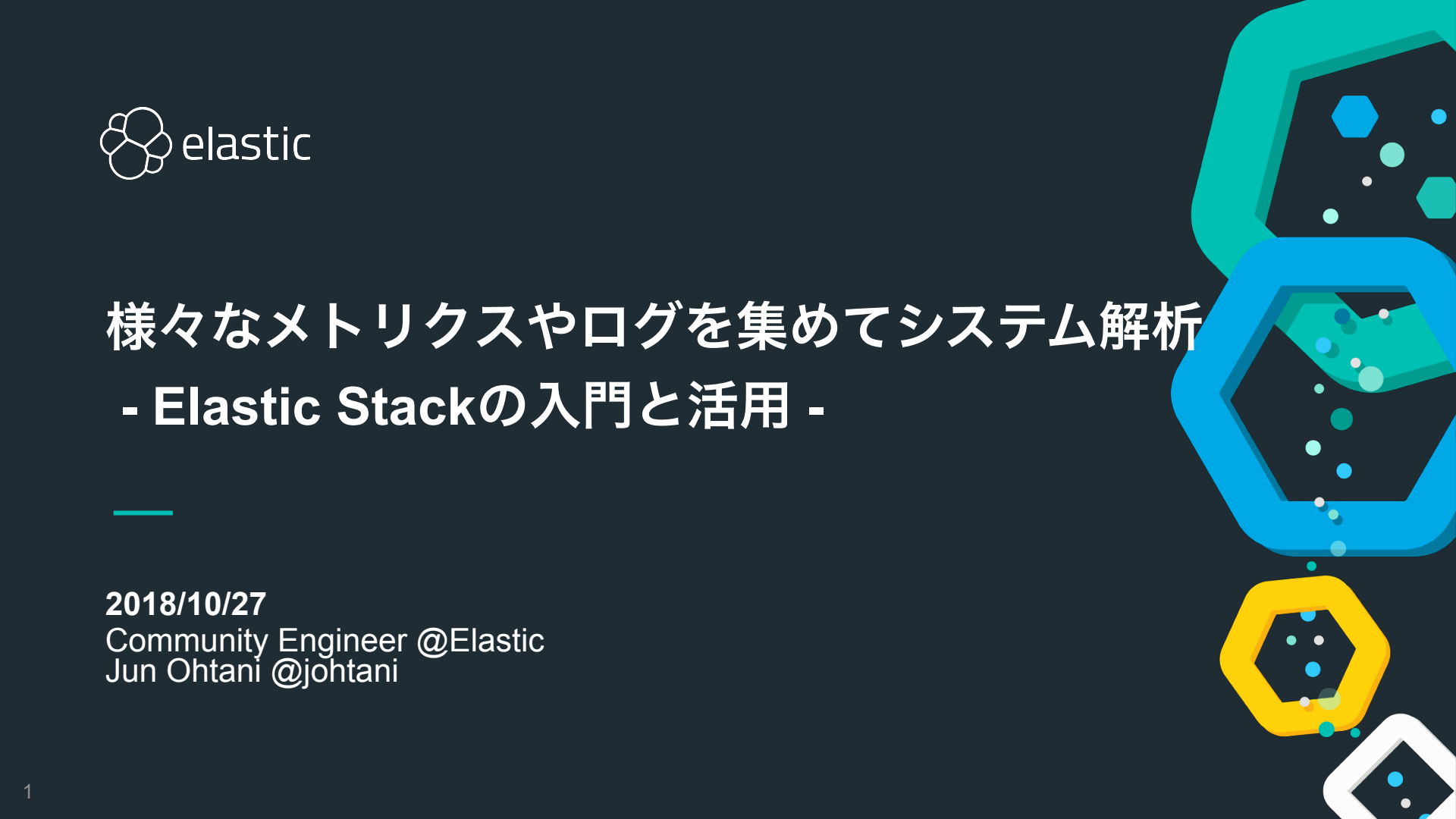


様々なメトリクスやログを集めてシステム解析
- Elastic Stackの入門と活用 -

2018/10/27

Community Engineer @Elastic
Jun Ohtani @johtani

アジェンダ

- メトリック／ログとは？
- システムメトリクス解析、ログ解析を試しにやってみよう
  - Beats - Elasticsearch - Kibanaで解析
- 本格的に解析をやるには？
  - Logstashでログやメトリクスを中継・集約
- さらに色々試してみるには？

about

- Me, Jun Ohtani / Community Engineer
  - lucene-gosenコミッター
  - データ分析基盤構築入門 共著
  - http://blog.johtani.info
- Elastic, founded in 2012
  - Products: Elasticsearch, Logstash, Kibana, Beats
    Elastic APM,
    Elastic Cloud, Swiftype
    Professional services: Support & development subscriptions
    Trainings, Consulting, SaaS

どんなメトリック、
ログを集めていますか？

メトリック

- CPU、メモリ使用率、ディスク使用率
- アクセス数、ネットワーク転送量
- 応答時間
- コネクション数
- トランザクション数、売上
- コンテナの上の各種メトリクス

ログ

- 認証ログ
- システムログ
- アプリケーションログ
- Slow log
- アクセスログ
- コンテナの中のログ

“

できればログとメトリックを
まとめて1つの画面で
見たいですよね？

Elastic Stack

Elastic Stack

Kibana

可視化、管理

Elasticsearch

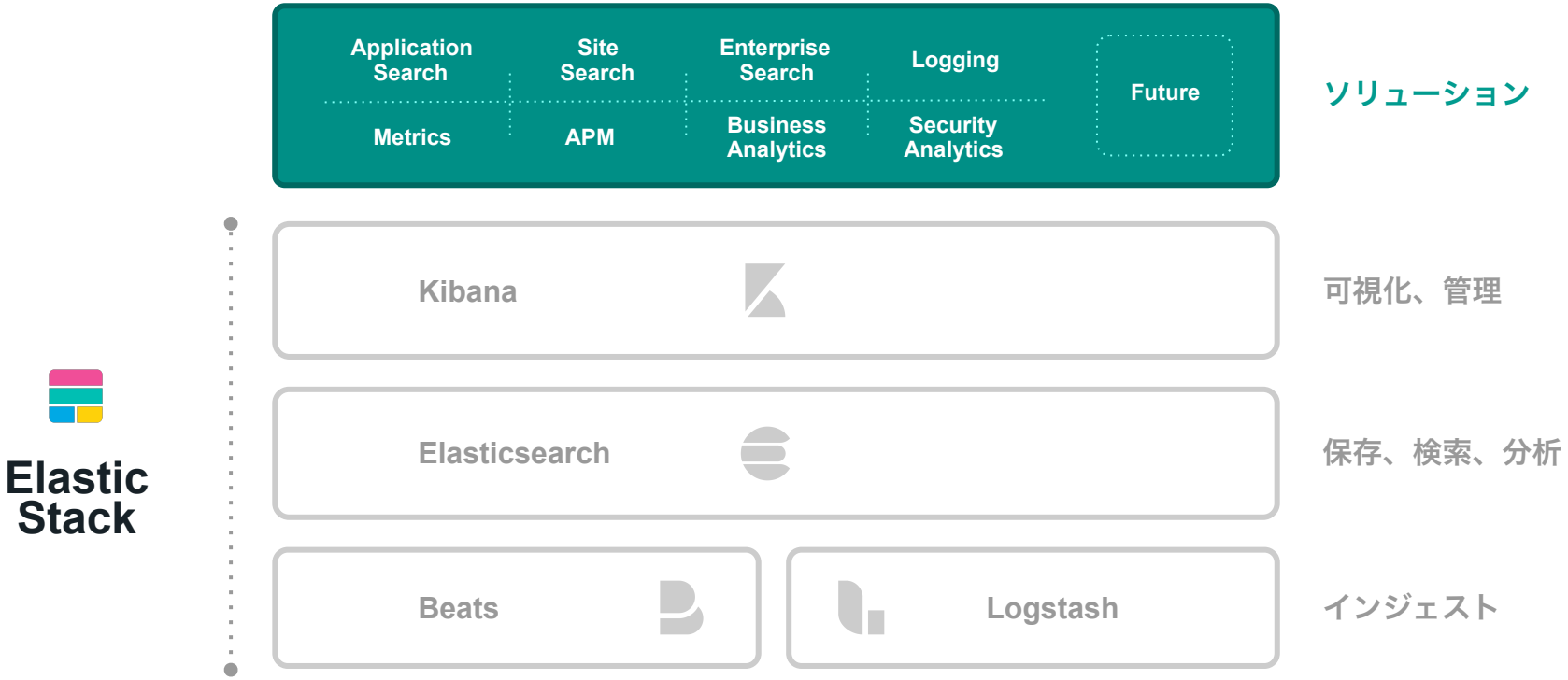
保存、検索、分析

Beats

Logstash

インジェスト

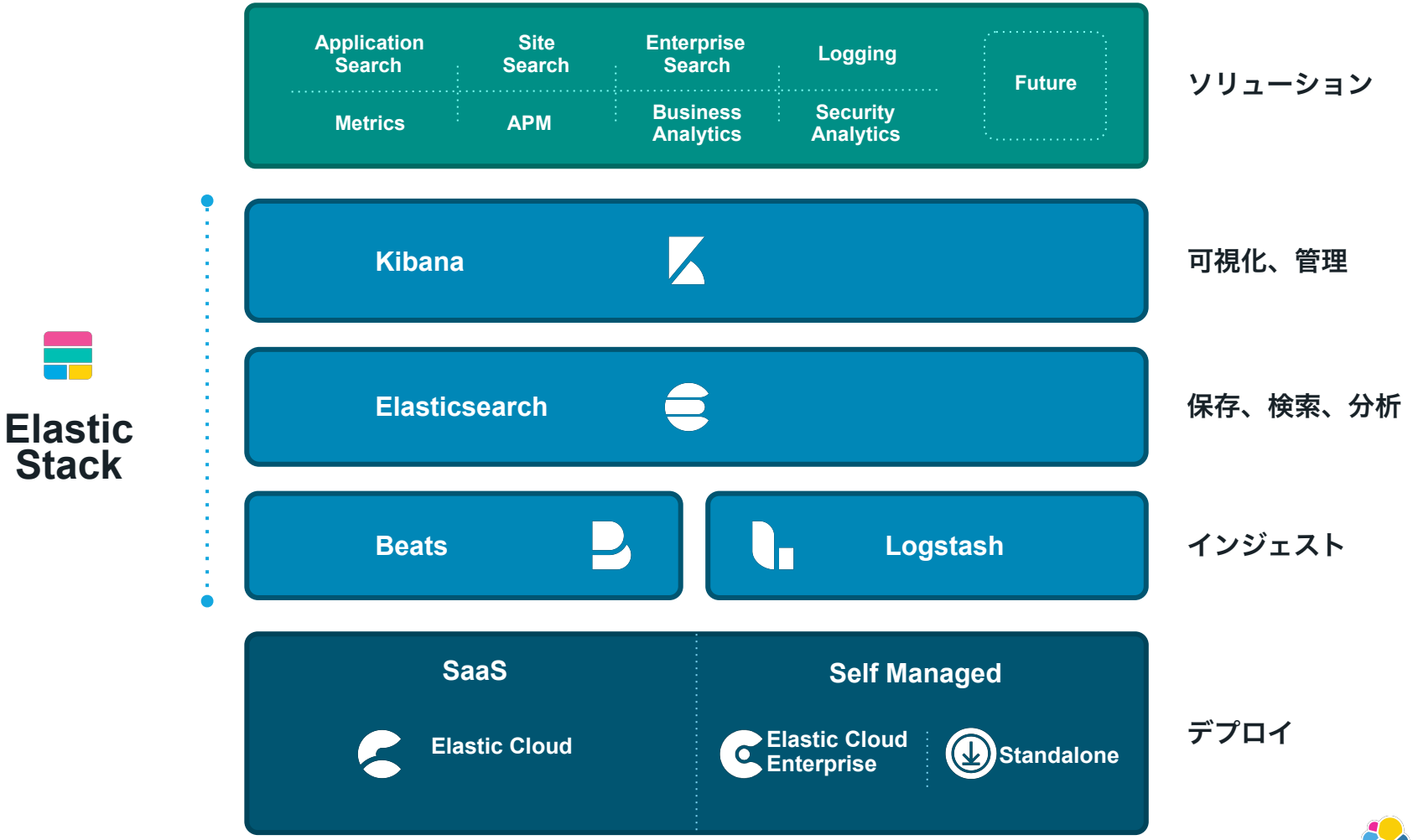
elastic


Application Search
Site Search
Enterprise Search
Logging
Future
Metrics
APM
Business Analytics
Security Analytics
ソリューション
Kibana
可視化、管理
Elasticsearch
保存、検索、分析
Beats
Logstash
インジェスト
Elastic Stack

