

ANALYZING TIME-SERIES DATA WITH **ELASTICSEARCH**, **LOGSTASH**, AND **KIBANA**

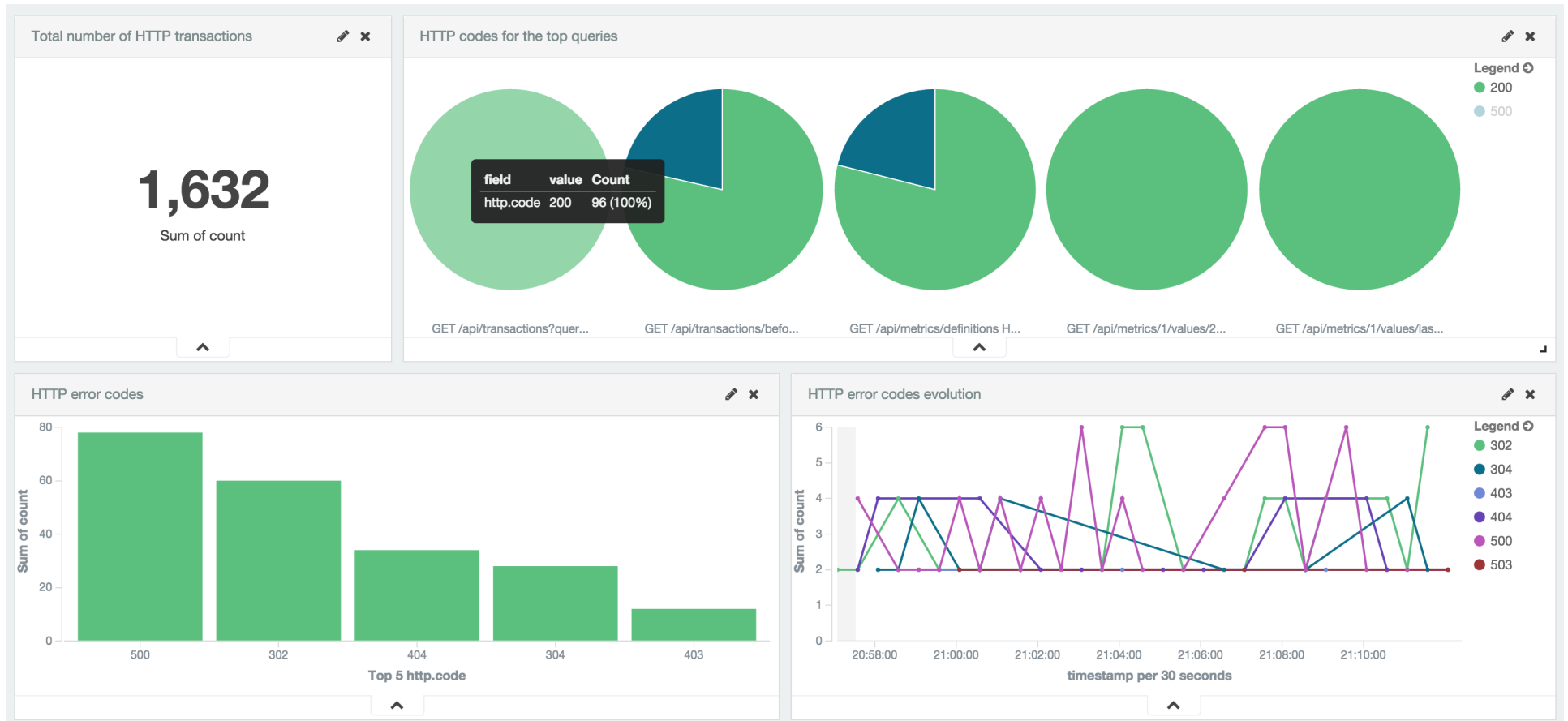
Shaunak Kashyap • [@shaunak](#) • Developer Advocate at [Elastic](#)

WHAT'S THE PROBLEM?

