

Xebia



WE ARE A GROUP OF
PASSI♥NATE

SOFTWARE DEVELOPMENT EXPERTS !

Analyse de vos logs en temps réel

Logstash|Elasticsearch|Kibana

Speaker



Vincent SPIEWAK
@vspiewak

- Master TA – UPMC (Paris VI)
- 5 ans XP
- <http://blog.xebia.fr>
- @vspiewak

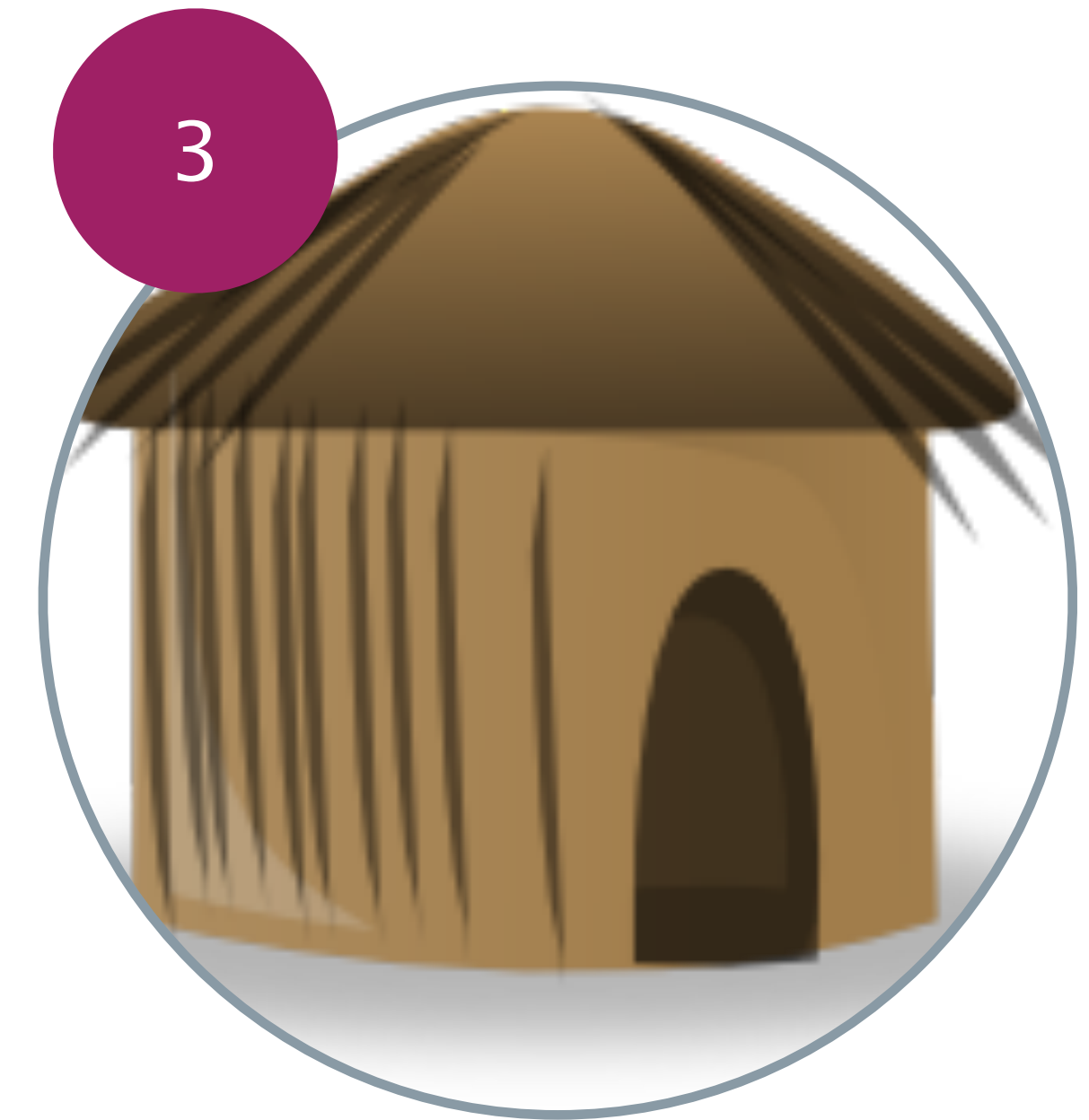
Stack



Logstash
Parse



Elasticsearch