Elastic Stack

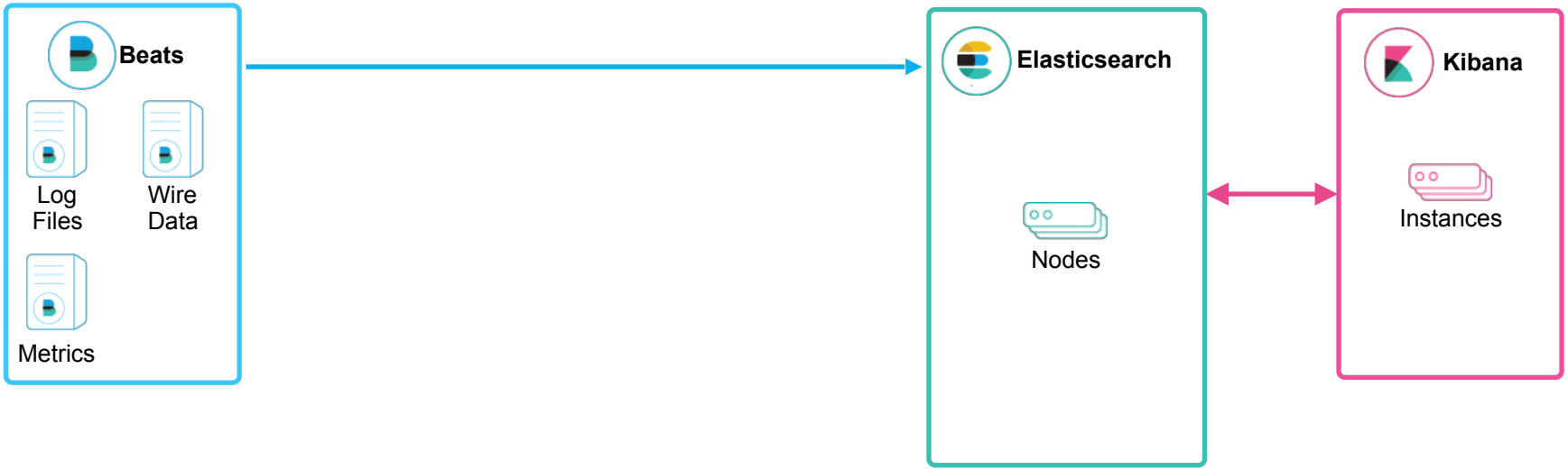
App Search	Site Search	Enterprise Search	Logging	Future	ソリューション
Metrics	APM	Business Analytics	Security Analytics		
Kibana					可視化、管理
Elasticsearch					保存、検索、分析
Beats		Logstash			インジェスト
SaaS		Self Managed			デプロイ
Elastic Cloud		Elastic Cloud Enterprise	Standalone		

elastic


Application Search
Site Search
Enterprise Search
Logging
Future
Metrics
APM
Business Analytics
Security Analytics
ソリューション
Kibana
可視化、管理
Elasticsearch
保存、検索、分析
Beats
Logstash
インジェスト
Elastic Stack
SaaS
Self Managed
Elastic Cloud
Elastic Cloud Enterprise
Standalone
デプロイ

定型のメトリクス/ログ解析を Elastic Stackで

メトリック・ログ分析（簡易版）

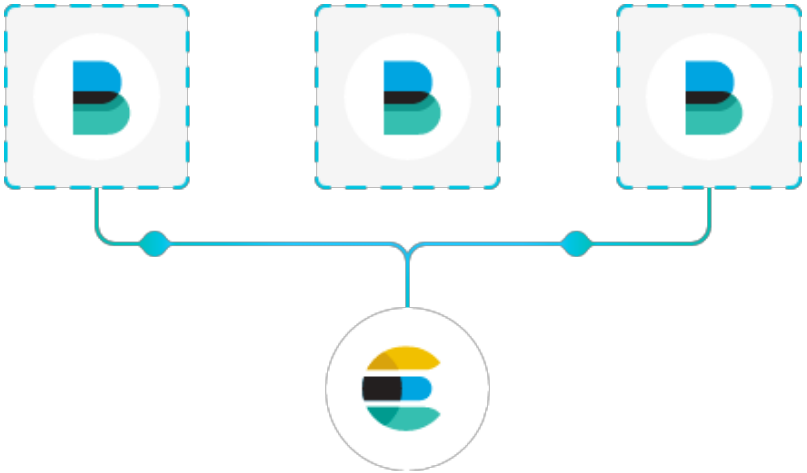


elastic

beats

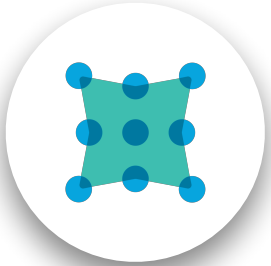
Beats

軽量データシッパー



ソースからデータを転送	転送しElasticsearchに集約	変換とパースのため Logstashに転送
Elastic Cloudに転送	Libbeat: カスタムbeatsのためのAPIフレームワーク	30以上のコミュニティbeats

The Beats family



Packetbeat

Network data

Metricbeat

Metrics

Winlogbeat

Windows Event Logs

Auditbeat

Audit data

Filebeat

Log files

Heartbeat

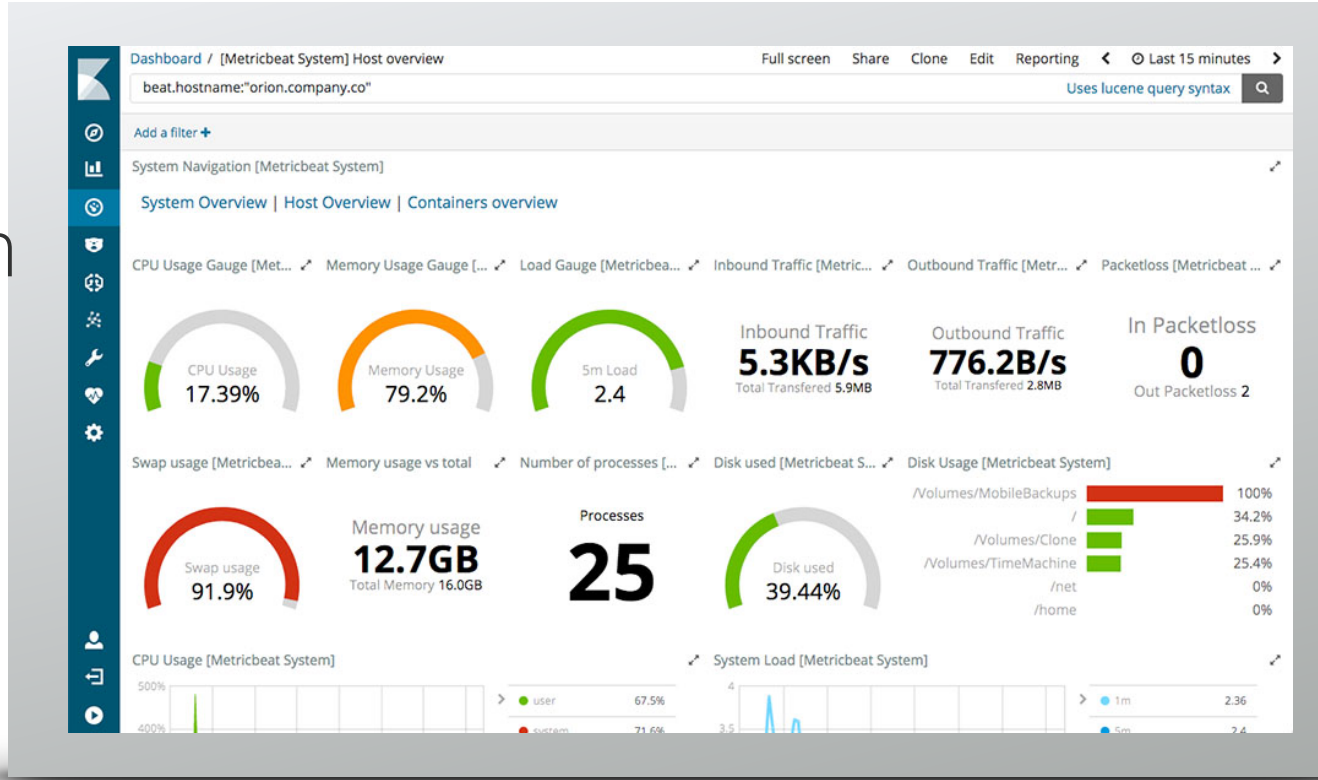
Uptime monitoring

+40 community Beats

elastic

Metricbeat

Collect system and application **metrics**



elastic

Metricbeat

lots of **modules**


System


Apache


Docker

NGINX


HAProxy


Kafka


MongoDB

MySQL


PostgreSQL


Prometheus


Jolokia


Add your own

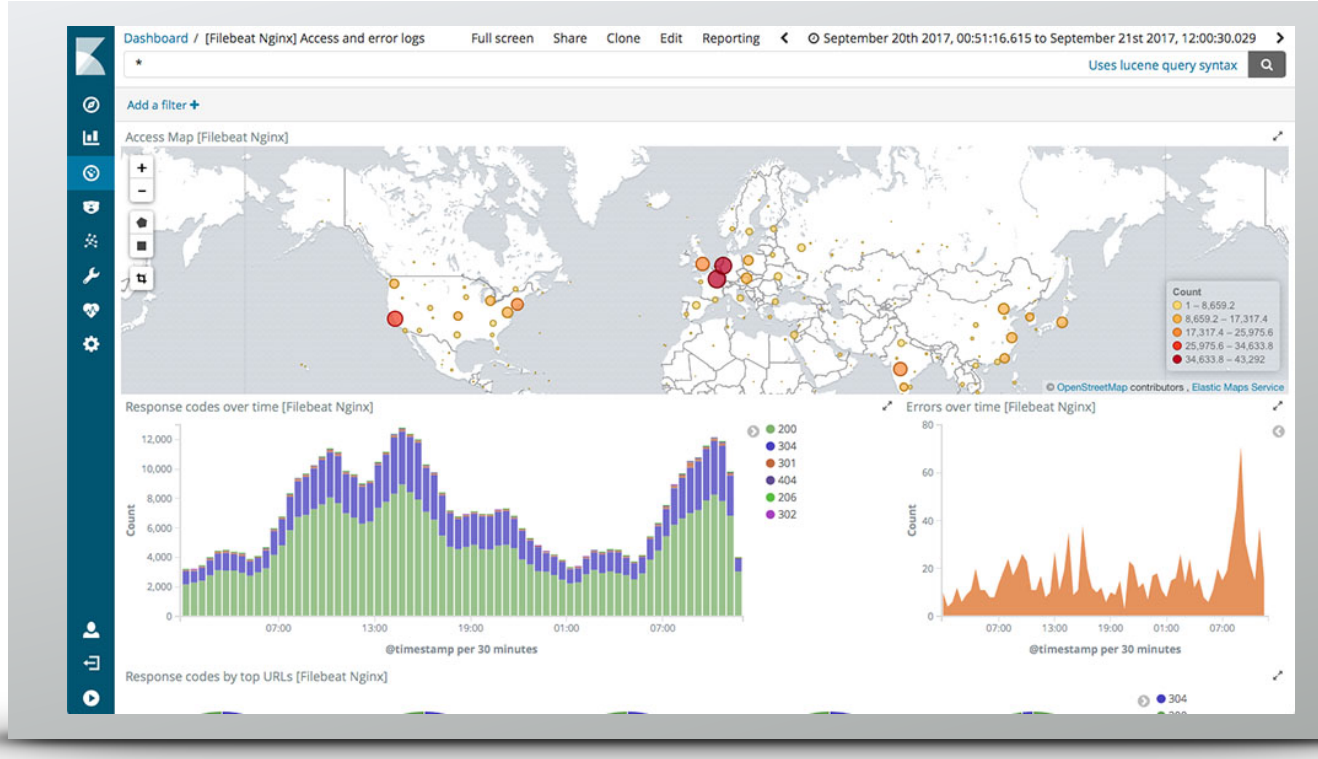
elastic

Metricbeat モジュール

Aerospike module
Apache module
Ceph module
Couchbase module
Docker module
Dropwizard module
Elasticsearch module
Etcd module
Golang module
Graphite module
HAProxy module
HTTP module
Jolokia module
Kafka module
Kibana module
Kubernetes module
kvm module
Logstash module
Memcached module
MongoDB module
Munin module
MySQL module
Nginx module
PHP_FPM module
PostgreSQL module
Prometheus module
RabbitMQ module
Redis module
System module
uwsgi module
vSphere module
Windows module
ZooKeeper module

