/  
gz
```

```
Extraction complete
```

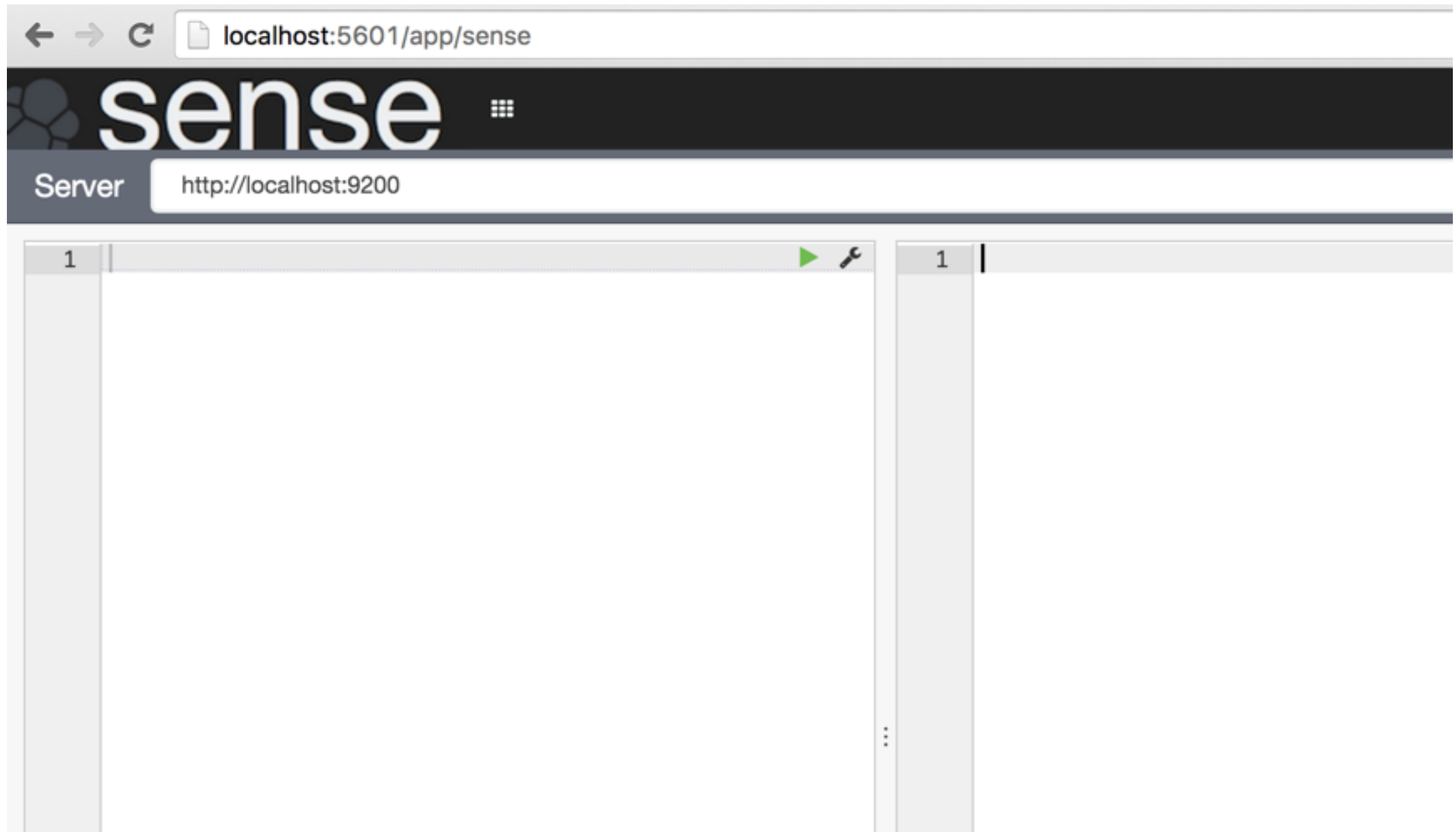
```
Optimizing and caching browser bundles...
```

```
Plugin installation complete
```

Restart Kibana

`$bin/kibana`

Welcome to Sense UI



การติดตั้ง Plugin อื่น ๆ

Head Plugin

`$/bin/plugin install mobz/elasticsearch-head`

The screenshot displays the Elasticsearch Head web interface. At the top, the browser address bar shows `localhost:9200/_plugin/head/`. The interface includes a navigation bar with tabs for Overview, Indices, Browser, Structured Query [+], and Any Request [+]. Below this, the 'Cluster Overview' section features buttons for 'Sort Cluster', 'View Aliases', and an 'Index Filter' input field. The main content area shows the status of the cluster, including a section for '.kibana' with details like 'size: 3.15ki (3.15ki)' and 'docs: 1 (1)', and buttons for 'Info' and 'Actions'. Below this, there are two rows of node information: 'Unassigned' with a warning icon and a box containing '0', and 'ElectroCute' with a star icon, 'Info' and 'Actions' buttons, and a green box containing '0'.

Let's start with elasticsearch