Stockage



Kibana
Visualisation

Logstash

Inputs

36

- » stdin
- » file
- » udp
- » tcp
- » rabbitmq
- » s3
- » ...

Codecs

14

- » plain
- » json
- » line
- » multiline
- » dots
- » msgpack
- » netflow
- » ...

Filters

40

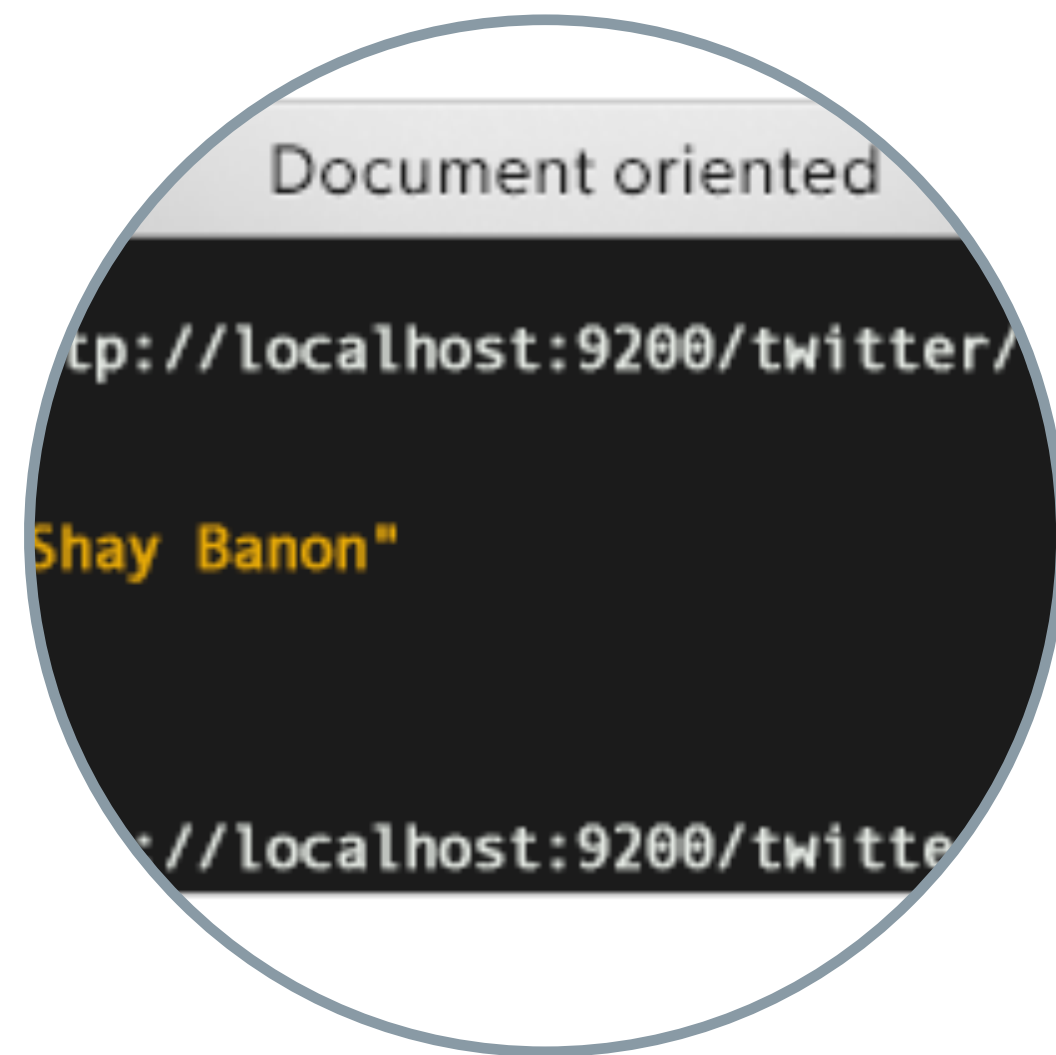
- » grok
- » date
- » drop
- » mutate
- » geoip
- » anonymize
- » ...