Filebeat

tail log from
file



elastic

many **modules**

Apache

Nginx

Auditd

MySQL

Filebeat modules - v6.4.2

Apache2 module

Auditd module

Icinga module

IIS module

Kafka module

Logstash module

MongoDB module

MySQL module

Nginx module

Osquery module

PostgreSQL module

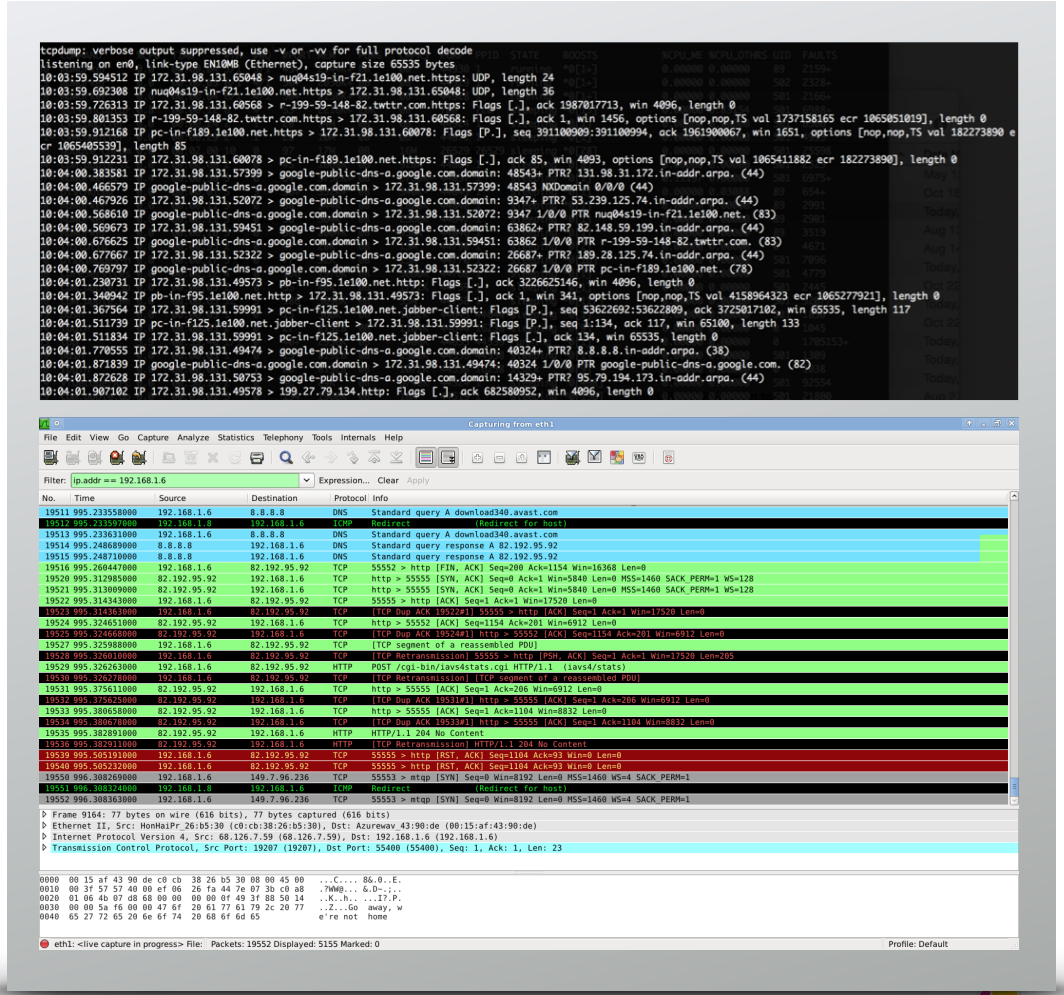
Redis module

System module

Traefik module

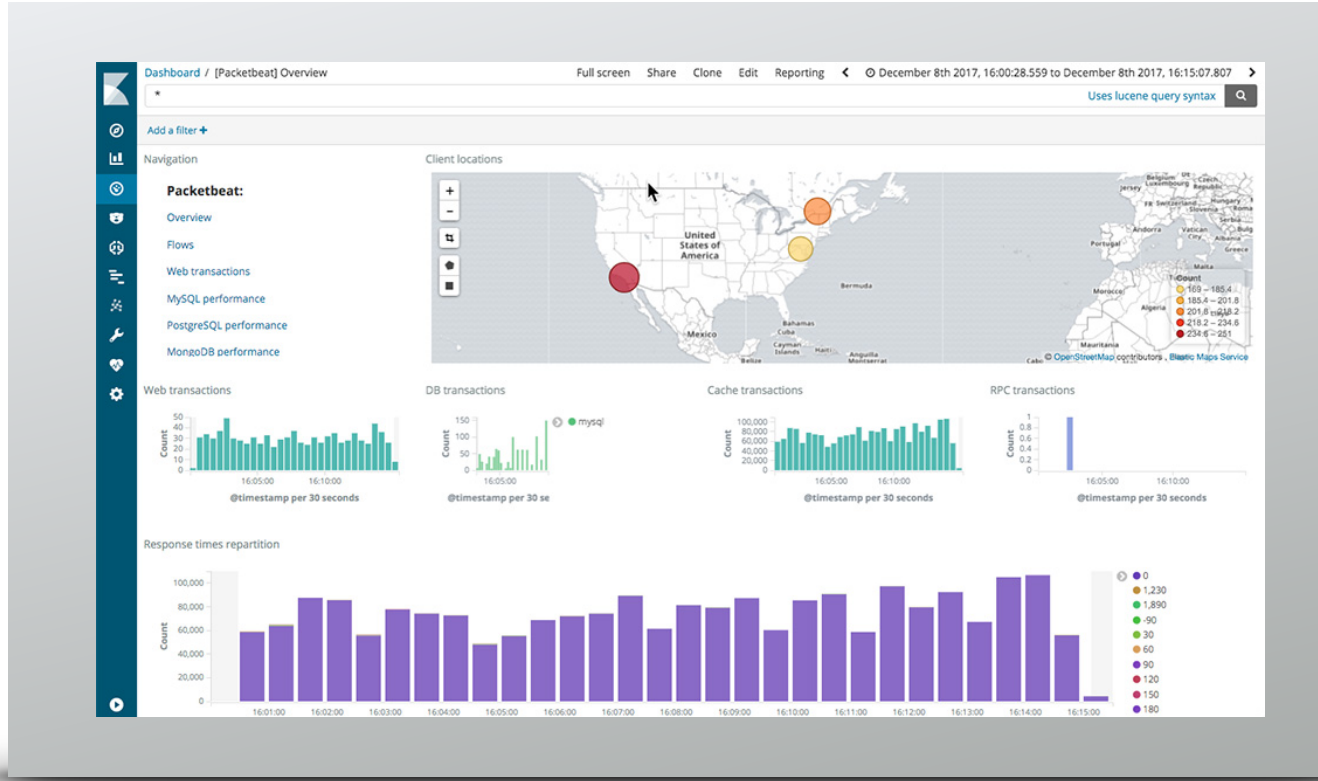
Packetbeat

Capture the **Packet**

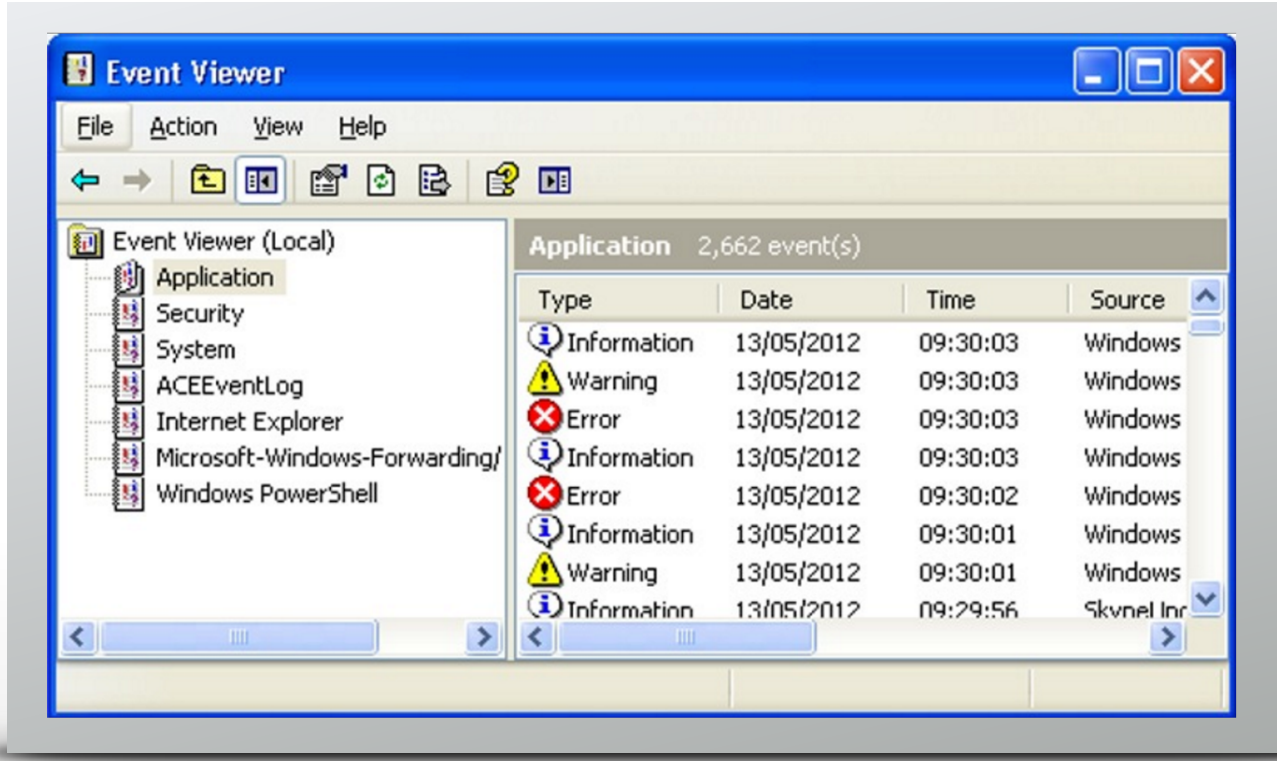


elastic

Capture the **Packet**



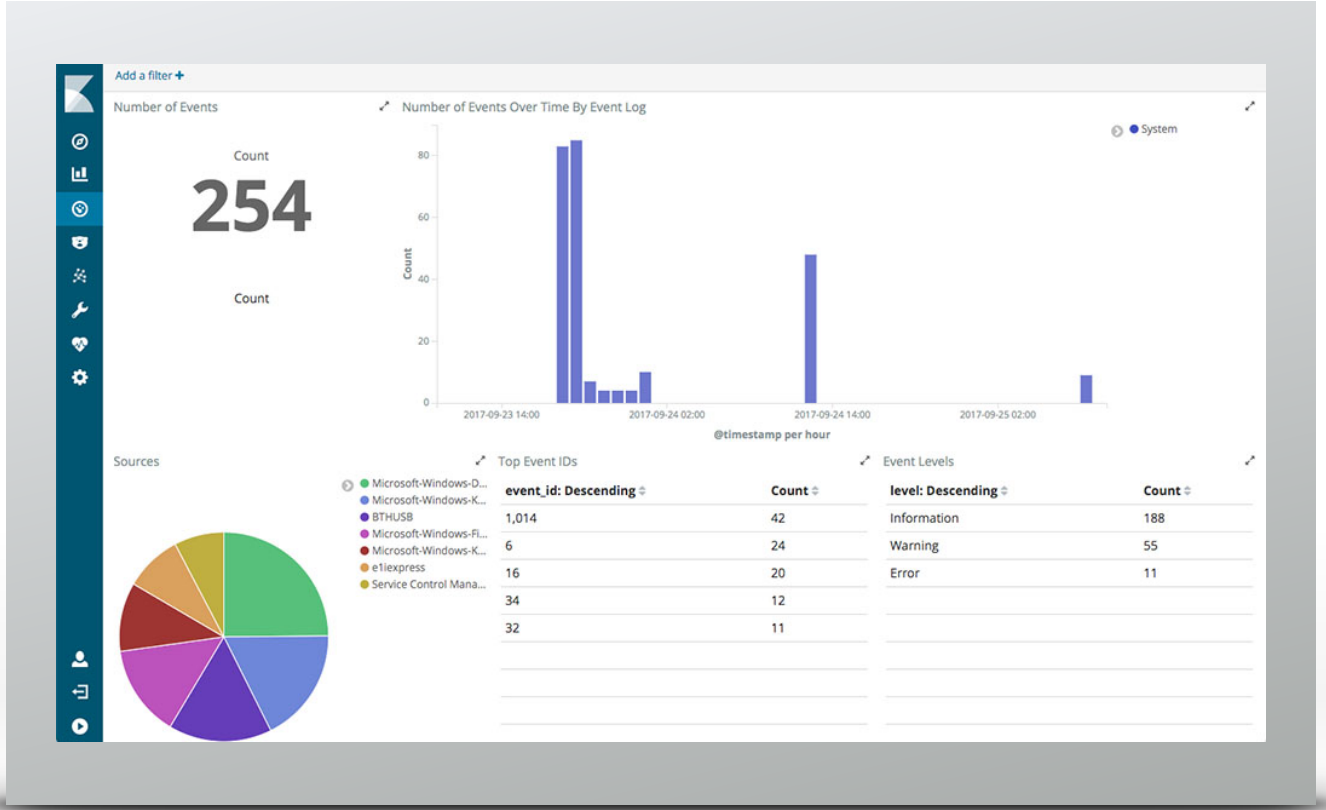
Welcome to **1998**



elastic

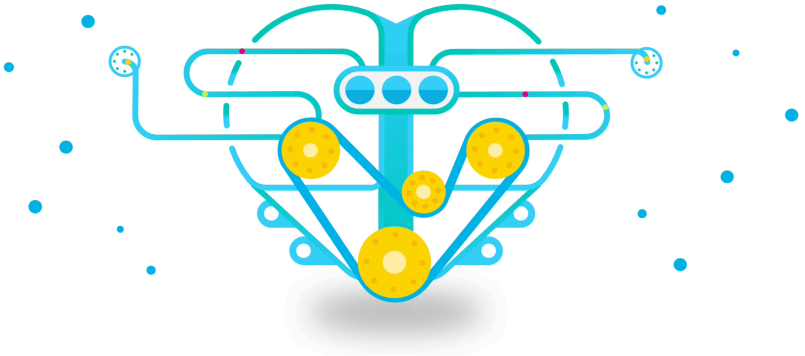
winlogbeat

Now



elastic

elasticsearch



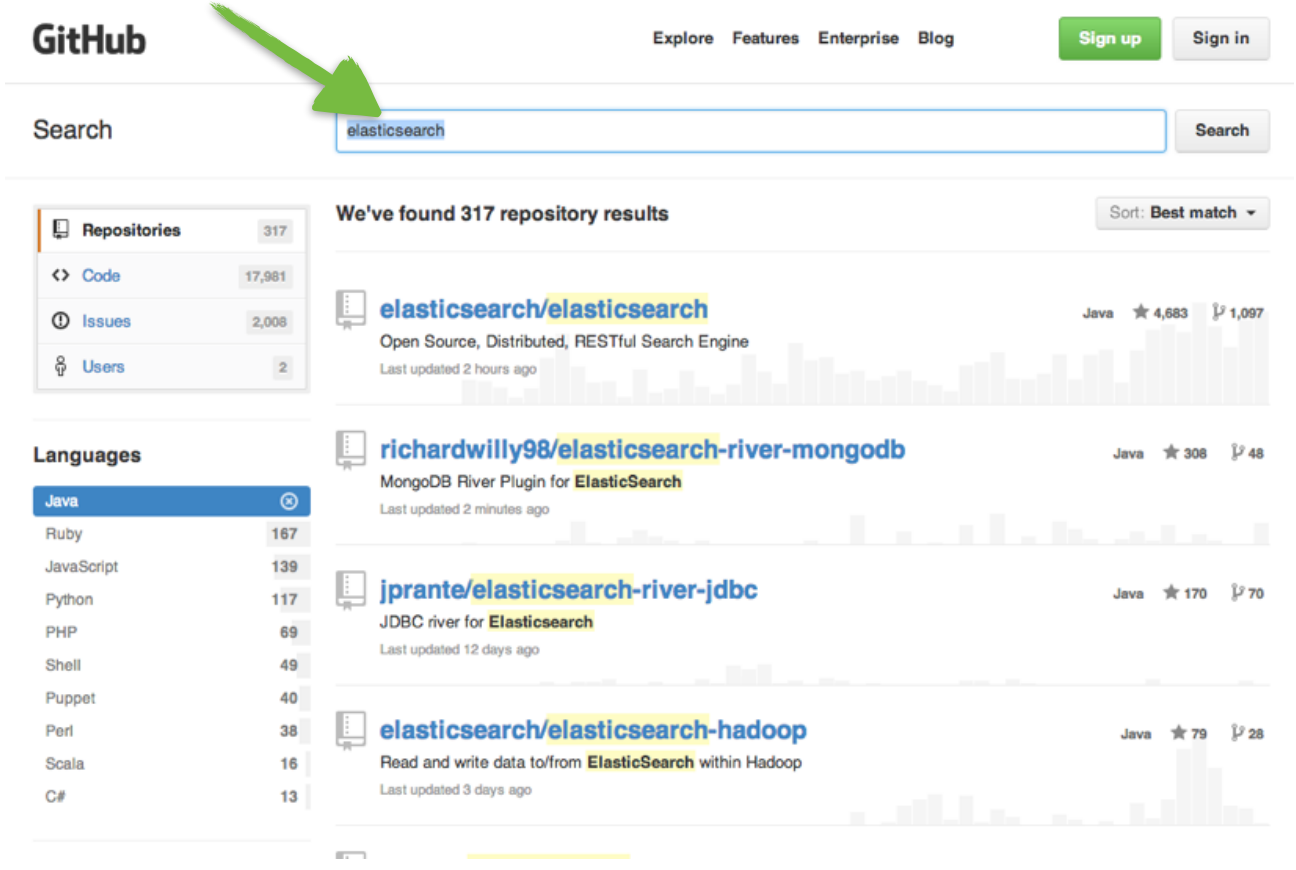
Elasticsearch

Heart of the Elastic Stack

分散型、スケーラブル	高可用性	マルチテナント
開発者フレンドリー	リアルタイム、全文検索	アグリゲーション

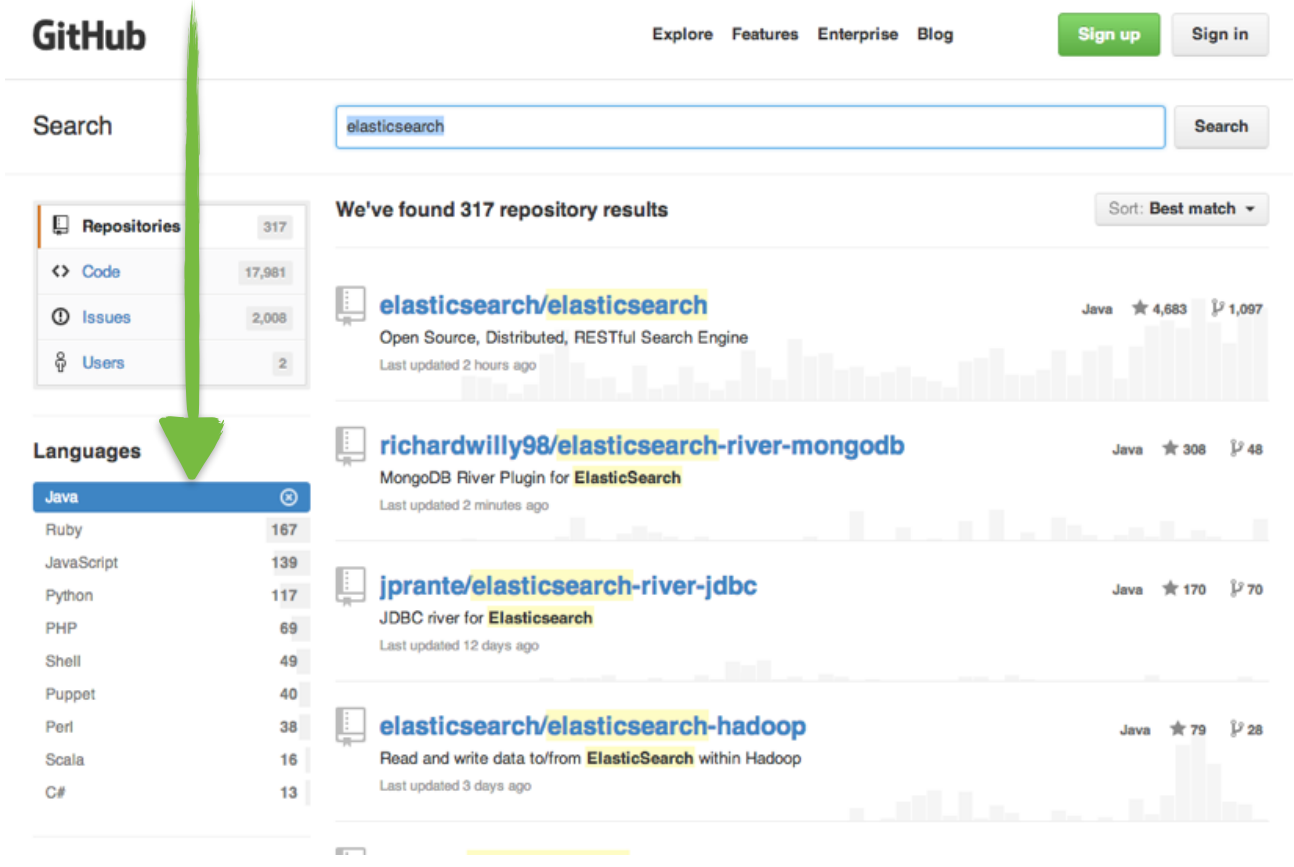
Elasticsearchとは？

フリーワード検索



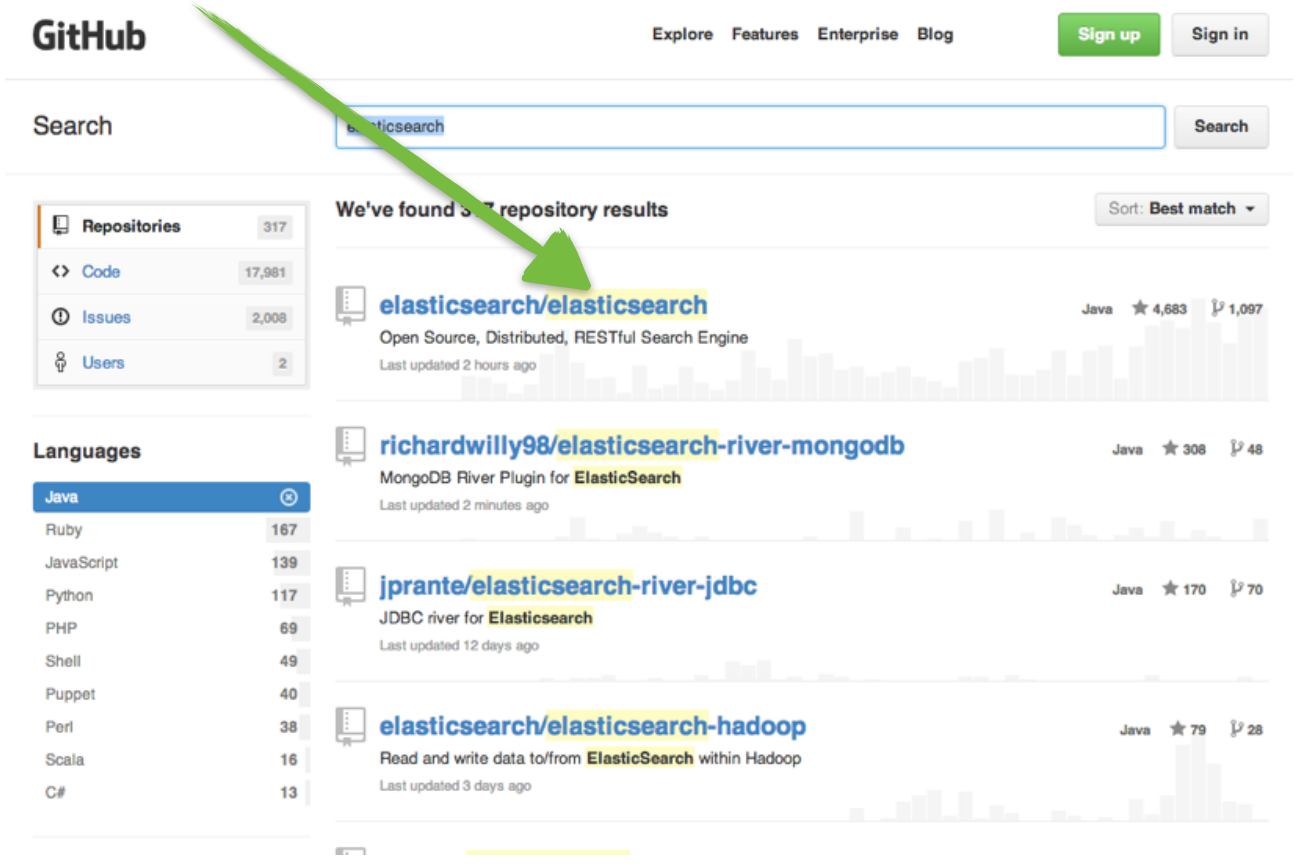
elastic

絞り込み



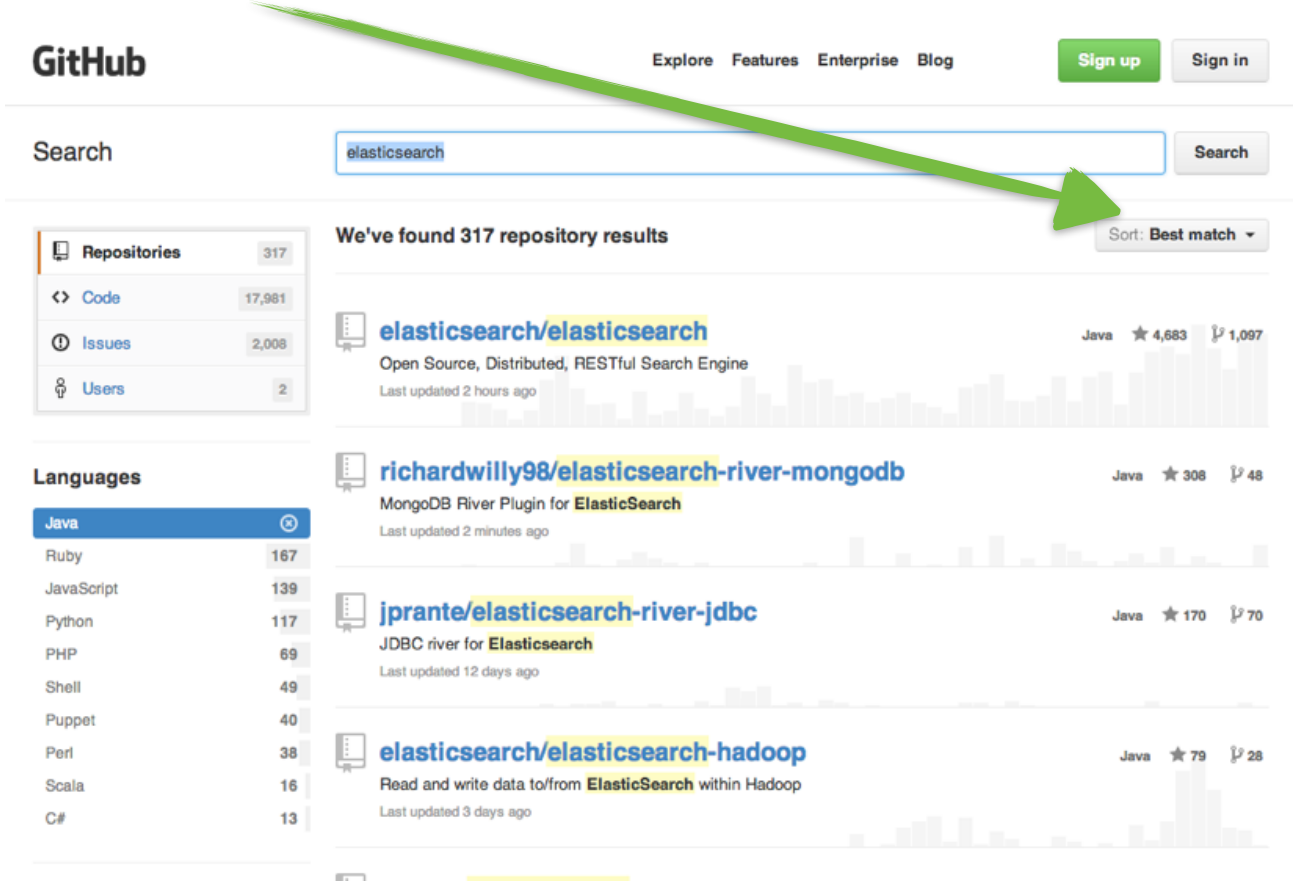
elastic

ハイライト



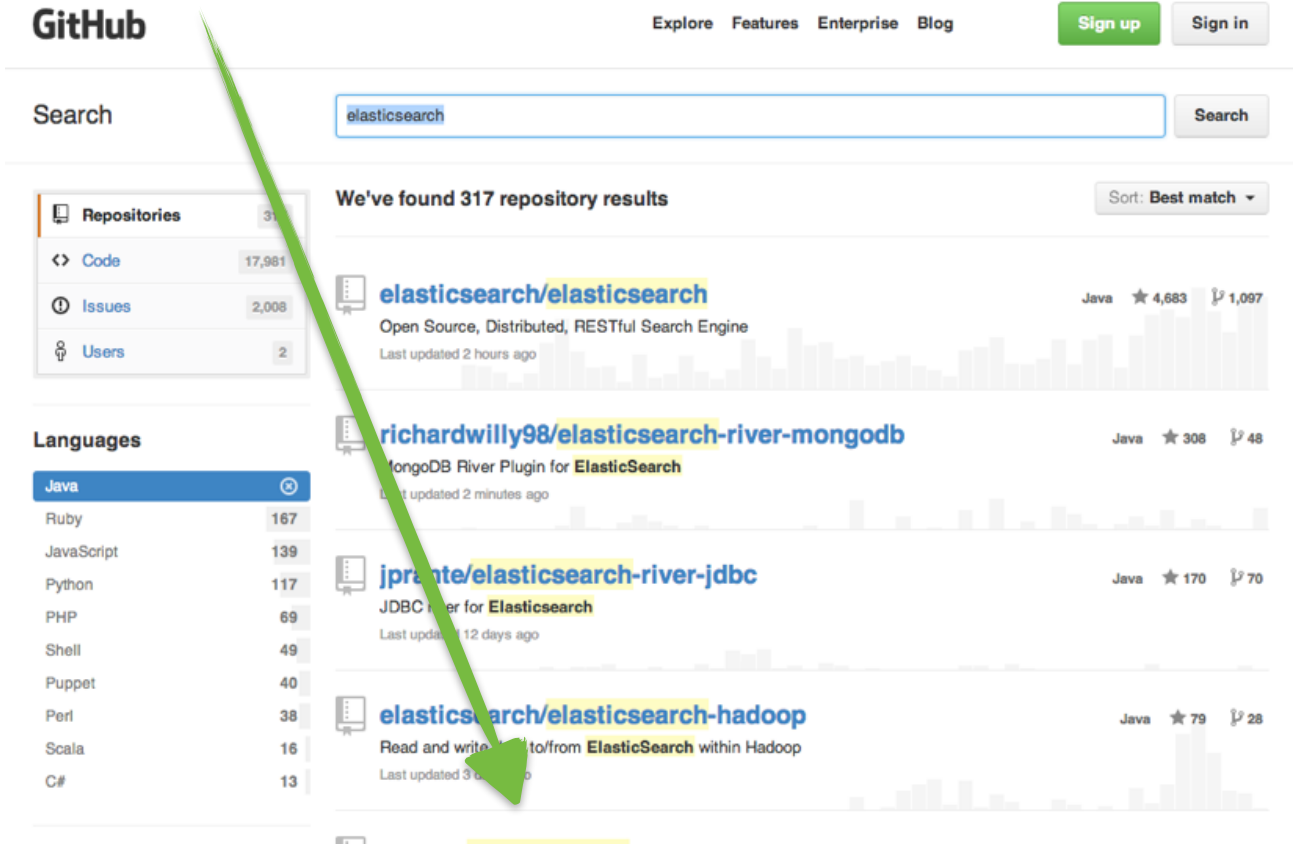
elastic

ソート


GitHub
Explore
Features
Enterprise
Blog
Sign up
Sign in
Search
elasticsearch
Search
Repositories 317
Code 17,981
Issues 2,008
Users 2
We've found 317 repository results
Sort: Best match
elasticsearch/elasticsearch
Open Source, Distributed, RESTful Search Engine