GOING FROM THIS

```
65.55.215.109 - - [18/Jan/2013:19:57:13 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "msnbot-media/1.1 (+http://search.msn.com/msnbot.htm)"
65.55.215.109 - - [18/Jan/2013:19:57:13 -0500] "GET /gallery/gallery/Subaru/ormeau_-_25_April_2005/thumbs/IMG_2854.JPG HTTP/1.1" 301 303 "-" "msnbot-media/1.1 (+http://search.msn.com/msnbot.htm)"
178.255.215.69 - - [18/Jan/2013:20:02:41 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; Exabot/3.0; +http://www.exabot.com/go/robot)"
178.255.215.69 - - [18/Jan/2013:20:02:42 -0500] "GET /wordpress/tag/smoke/ HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; Exabot/3.0; +http://www.exabot.com/go/robot)"
66.249.73.60 - - [18/Jan/2013:20:08:19 -0500] "GET /wordpress/cooking/mozambique-style-piri-piri-chicken/feed/ HTTP/1.1" 301 351 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
24.225.83.49 - - [18/Jan/2013:20:17:53 -0500] "GET /favicon.ico HTTP/1.1" 301 303 "http://www.eatinginabox.com/2009/10/foodblogger-event-zoes-kitchen.html" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
66.249.73.60 - - [18/Jan/2013:20:21:19 -0500] "GET /wordpress/cooking/mushroom-ragu-on-creamy-polenta/trackback/ HTTP/1.1" 301 348 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
205.169.30.2 - - [18/Jan/2013:20:23:44 -0500] "GET /favicon.ico HTTP/1.1" 301 303 "http://www.eatinginabox.com/2011/10/paleo-diet-bento.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.52 Safari/537.17"
72.14.199.133 - - [18/Jan/2013:20:23:45 -0500] "GET /wordpress/feed/ HTTP/1.1" 301 303 "-" "Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 18 subscribers; feed-id=12636598490283692241)"
66.249.73.60 - - [18/Jan/2013:20:34:00 -0500] "GET /wordpress/cooking/fettucini-with-fresh-vegetables/comment-page-1/ HTTP/1.1" 301 348 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
157.55.33.80 - - [18/Jan/2013:20:48:51 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
157.55.33.80 - - [18/Jan/2013:20:50:50 -0500] "GET /wordpress/tag/cheese/ HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
66.249.73.60 - - [18/Jan/2013:21:00:01 -0500] "GET /wordpress/cooking/cider-bean-stew-with-truffle-pate-stuffed-chicken-legs/trackback/ HTTP/1.1" 301 350 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
58.22.10.92 - - [18/Jan/2013:21:00:04 -0500] "GET /wordpress/cooking/pate-de-campagne-meatball-bacon-and-pastrami-pizza-with-garlic-pizza-fritta/ HTTP/1.0" 301 352 "http://xesla.ro/wordpress/cooking/pate-de-campagne-meatball-bacon-and-pastrami-pizza-with-garlic-pizza-fritta/" "Opera/9.80 (Windows NT 6.1; Win64; x64; U; ru) Presto/2.10.289 Version/12.00"
24.220.125.231 - - [18/Jan/2013:21:06:00 -0500] "GET /wordpress/cooking/wild-duck-gumbo/ HTTP/1.1" 301 332 "http://honest-food.net/wild-game/venison-recipes/venison-stews/wild-game-gumbo/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17"
72.14.199.133 - - [18/Jan/2013:21:23:45 -0500] "GET /wordpress/feed/ HTTP/1.1" 301 303 "-" "Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 18 subscribers; feed-id=12636598490283692241)"
66.249.73.60 - - [18/Jan/2013:21:26:07 -0500] "GET /wordpress/cooking/jagerbomb-icecream-cake/ HTTP/1.1" 301 340 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.73.60 - - [18/Jan/2013:21:28:57 -0500] "GET /wordpress/cooking/sous-vide-party/ HTTP/1.1" 301 332 "-" "DoCoMo/2.0 N905i(c100;TB;W24H16) (compatible; Googlebot-Mobile/2.1; +http://www.google.com/bot.html)"
95.108.150.235 - - [18/Jan/2013:21:29:07 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)"
95.108.150.235 - - [18/Jan/2013:21:29:07 -0500] "GET /robots.txt HTTP/1.1" 301 307 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)"
95.108.150.235 - - [18/Jan/2013:21:29:08 -0500] "GET / HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)"
95.108.150.235 - - [18/Jan/2013:21:29:08 -0500] "GET / HTTP/1.1" 301 307 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)"
94.228.34.233 - - [18/Jan/2013:21:30:08 -0500] "GET /wordpress/cooking/chocolate-bread/feed/ HTTP/1.1" 301 332 "-" "magpie-crawler/1.1 (U; Linux amd64; en-GB; +http://www.brandwatch.net)"
```