Outputs

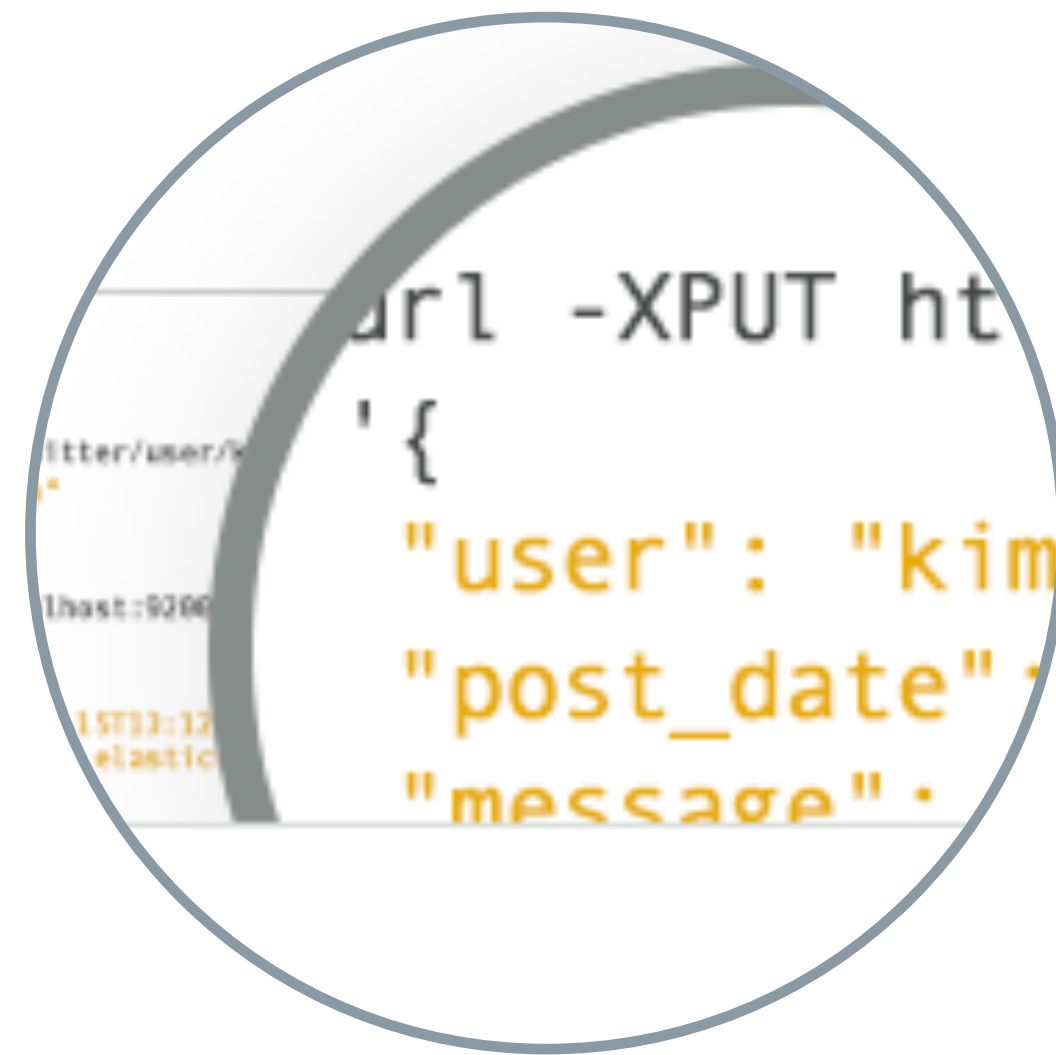
50

- » stdout
- » file
- » udp
- » tcp
- » rabbitmq
- » elasticsearch
- » ...