Last updated 2 hours ago
Java 4,683 1,097
richardwilly98/elasticsearch-river-mongodb
MongoDB River Plugin for ElasticSearch
Last updated 2 minutes ago
Java 308 48
jprante/elasticsearch-river-jdbc
JDBC river for Elasticsearch
Last updated 12 days ago
Java 170 70
elasticsearch/elasticsearch-hadoop
Read and write data to/from ElasticSearch within Hadoop
Last updated 3 days ago
Java 79 28
Languages
Java
Ruby 167
JavaScript 139
Python 117
PHP 69
Shell 49
Puppet 40
Perl 38
Scala 16
C# 13

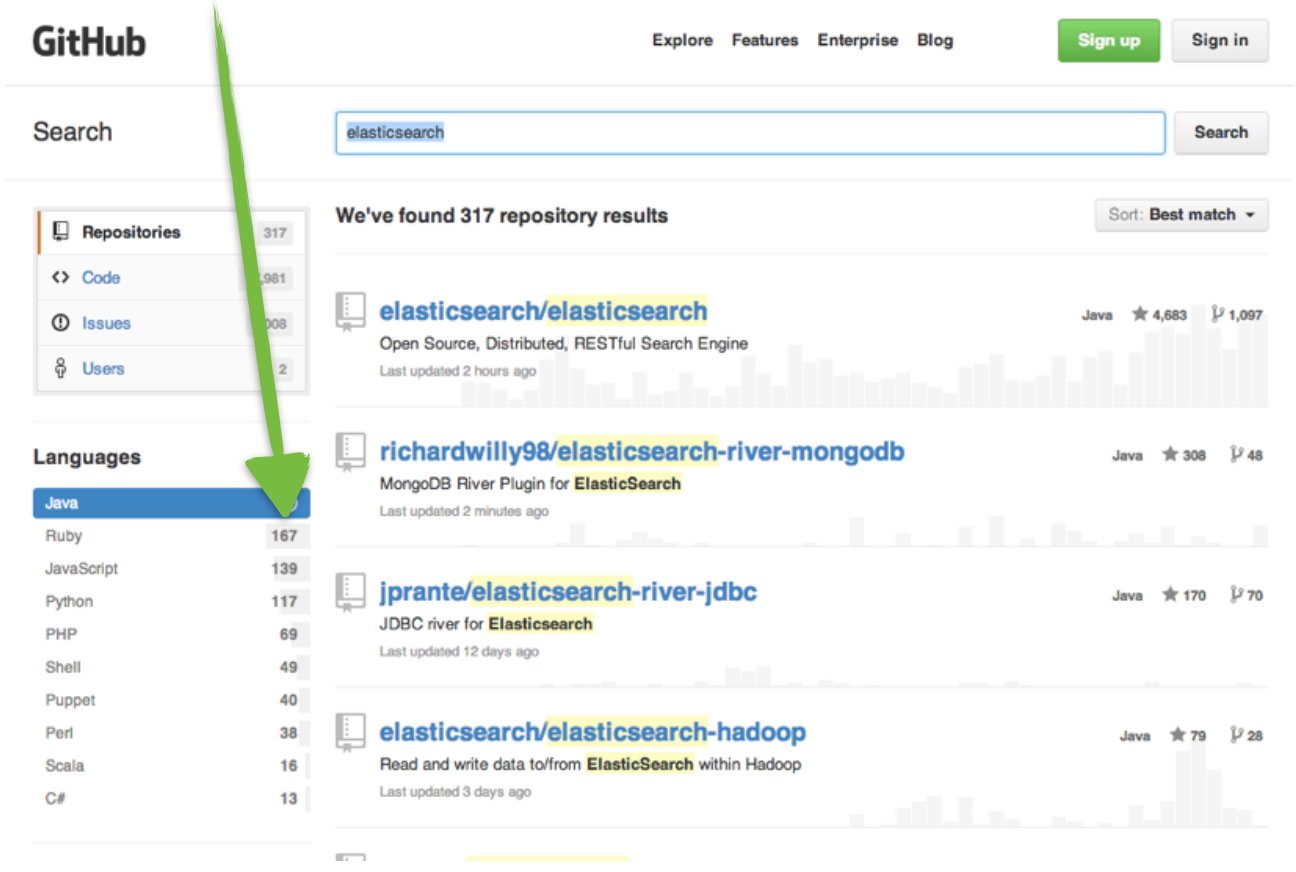
elastic

ページング



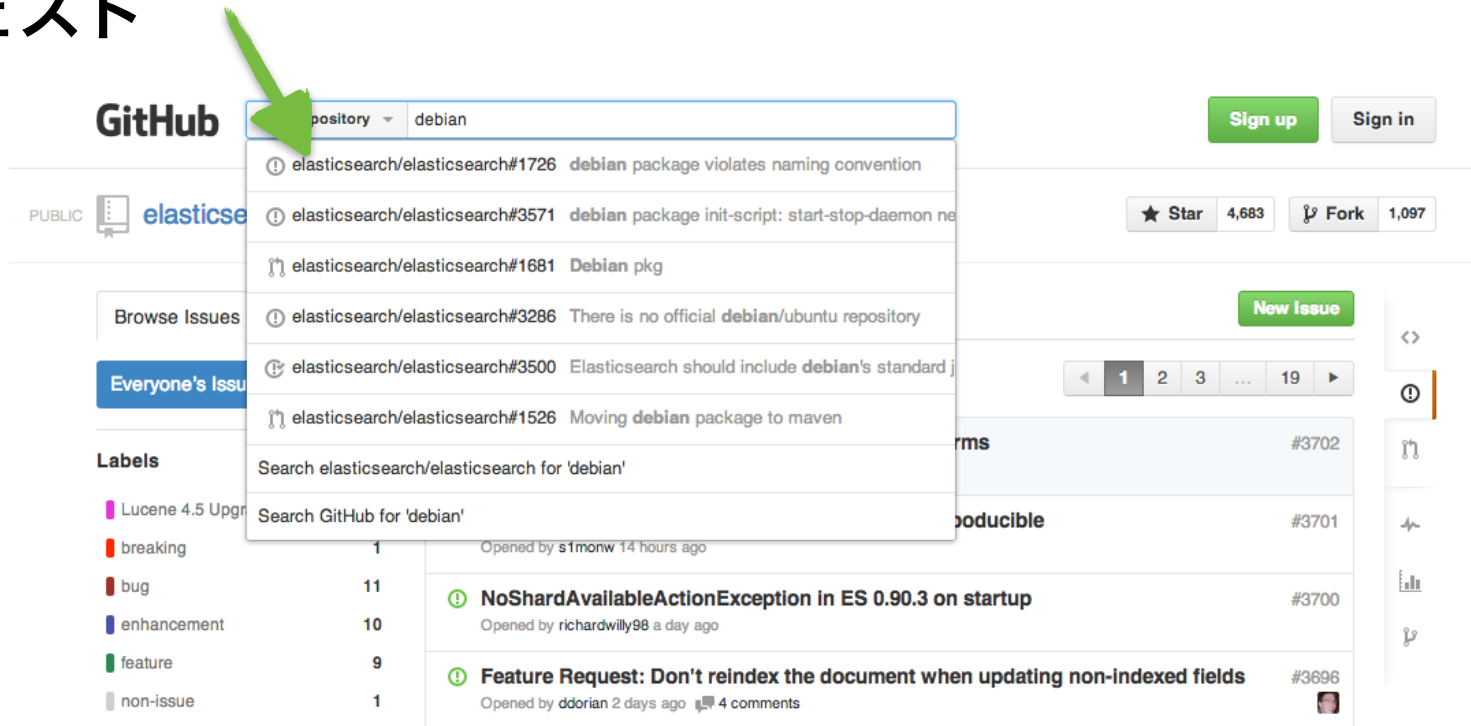
elastic

集計


GitHub
Explore
Features
Enterprise
Blog
Sign up
Sign in
Search
elasticsearch
Search
Repositories 317
Code
Issues
Users
We've found 317 repository results
Sort: Best match
elasticsearch/elasticsearch
Open Source, Distributed, RESTful Search Engine
Last updated 2 hours ago
Java 4,683 1,097
Languages
Java
Ruby 167
JavaScript 139
Python 117
PHP 69
Shell 49
Puppet 40
Perl 38
Scala 16
C# 13
richardwilly98/elasticsearch-river-mongodb
MongoDB River Plugin for ElasticSearch
Last updated 2 minutes ago
Java 308 48
jprante/elasticsearch-river-jdbc
JDBC river for Elasticsearch
Last updated 12 days ago
Java 170 70
elasticsearch/elasticsearch-hadoop
Read and write data to/from ElasticSearch within Hadoop
Last updated 3 days ago