TO THIS



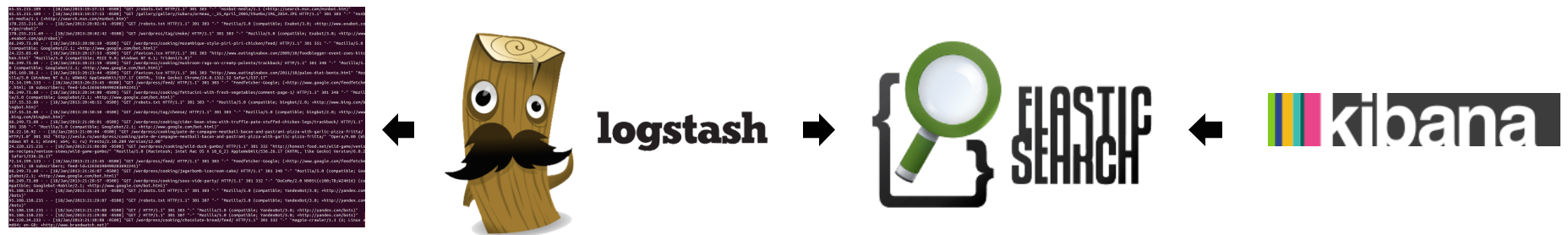
WHAT'S IN OUR TOOLKIT?



logstash



BASIC ARCHITECTURE



LOGSTASH

PLUGIN-BASED
EVENT PROCESSING PIPELINE

THE PIPELINE

```
$ cat logstash-apache.conf
```

```
input {  
  ...  
}  
  
filter {  
  ...  
}  
  
output {  
  ...  
}
```

```
$ logstash --config logstash-apache.conf
```


SAMPLE CONFIGURATION FILE

```
input {
  file {
    path => "/var/log/apache/access.log"
  }
}

filter {
  grok {
    match => [ "message", "%{IP:client} %{WORD:method} %{URIPATHPARAM:request} %{NUMBER:bytes}" ]
  }
  geoip {
    source => "client"
  }
}

output {
  elasticsearch {
    host => "192.168.0.23"
```

INPUT PLUGINS

`file , syslog , eventlog , irc , twitter , ...`

FILTER PLUGINS

`grok , geoip , anonymize , mutate , json , csv , ...`

OUTPUT PLUGINS

`elasticsearch , email , nagios , pagerduty , hipchat , zeromq ,
rabbitmq , sqs , redis , http , ...`