Elasticsearch



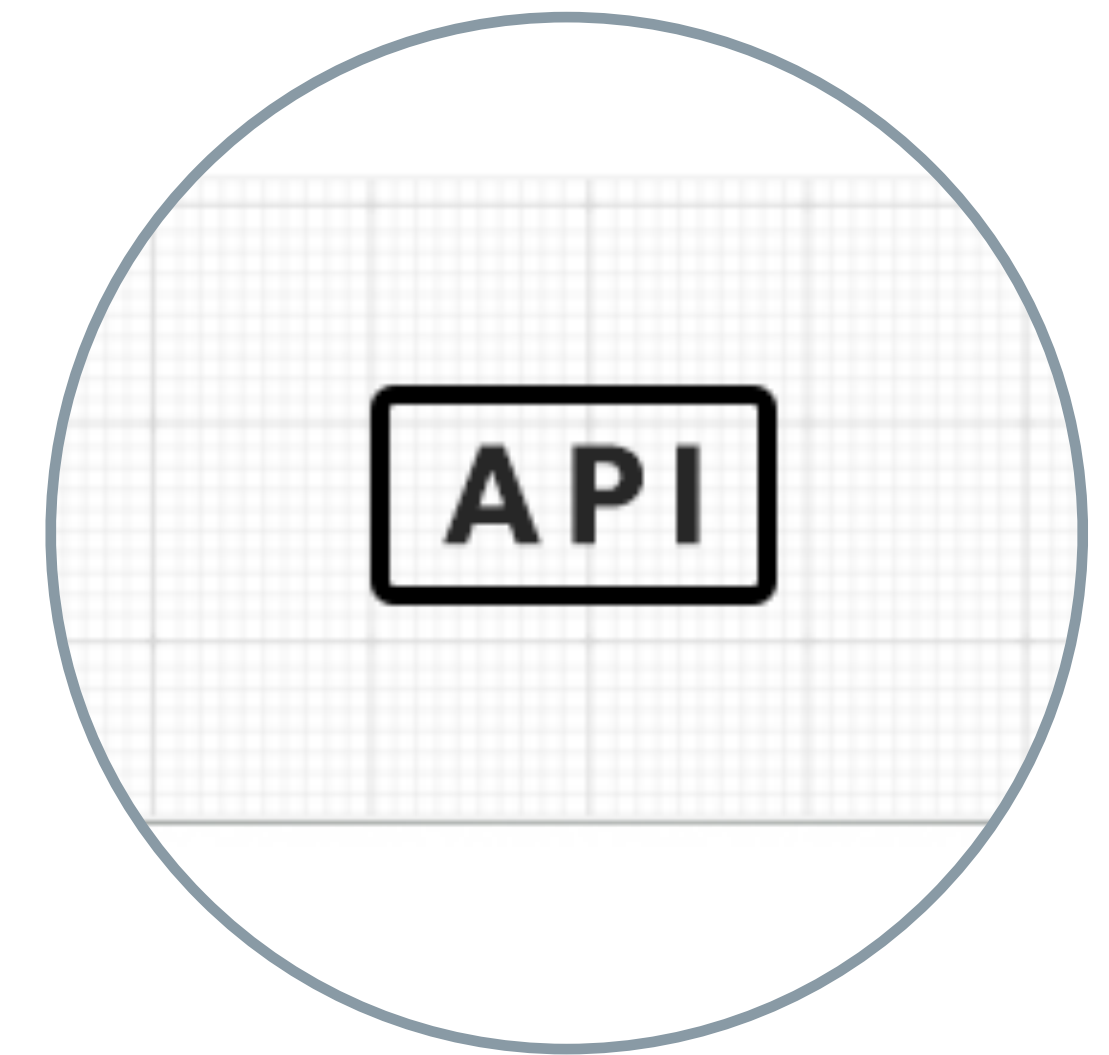
document
json documents in index