Java 79 28

elastic

サジェスト



elastic

Elasticsearch in 10 seconds

- スキーマフリー、分散ドキュメントストア、REST & JSON
- オープンソース: Apache License 2.0
- 設定なしで簡単に試すことが可能
- Javaで実装。拡張も容易

簡単なCRUD

データ登録

```
curl -XPUT localhost:9200/books/book/1 -d '
{
  "title" : "Elasticsearch - The definitive guide",
  "authors" : "Clinton Gormley",
  "started" : "2013-02-04",
  "pages" : 230
}'
```

データ更新

```
curl -XPUT localhost:9200/books/book/1 -d '
{
  "title" : "Elasticsearch - The definitive guide",
  "authors" : [ "Clinton Gormley", "Zachary Tong" ],
  "started" : "2013-02-04",
  "pages" : 230
}'
```

データ削除

```
curl -X DELETE localhost:9200/books/book/1
```

データの取得

```
curl -X GET localhost:9200/books/book/1
curl -X GET localhost:9200/books/book/1/_source
```

検索 - Query DSL

```
curl –XGET ‘localhost:9200/books/doc/_search' –d '{
  "query": {
    "bool": {
      "must": [
        { "match": { "title":   "Search"        }},
        { "match": { "content": "Elasticsearch" }}
      ],
      "filter": [
        { "term":  { "status": "published" }},
        { "range": { "publish_date": { "gte": "2015-01-01" }}}
      ]
    }
  }
}'
```

分散構成、スケール

Basic terms

- インデックス
  - データの論理的な集合。
    RDBのデータベースのようなものLogical
- レプリケーション
  - 読み込みのスケーラビリティ向上
  - SPOFの解消
- シャーディング
  - 複数マシンへデータを分割
    書き込みのスケーラビリティ向上
    データフロー制御