ELASTICSEARCH

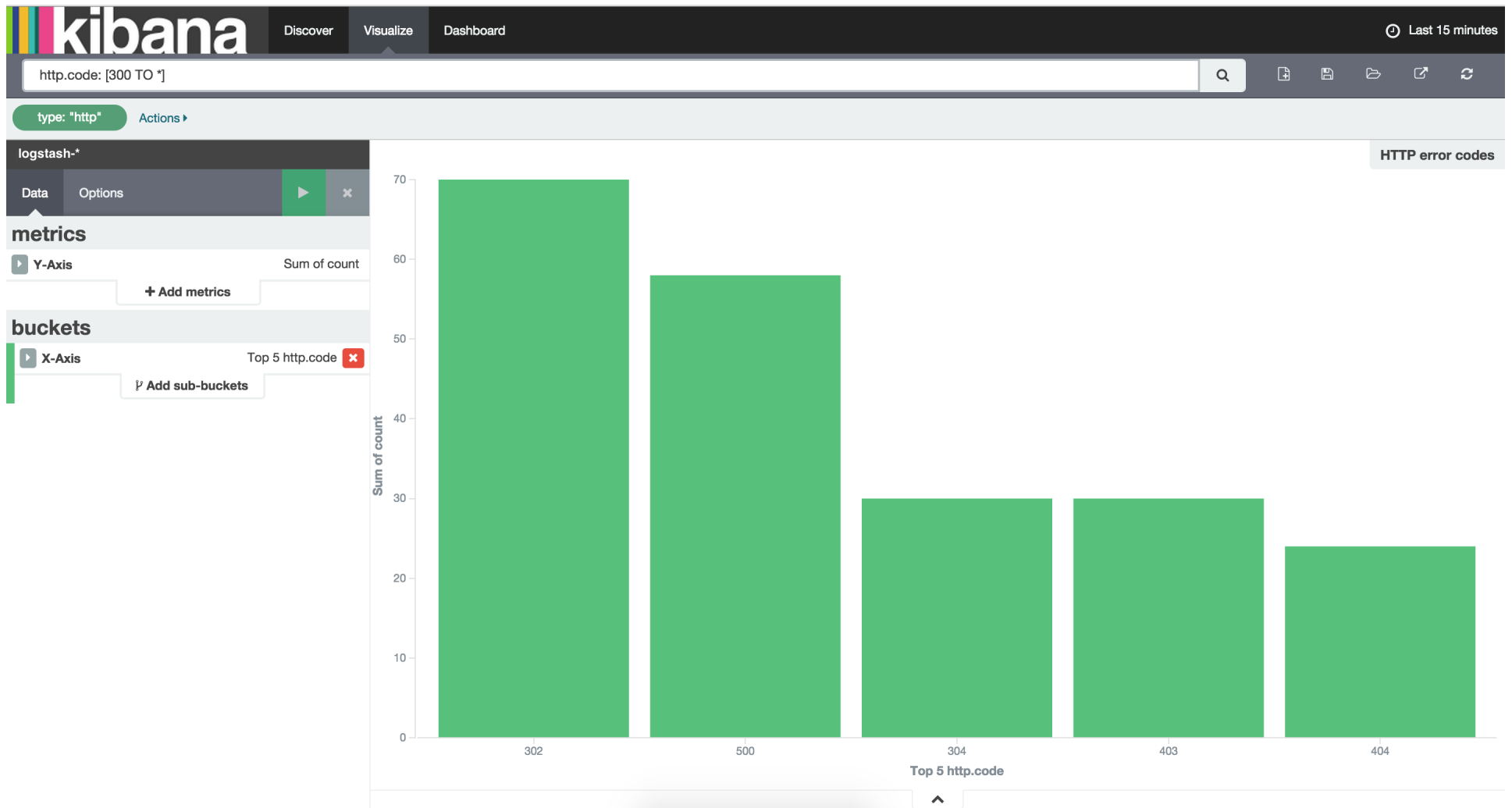
- Search and Analytics engine
- Supports fast full-text, structured, and aggregations queries
- Distributed architecture
- Has HTTP/RESTful API