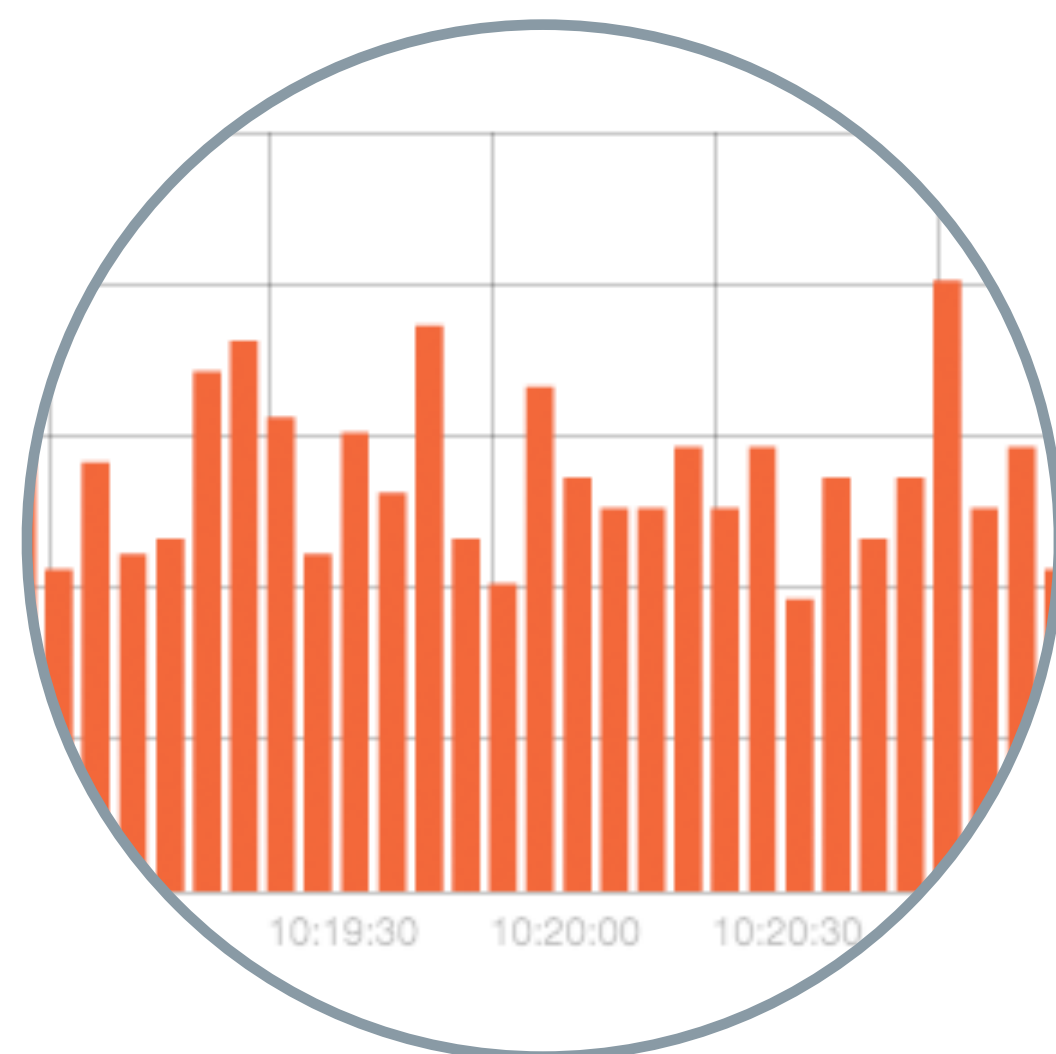
schema free
structure your datas progressively