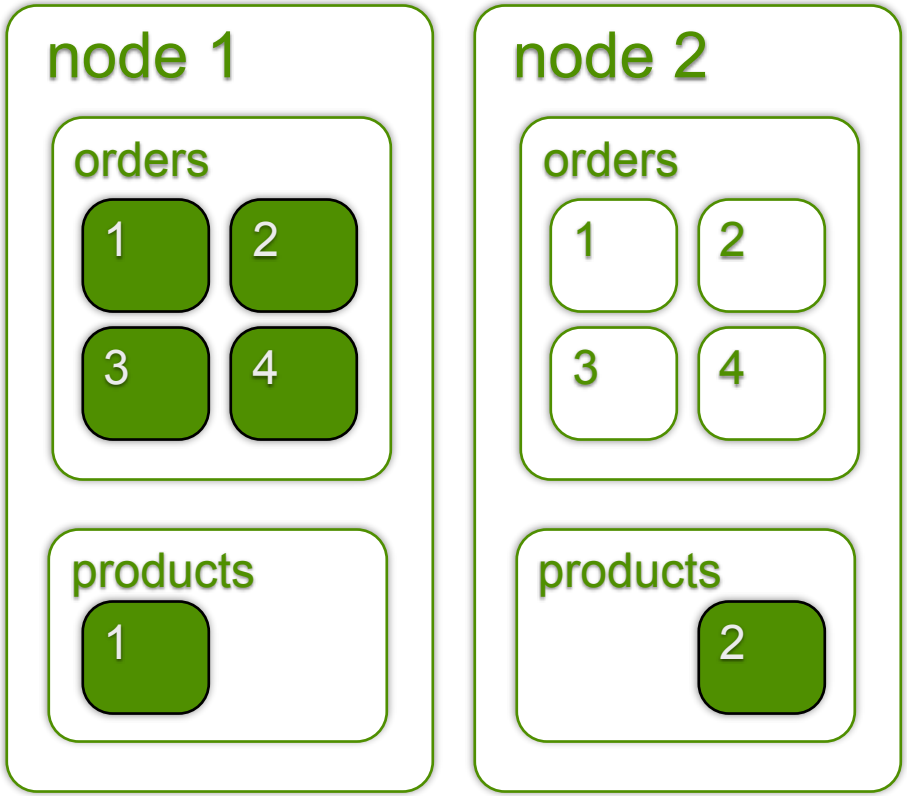
シャードとレプリカ


```
curl -X PUT localhost:9200/orders -d '{
  "settings.index.number_of_shards" : 4
  "settings.index.number_of_replicas" : 1
}'
```

```
curl -X PUT localhost:9200/products -d '{
  "settings.index.number_of_shards" : 2
  "settings.index.number_of_replicas" : 0
}'
```

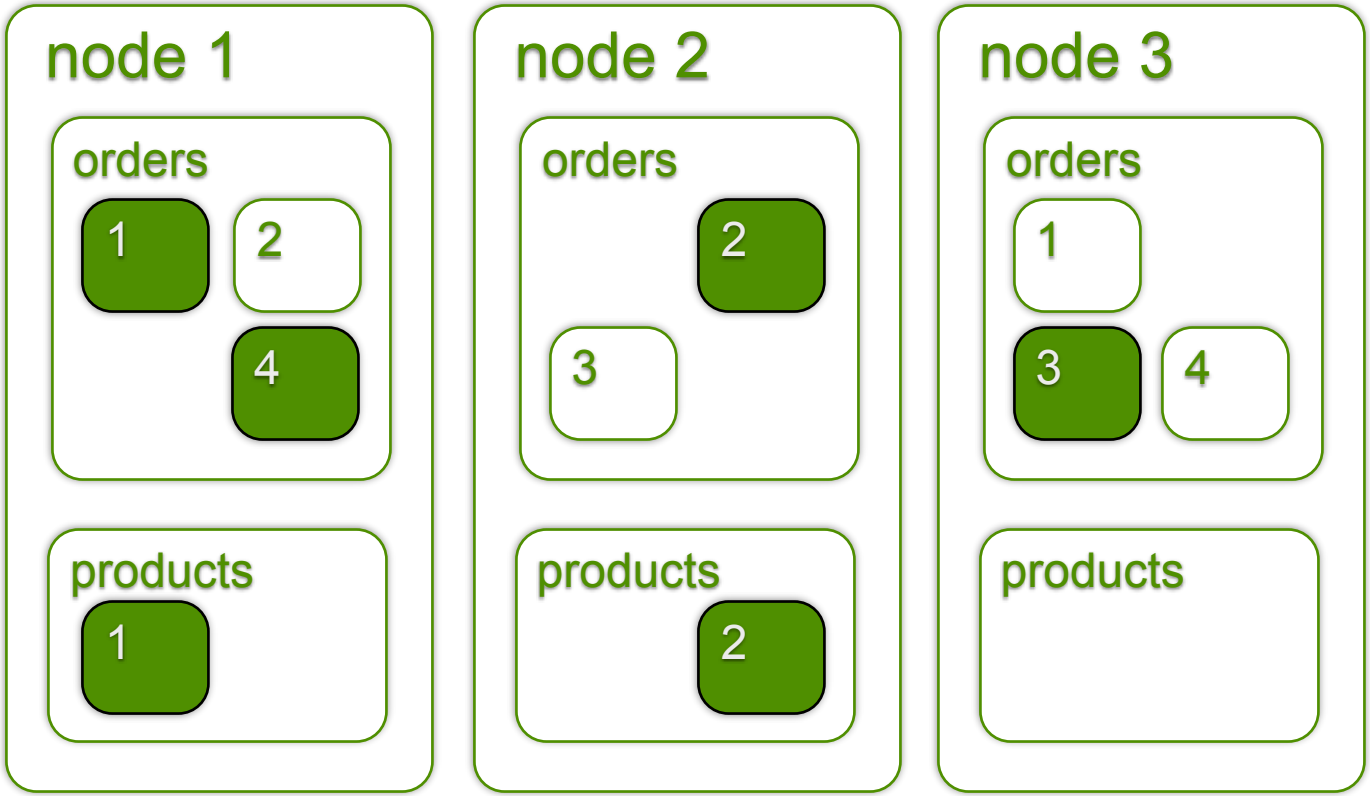

elastic

シャードとレプリカ



elastic

自動的な分散



elastic

全文検索とは？

全文検索とは？

- 全文検索（Full text search）とは、コンピュータにおいて、複数の文書（ファイル）から特定の文字列を検索すること。「ファイル名検索」や「単一ファイル内の文字列検索」と異なり、「複数文書にまたがって、文書に含まれる全文を対象とした検索」という意味で使用される。（Wikipediaより）

用語

- インデックス

  検索エンジンが検索に使用するデータの保存先

- ドキュメント（文書）
  - 検索エンジンに保存されたデータ
- フィールド
  - ドキュメントに含まれる属性
- クエリ
  - 検索条件、検索式

用語

- スキーマ
  - ドキュメントの構造を定義するもの
- ターム（Term）、トークン（Token）
  - インデックスのキーになる単語（文字列）
  - 文章を一定の法則で区切った単語
  - 単語だけでなく、単語の位置なども含む

ドキュメントの登録

1	カツオはサザエの弟
2	サザエはワカメの姉

ドキュメントの登録

ドキュメントの登録

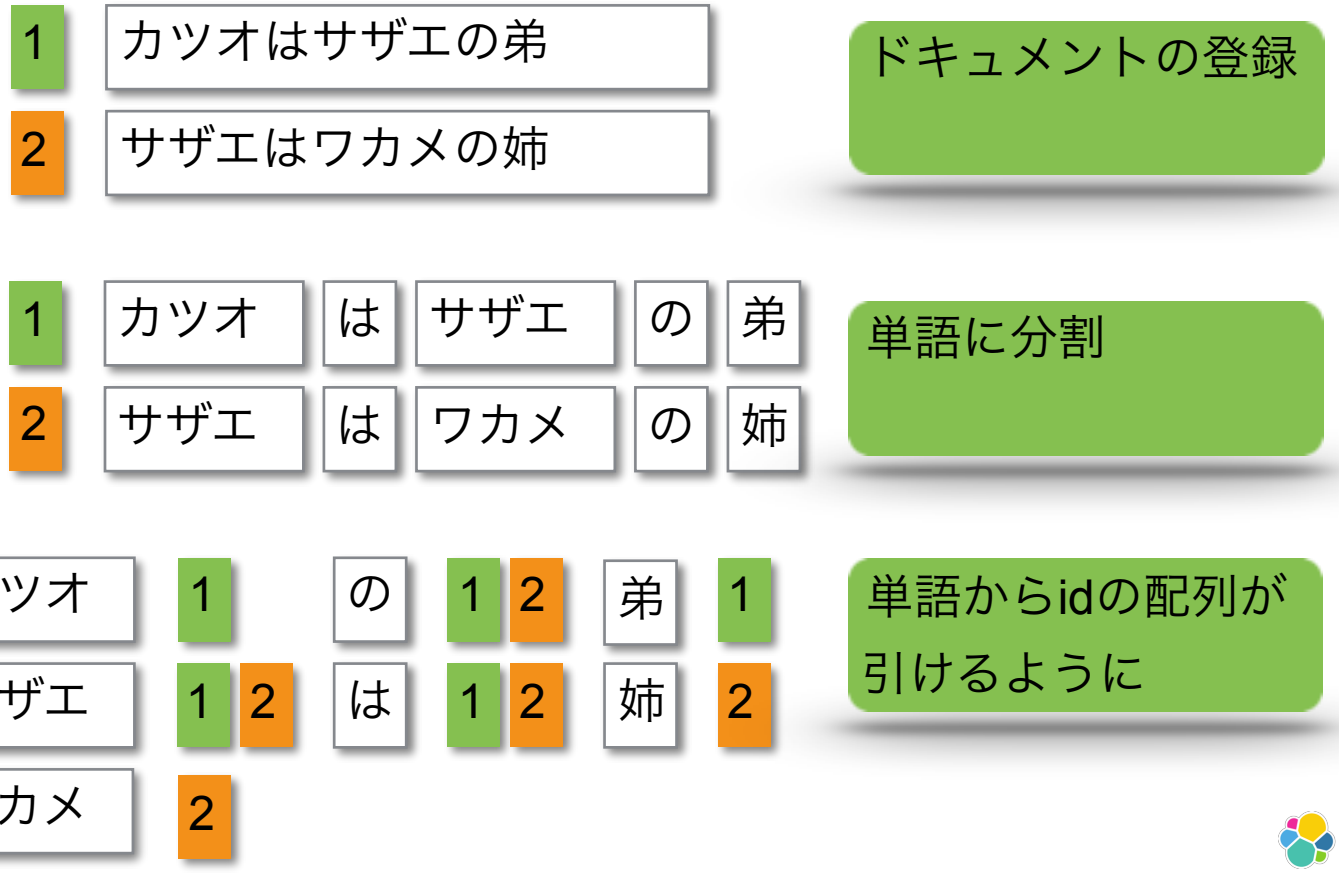
1	カツオはサザエの弟
2	サザエはワカメの姉

ドキュメントの登録

1	カツオ	は	サザエ	の	弟
2	サザエ	は	ワカメ	の	姉

単語に分割

ドキュメントの登録

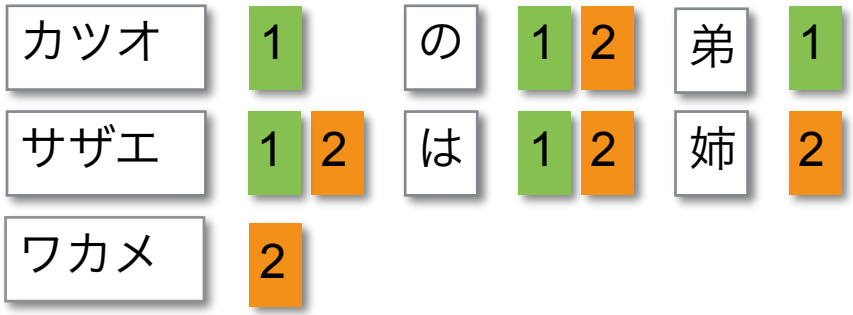


elastic

検索

カツオ　サザエ

検索条件入力



elastic

検索

カツオ　サザエ

検索条件入力

カツオ　AND　サザエ

検索条件のパース
検索クエリ化

カツオ	1		の	1	2	弟	1
サザエ	1	2	は	1	2	姉	2
ワカメ	2						

検索

カツオ　サザエ

検索条件入力

カツオ AND サザエ

検索条件のパース
検索クエリ化

カツオ	1	の	1	2	弟	1	
サザエ	1	2	は	1	2	姉	2
ワカメ	2						

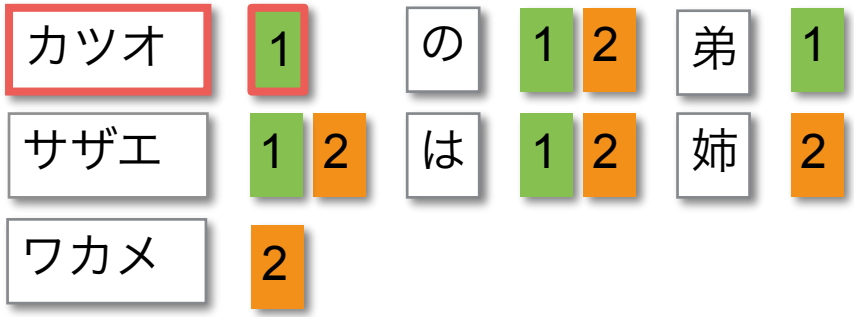
検索

カツオ　サザエ

検索条件入力

カツオ AND サザエ

検索条件のパース
検索クエリ化



elastic

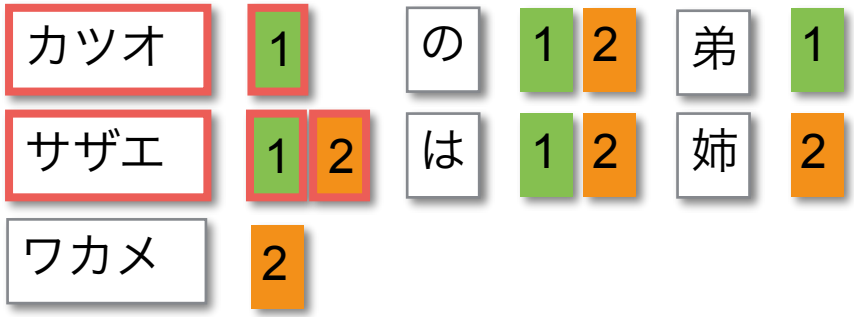
検索

カツオ　サザエ

検索条件入力

カツオ AND サザエ

検索条件のパース
検索クエリ化



elastic

検索

カツオ　サザエ

検索条件入力

カツオ　AND　サザエ

検索条件のパース
検索クエリ化

カツオ	1		の	1	2	弟	1
サザエ	1	2	は	1	2	姉	2
ワカメ	2						

検索

カツオ　サザエ

検索条件入力

カツオ　AND　サザエ

検索条件のパース
検索クエリ化

カツオ	1		の	1	2	弟	1
サザエ	1	2	は	1	2	姉	2
ワカメ	2						

単語の区切り方

- 英語の場合

  I am speaking Introduction Elasticsearch.