- Stores data as documents
- Accepts documents as JSON
- 1 Logstash event = 1 Elasticsearch document

```
{  
  "@timestamp": "2015-09-17T01:04:32Z",  
  "client": "234.56.78.90",  
  "method": "GET",  
  "request": "/index.html",  
  "bytes": 98412,  
  "duration": 231  
}
```

- Documents are stored in user-defined indices
- Default indices created by Logstash are named `logstash-YYYY.MM.DD`
- Can accept documents one-by-one or in bulk
- Logstash uses bulk API

KIBANA



HTTP



Web transactions

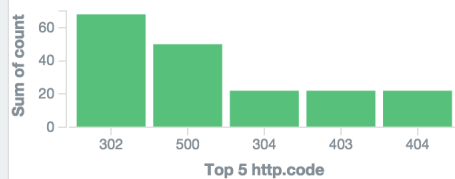


Total number of HTTP tr...

1,636

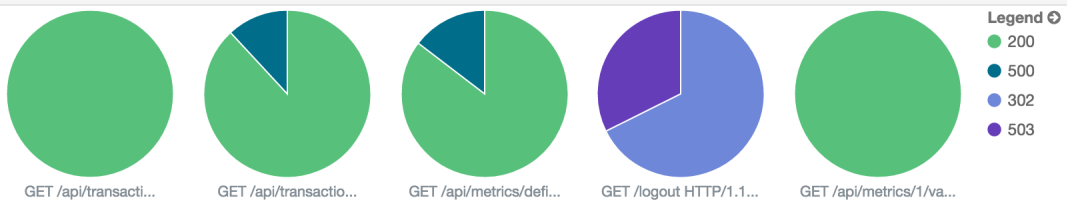
Sum of count

HTTP error codes

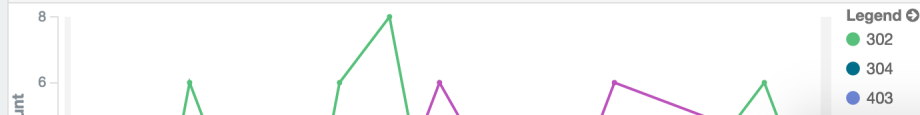


Top 5 http.code

HTTP codes for the top queries



HTTP error codes evolution



Top 10 HTTP requests

Top 10 query ↕ Q


Query	Sum of count
GET /api/transacti...	1636
GET /api/transactio...	1636
GET /api/metrics/defi...	1636
GET /logout HTTP/1.1...	1636
GET /api/metrics/1/va...	1636

- Quick

Relative

Absolute
- | | | | |
|----------------|----------------------|-----------------|---------------|
| Today | Yesterday | Last 15 minutes | Last 30 days |
| This week | Day before yesterday | Last 30 minutes | Last 60 days |
| This month | This day last week | Last 1 hour | Last 90 days |
| This year | Previous week | Last 4 hours | Last 6 months |
| The day so far | Previous month | Last 12 hours | Last 1 year |
| Week to date | Previous year | Last 24 hours | Last 2 years |
| Month to date | | Last 7 days | Last 5 years |
| Year to date | | | |






- Off
- | | | |
|------------|------------|---------|
| 5 seconds | 1 minute | 1 hour |
| 10 seconds | 5 minutes | 2 hour |
| 30 seconds | 15 minutes | 12 hour |
| 45 seconds | 30 minutes | 1 day |

DiscoverVisualizeDashboard

Last 15 minutes

HTTP

Q



Embed this dashboard.  Add to your html source. Note all clients must still be able to access kibana

```
<iframe src="http://demo.elastic.co/packetbeat/#/dashboard/HTTP?embed&_g={}&_a=(filters:!(),panels:!((col:1,id:Web-transactions,row:1,size_x:12,size_y:3,type:visualization),(col:3,id:HTTP-error-codes,row:4,size_x:3,size_y:2,type:visualization),(col:1,id:HTTP-error-codes-evolution,row:6,size_x:6,size_y:3,type:visualization),(col:1,id:Total-number-of-HTTP-transactions,row:4,size_x:2,size_y:2,type:visualization),(col:6,id:HTTP-codes-for-the-top-queries,row:4,size_x:7,size_y:2,type:visualization),(col:7,id:Top-10-HTTP-requests,row:6,size_x:6,size_y:3,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*'))),title:HTTP" height="600" width="800"></iframe>
```