full text search
based on apache lucene



restful api
for seamless integration



real time
real time is only acceptable



distributed
cluster datas sharded on nodes



high availability
auto



multi-tenancy
multi index

Kibana



HTML



Dashboards adaptés



Ops

Infrastructure

- » état serveur
- » répartition de charge



Dev

Applicatif

- » stacktrace
- » info, warn, error



Marketing

Business

- » client
- » produit



Direction

Objectifs

- » résultat
- » progression

Logstash: Configuration

```
input {  
  stdin {}  
  file {  
    type => "syslog"  
    path => ["/var/app.log", "/var/log/*.log"]  
  }  
}  
  
# filters  
  
output {  
  stdout { debug => true }  
  elasticsearch {}  
}
```





Logstash: Agent

```
java -jar logstash.jar agent -f app.conf
```

```
2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043
```

```
{  
  "message" => "2011-04-19T03:44:01.103Z GET /index.html 15824 0.043",  
  "@timestamp" => "2013-11-03T19:48:53.175Z",  
  "@version" => "1",  
  "host" => "macbook"  
}
```


Sortie Elasticsearch

	_river size: 7.25k (7.25k) docs: 2 (3) Info Actions	logstash-2013.12.01 size: 73.5k (73.5k) docs: 26 (26) Info Actions	mobiles size: 123M (123M) docs: 127977 (127977) Info Actions
 Epoch macbookpro Info Actions			
 Thundra macbookpro Info Actions	<div>0</div>	<div>0</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div>	<div>0</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div>
 Unassigned	<div>0</div>	<div>0</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div>	<div>0</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div>

	_type	_id	_score ▼	message
2013.12.01	logs	ggN5QL6SSueQsGR_9q28Yg	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	5k1fOjRhSzyOLKO63p5wwg	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	3hz2500ySI-bzWsHCucZXw	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	3hz2500ySI-bzWsHCucZXw	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	3e1kyeP5TK-ZF6MkmUIQTQ	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	55.3.244.1 GET /index.html 15824 0.043	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	2013-12-01T21:17:28.821Z	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	1	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	macbookpro	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	55.3.244.1	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	GET	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	/index.html	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	15824	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	0.043	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	DIIQk4-KSam2XPxwE78Jrg	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	aOXeUNCISeCEHhTSKJIng	1	55.3.244.1 GET /index.html 1582
2013.12.01	logs	TXFKXcQqQ6aYEmfsDo5upw	1	dsqddqs

Filtre Grok

```
2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043
```

```
filter {
  grok {
    match => [
      "message",
      "%{TIMESTAMP_ISO8601:date} %{IP:client} %{WORD:method} %{URIPATHPARAM:uri} %{NUMBER:bytes} %{NUMBER:duration}"
    ]
  }
}
```


Filtre Grok: sortie

```
java -jar logstash.jar agent -f app.conf
```

```
2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043
```

```
{
  "@timestamp" => "2013-12-01T21:19:11.303Z",
  "@version"   => "1",
  "@bytes"     => "15824",
  "@client"    => "55.3.244.1",
  "date"       => "2011-04-19T03:44:01.103Z",
  "@duration"  => "0.043",
  "host"       => "macbookpro",
  "message"    => "2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043",
  "method"     => "GET",
  "uri"        => "/index.html",
}
```


Filtre Grok: failure

```
java -jar logstash.jar agent -f app.conf
```

this line will fail...

```
{
  "@timestamp" => "2013-12-01T21:19:11.303Z",
  "@version"   => "1",
  "host"       => "macbookpro",
  "message"    => "this line will fail...»,
  "tags"       => [
    [0] "_grokparsefailure"
  ]
}
```