- 日本語の場合

  私は入門Elasticsearchについて話している。

単語の区切り方

- 英語の場合

  I am speaking Introduction Elasticsearch.

  スペースが切れ目とわかる

- 日本語の場合

  私は入門Elasticsearchについて話している。

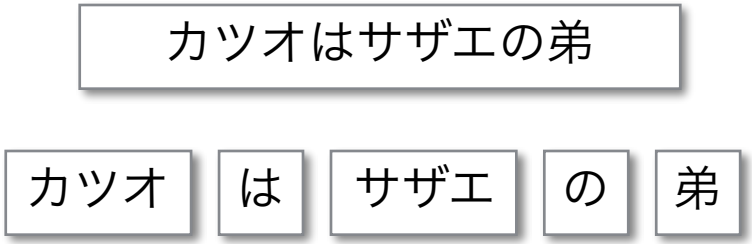
  

  どこで区切ればよい？

N-Gramと形態素解析

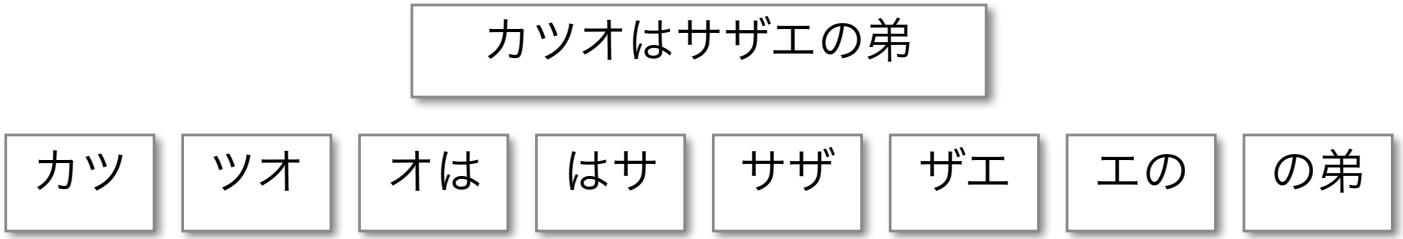
- 転置インデックスのキーの作り方
  - 日本語は単語の切れ目がわからないので、転置インデックスのキーは主に次の２つの手法で作成
- N-Gram
  - N文字ずつ文章を区切る
- 形態素解析
  - 辞書などを用いて意味のある単語で区切る

形態素解析



- メリット：
  - 意味のある単語の切れ目
    品詞情報を元に追加処理が可能（語幹変換など）
- デメリット：
  - 新語（未知語）に弱い→辞書ベースの場合、辞書にない単語は検出不能。

N-Gram



- メリット：
  - 未知語に対応可能
- デメリット：
  - インデックス肥大化
  - 品詞情報に基づく処理が不可能

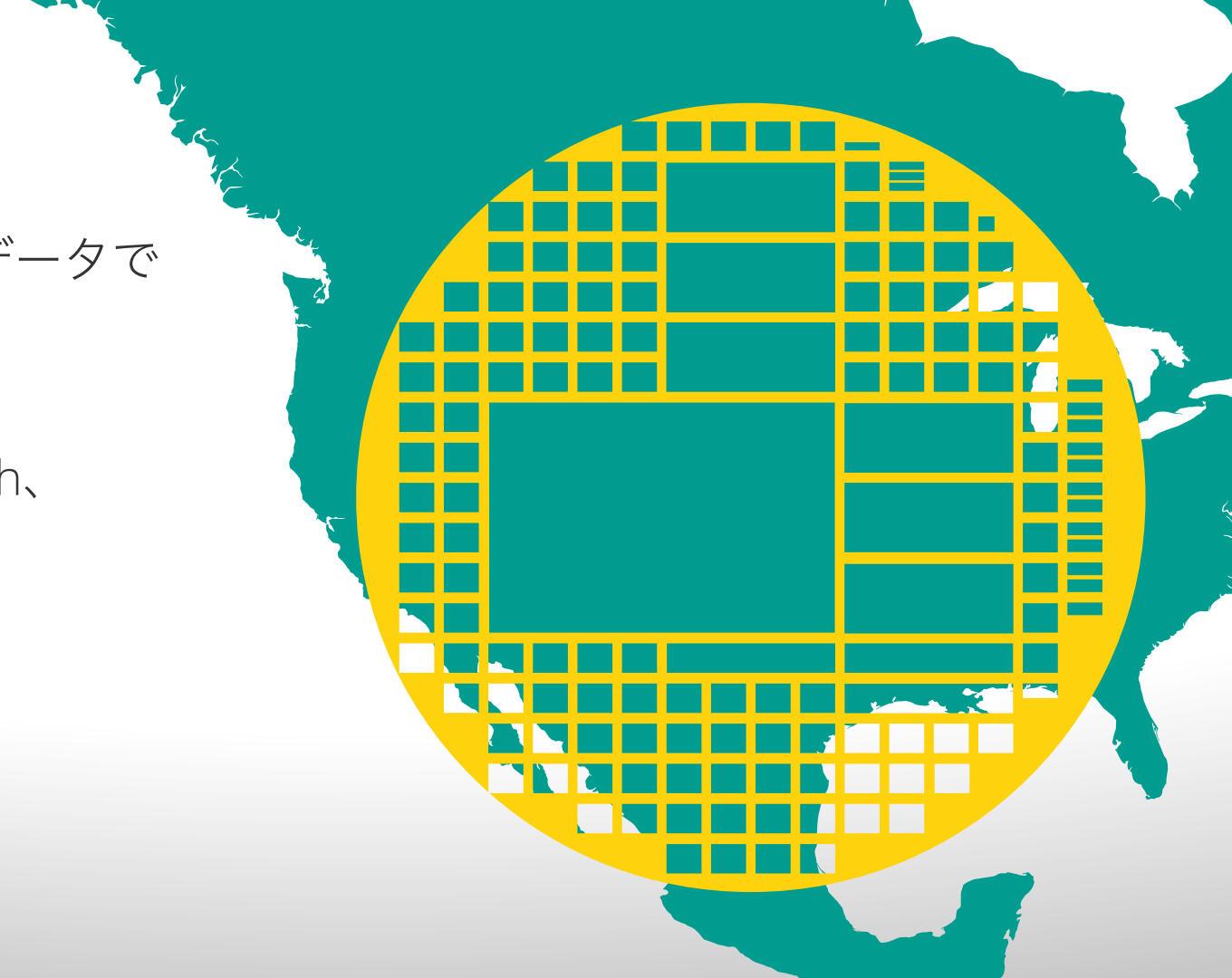
elastic

その他の機能

GEO

さまざまな形式のデータで
Geo検索可能

緯度経度、GeoHash、
GeoShape...



elasticsearch

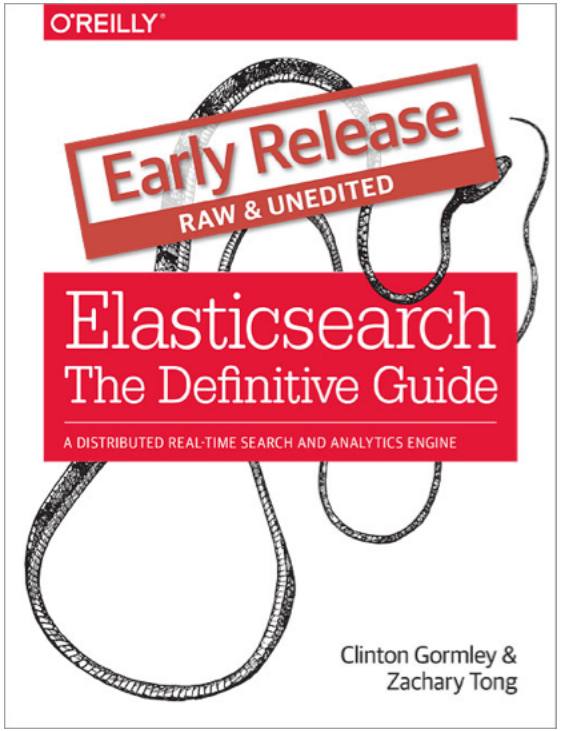
Ecosystem

- Plugins
  - プラグインによる機能の追加
- クライアントライブラリ
  - Java, Ruby, python, php, perl, javascript, .NET
  - Scala, clojure, go

詳しく知りたい方は

Elasticsearch – The Definitive guide

http://www.elastic.co/guide/en/elasticsearch/guide/current/index.html



elastic

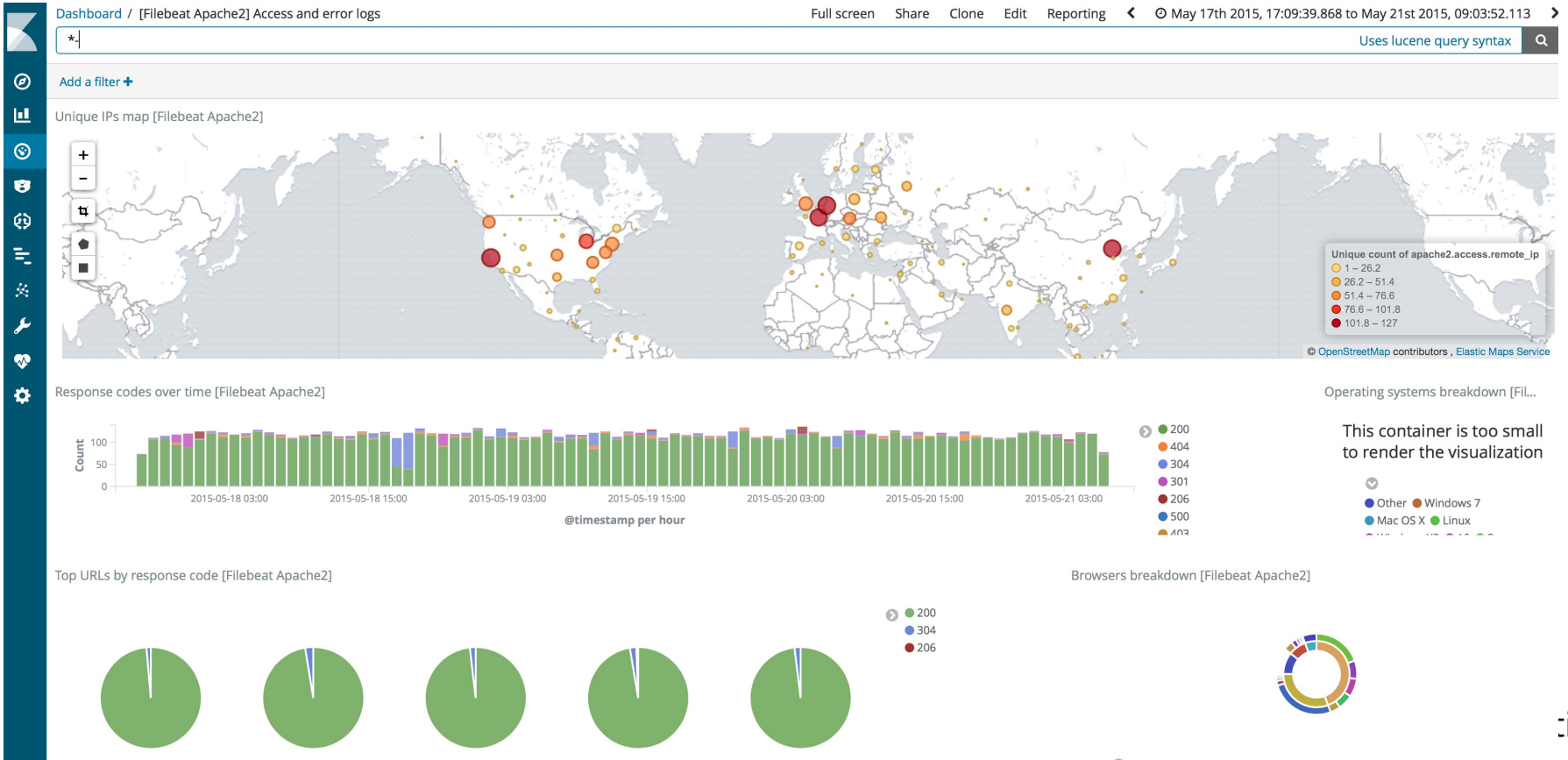
kibana

Kibana

Window into the Elastic Stack

可視化と分析	地理空間	カスタマイズと レポートの共有
グラフ探索	Elastic Stackへの セキュアなアクセスと管理	カスタムAppsの作成

Kibana 6

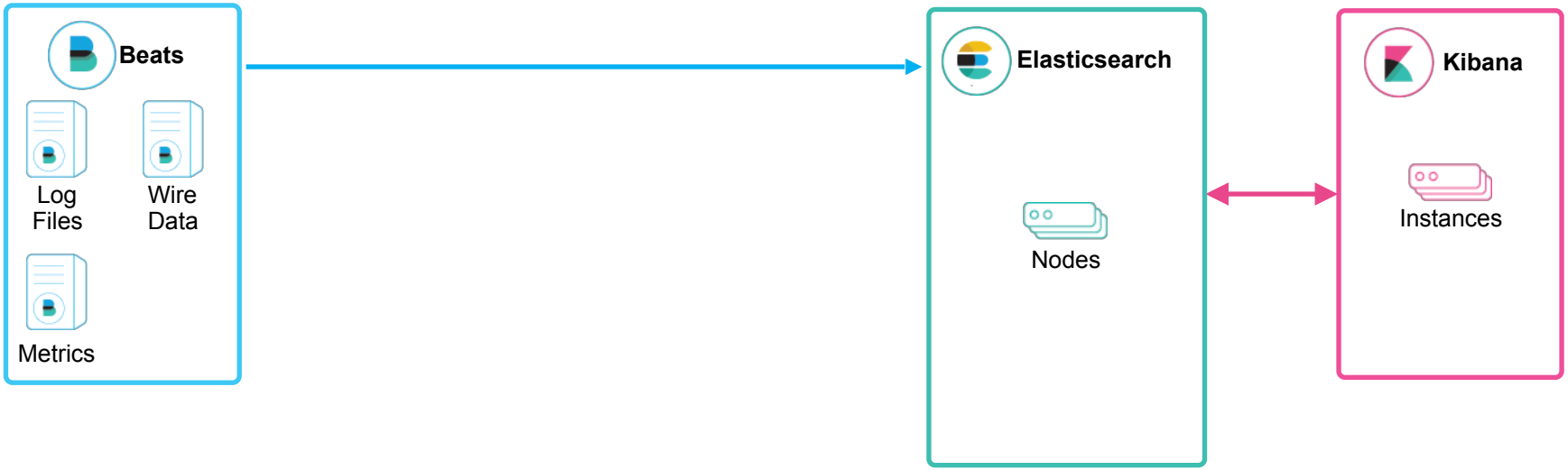

Dashboard / [Filebeat Apache2] Access and error logs
Full screen
Share
Clone
Edit
Reporting
May 17th 2015, 17:09:39.868 to May 21st 2015, 09:03:52.113
*
Uses lucene query syntax
Add a filter +
Unique IPs map [Filebeat Apache2]
Unique count of apache2.access.remote_ip
1 – 26.2
26.2 – 51.4
51.4 – 76.6
76.6 – 101.8
101.8 – 127
© OpenStreetMap contributors , Elastic Maps Service
Response codes over time [Filebeat Apache2]
Count
100
50
0
2015-05-18 03:00
2015-05-18 15:00
2015-05-19 03:00
2015-05-19 15:00
2015-05-20 03:00
2015-05-20 15:00
2015-05-21 03:00
@timestamp per hour
200
404
304
301
206
500
Operating systems breakdown [Fil...
This container is too small to render the visualization
Other
Windows 7
Mac OS X
Linux
Top URLs by response code [Filebeat Apache2]
200
304
206
Browsers breakdown [Filebeat Apache2]