Share a link 

```
http://demo.elastic.co/packetbeat/#/dashboard/HTTP?_g={}&_a=(filters:!(),panels:!((col:1,id:Web-transactions,row:1,size_x:12,size_y:3,type:visualization),(col:3,id:HTTP-error-codes,row:4,size_x:3,size_y:2,type:visualization),(col:1,id:HTTP-error-codes-evolution,row:6,size_x:6,size_y:3,type:visualization),(col:1,id:Total-number-of-HTTP-transactions,row:4,size_x:2,size_y:2,type:visualization),(col:6,id:HTTP-codes-for-the-top-queries,row:4,size_x:7,size_y:2,type:visualization),(col:7,id:Top-10-HTTP-requests,row:6,size_x:6,size_y:3,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*'))),title:HTTP)
```

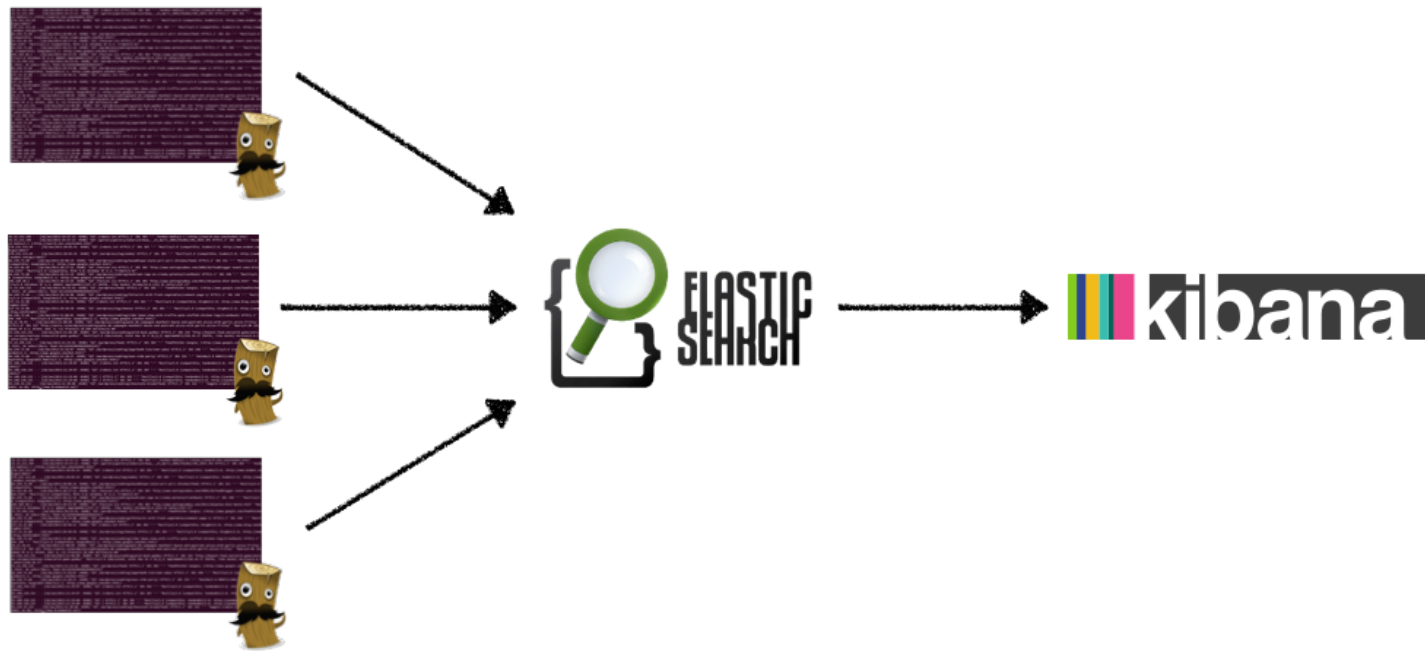


DEPLOYMENT PATTERNS

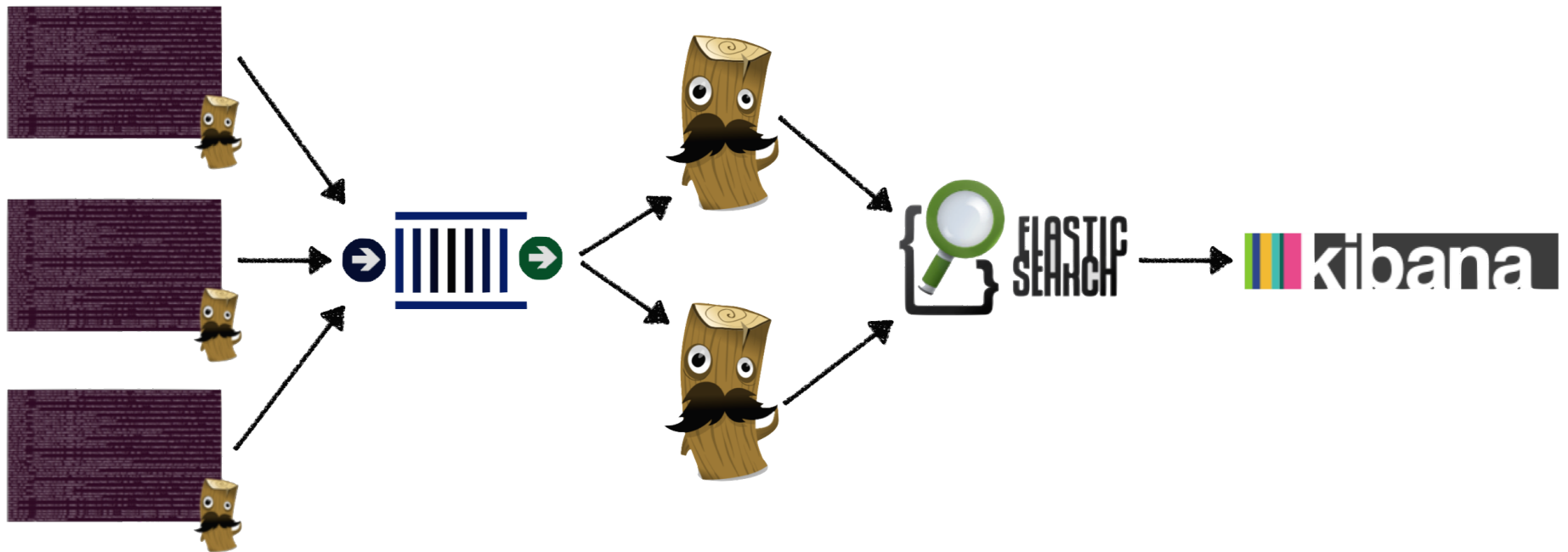
BASIC — ONE MACHINE



BASIC — MULTIPLE MACHINES



TWO TIERS — SHIPPERS AND TRANSFORMERS



BEATS

DATA SHIPPERS FOR ELASTICSEARCH

- **Packetbeat** — *for network packet analysis*
- **Topbeat** — *for system metrics analysis*
- **Filebeat** — *future replacement for logstash-forwarder*
- **BYOBeat** — *developer guide: creating a new Beat*

SUMMARY

ELASTICSEARCH, LOGSTASH, AND KIBANA

DEPLOYMENT PATTERNS

BEATS

QUESTIONS?

Shaunak Kashyap • [@shaunak](#)