Patterns Grok

<https://github.com/logstash/logstash/blob/master/patterns/grok-patterns>

USERNAME `[a-zA-Z0-9._-]+`

USER `%{USERNAME}`

INT `(?:[+-]?(?:[0-9]+))`

WORD `\b\w+\b`

NOTSPACE `\S+`

SPACE `\s*`

DATA `. *?`

GREEDYDATA `. *`

HTTPDATE `%{MONTHDAY}/%{MONTH}/%{YEAR}:%{TIME} %{INT}`

COMBINEDAPACHELOG `%{IPORHOST:clientip} ...`

Filtre Date: @timestamp

```
2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043
```

```
filter {
  geoip {
    match => [ "date", "ISO8601" ],
  }
}

{
  "@timestamp" => "2013-12-01T21:19:11.303Z",
  "@version" => "1",
  "@bytes" => "15824",
  "@client" => "55.3.244.1",
  "date" => "2011-04-19T03:44:01.103Z",
  "@duration" => "0.043",
  "host" => "macbookpro",
  "message" => "2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043",
  "method" => "GET",
  "uri" => "/index.html",
}
```


Filtre Mutate, If ... else

```
filter {  
  if [uri] =~ /^\/index.html/ {  
    mutate { add_tag => "landing-page" }  
  } else if [uri] =~ /^\/blog/ {  
    mutate { add_tag => "blog" }  
  }  
}
```

```
2011-04-19T03:44:01.103Z 55.3.244.1 GET /index.html 15824 0.043
```

```
"tags" => [  
  [0] "landing-page"  
]
```

```
2011-04-19T03:44:01.103Z 55.3.244.1 GET /blog/article-123.html 15824 0.043
```

```
"tags" => [  
  [0] "blog"  
]
```


Filtre GeoIP

```
filter {  
  geoip {  
    source => "client",  
  }  
}  
  
"geoip" => {  
  "area_code" => "520",  
  "city_name" => "Fort Huachuca",  
  "continent_code" => "NA",  
  "country_code2" => "US",  
  "country_code3" => "USA",  
  "country_name" => "United States",  
  "dma_code" => "789",  
  "ip" => "55.3.244.1",  
  "latitude" => 31.527299999999997,  
  "longitude" => -110.3607,  
  "postal_code" => "85613",  
  "real_region_name" => "Arizona",  
  "region_name" => "AZ",  
  "timezone" => "America/Phoenix",  
}
```


Kibana: terms

Top clients, Top produits

TOP CUSTOMERS						
Term	Count	Action				
gmail.com	367	Q Ø				
client920	2	Q Ø				
client828	2	Q Ø				
client706	2	Q Ø				
client677	2	Q Ø				

TOP PRODUCTS						
Term	Count	Action				
ipod	153	Q Ø				
touch	78	Q Ø				
iphone	72	Q Ø				
macbook	31	Q Ø				
nano	19	Q Ø				

Elasticsearch Template Mapping

change analyzer on specific indexes

```
curl -XPUT http://localhost:9200/_template/logstash_per_index -d '{
  "template" : "logstash*",
  "mappings" : {
    "_default_" : {
      "_all" : {"enabled" : false},
      "properties" : {
        "@timestamp": { "type": "date", "index": "not_analyzed" },
        "ip": { "type" : "ip", "index": "not_analyzed" },
        "name": { "type" : "string", "index": "not_analyzed" },
        "options": { "type" : "string", "index": "not_analyzed" },
        "email": { "type" : "string", "index": "not_analyzed" }
      }
    }
  }
}
```


Vente en ligne

geekshop

A Quels sont les produits les plus achetés ?

B Quelle est la répartition H/F de mes clients

C Quels sont mes clients les plus fidèles ?

D Combien de femmes à Paris ont acheté un iPod Touch Bleu 32 Go entre le 12 octobre 2012 à 14h30 et le 4 novembre 2013 à 19h ?



**THANK
YOU**

FOR watching

Merci!