デモ

データ投入から可視化まで

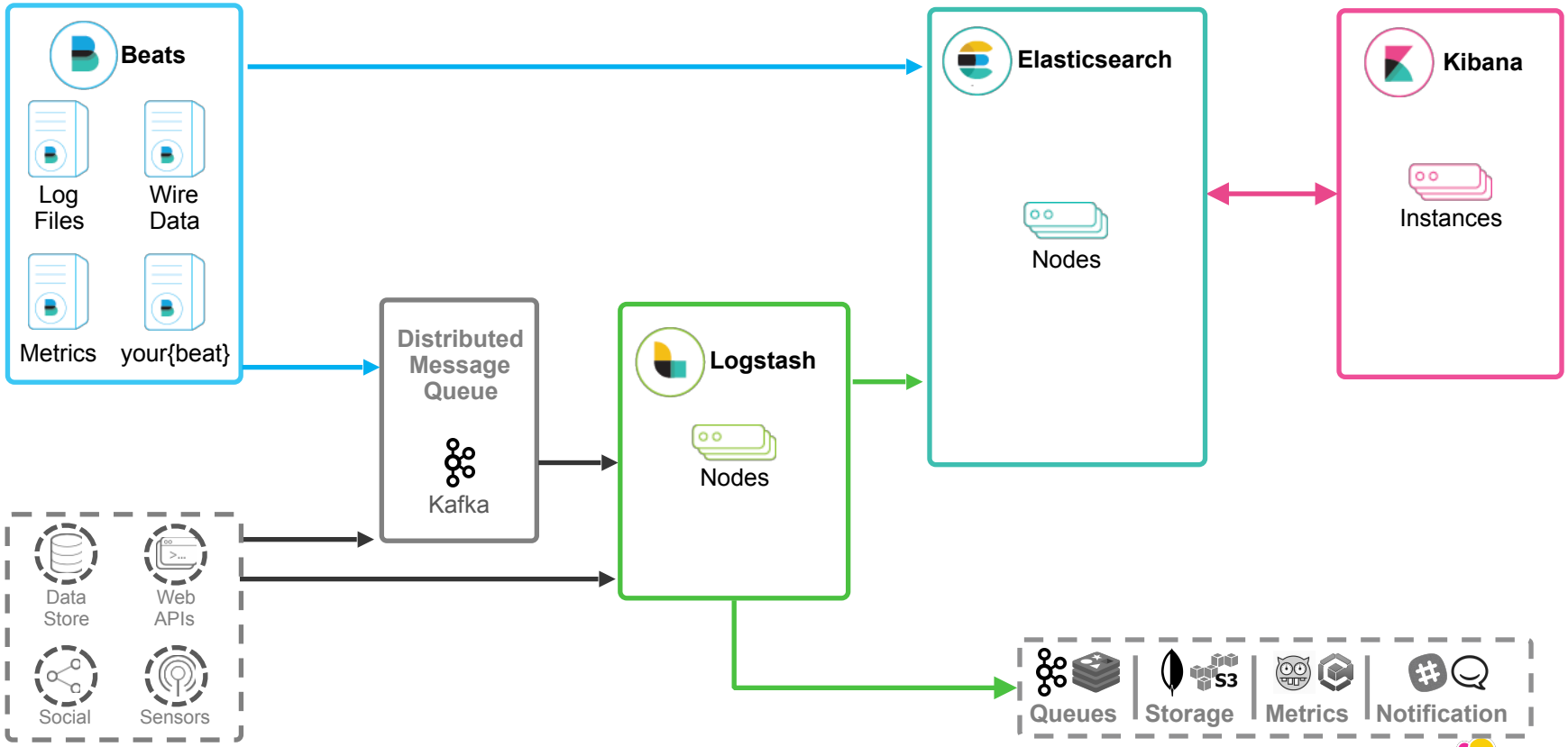
本格的に解析を行うには？

Elastic Stackの構成



elastic

Elastic Stackの構成

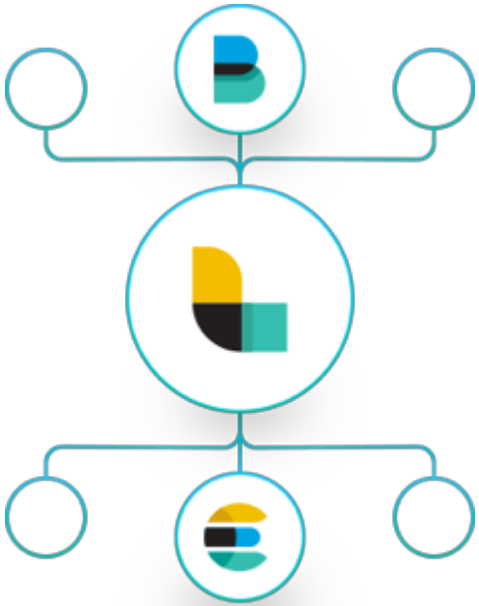


elastic

logstash

Logstash

データ加工パイプライン



全ての形式、サイズとデータソースの投入	パースと動的なデータ変換	あらゆる出力にデータ転送
安全で暗号化されたデータ入力	独自のパイプライン処理の作成	200以上のプラグイン

Logstash in 10 seconds

- ログ・データの収集・管理
- 収集、パース・加工、送出
- オープンソース：Apache License 2.0
- Ruby app (JRuby)

elastic

Logstash architecture

Input

collect and split

Filter

alter and enrich

Output

store and visualize

elastic

設定

```
input {
  …
}

filter {
  …
}

output {
  …
}
```

設定：input

```
input {
  file {
    path => “/Users/johtani/sample/*_log"
    start_position => "beginning"
  }
}
```

1行1データ

189.120.xx.xx - - [02/Dec/2014:12:18:29 +0900] "GET /manager/html HTTP/1.1" 404 274 "-" "Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0"

設定：filter

```
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
    break_on_match => false
  }
  date {
    match => ["timestamp", "dd/MMM/YYYY:HH:mm:ss Z"]
    locale => en
  }
  geoip { source => ["clientip"]  }
  useragent {
    source => "agent"
    target => "useragent"
  }
}
```

パース

189.120.xx.xx - - [02/Dec/2014:12:18:29 +0900] "GET /manager/html HTTP/1.1" 404 274 "-" "Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0"


```
{…
  "@timestamp": "2015-04-10T09:07:49.325Z",
  "clientip": "189.120.xx.xx",
  "ident": "-",
  "auth": "-",
  "timestamp": "02/Dec/2014:12:18:29 +0900",
  "verb": "GET",
  "request": "/manager/html",
  …
  "agent": "\"Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/
```


elastic

設定：filter

```
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
    break_on_match => false
  }
  date {
    match => ["timestamp", "dd/MMM/YYYY:HH:mm:ss Z"]
    locale => en
  }
  geoip { source => ["clientip"]  }
  useragent {
    source => "agent"
    target => "useragent"
  }
}
```

日付のパース

```
{…
  "@timestamp": "2015-04-10T09:07:49.325Z",
…
  "timestamp": "02/Dec/2014:12:18:29 +0900",
…
}
```

```
{…
  "@timestamp": "2014-12-02T03:18:29.000Z",
…
  "timestamp": "02/Dec/2014:12:18:29 +0900",
…
}
```

設定：filter

```
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
    break_on_match => false
  }
  date {
    match => ["timestamp", "dd/MMM/YYYY:HH:mm:ss Z"]
    locale => en
  }
  geoip { source => ["clientip"]  }
  useragent {
    source => "agent"
    target => "useragent"
  }
}
```

IPから緯度経度など付与

```
  "clientip": "189.120.xx.xx",
```

```
  "clientip": "189.120.xx.xx",
  "geoip": {
    "ip": “189.120.xxx.xxx”,
…
    "country_name": "Brazil",
    "continent_code": "SA",
    "region_name": "27",
    "city_name": "São Paulo",
    "latitude":
```

設定：filter

```
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
    break_on_match => false
  }
  date {
    match => ["timestamp", "dd/MMM/YYYY:HH:mm:ss Z"]
    locale => en
  }
  geoip { source => ["clientip"]  }
  useragent {
    source => "agent"
    target => "useragent"
  }
}
```

ユーザエージェントのパース

```
"agent": "\"Mozilla/5.0 (Windows NT 5.1; rv:
5.0) Gecko/20100101 Firefox/5.0\""
```

```
"agent": "\"Mozilla/5.0 (Windows NT 5.1; rv:
5.0) Gecko/20100101 Firefox/5.0\""
  "useragent": {
    "name": "Firefox",
    "os": "Windows XP",
    "os_name": "Windows XP",
    "device": "Other",
    "major": "5",
    "minor": "0"
  }
```

設定：output

```
output {
 elasticsearch {
    hosts => ["localhost"]
    index => “demo_access_log-%{+YYYY.MM.dd}”
 }
}
```

さらに活用するには？

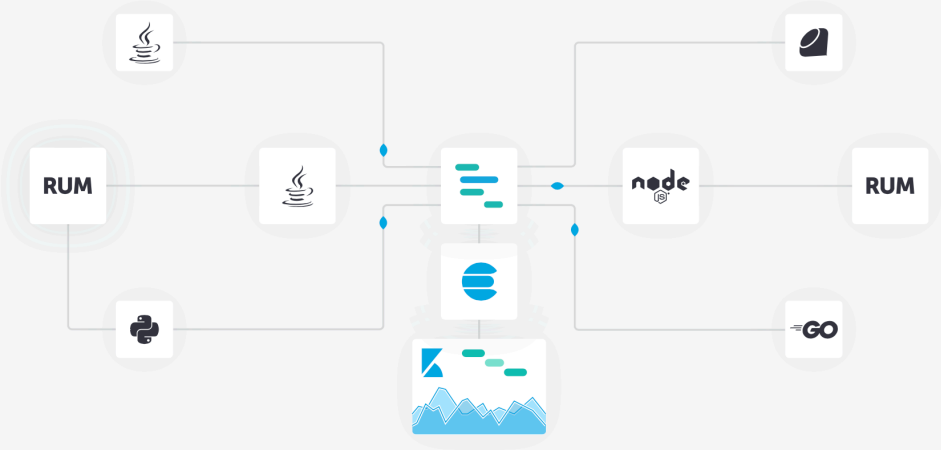
elasticsearch-hadoop

ES-Hadoop：Hadoop、Spark、その他の製品との統合

- Hadoopデータのリアルタイムサーチ
- Hadoopに関するスタンドアロンの自己充足型のライブラリ
- ESデータへの双方向アクセス
- MapReduce、Hive、Pig、Cascading、Spark、Stormをサポート
- HDFSを使用してESデータのバックアップやアーカイブを実施

オープンソースのアプリケーション パフォーマンス監視（APM）

ログやシステムのメトリックをElasticsearchに取り込みましたか？
ElasticのAPMで、アプリケーションのメトリックも取り込むことができます。
初期設定に、4行コードを加えるだけ。
問題箇所をすばやく確認し、自信をもってコードをプッシュできます。



ElasticのAPMで、パフォーマンスメトリックの可視化が簡単に。 | 今すぐトライ

NEW Elastic APM UIに新メニューが登場。検索バー、機械学習統合、RubyとJavaScriptのRUM向けエージェント、JavaとGoのベータ版が加わりました。 さらに詳しく

検索 + APM

今すぐはじめる

ELASTIC STACK

Elastic Stackのオプション

エンタープライズグレードのセキュリティと、開発者フレンドリーなAPIを備えたオプション（旧X-Pack）。機械学習からグラフ分析まで、多彩な機能を手軽に、楽しく使えます。

セキュリティ

Elasticsearchデータを堅牢に、きめ細やかな設定で保護

さらに詳しく

アラート

データの変化を通知

さらに詳しく

監視

Elastic Stackを監視し、高水準な稼働状況を保つ

さらに詳しく

elastic

Elasticsearch Service　App Search　Site Search

ELASTIC CLOUD

Elasticsearchのパワーを利用したSaaS製品群

Elastic Cloudは、展開、運用、スケールが容易にできるElasticの製品とソリューションをCloudで利用可能にした、成長し続けるSaaS製品群です。容易に利用できるElasticsearchのマネージドサービスから、パワフルですぐに利用可能なソリューションまで、Elastic Cloudは、Elasticを継ぎ目なく業務に適用するための足がかりです。

Elasticsearch Service

AWSやGCPで、Kibanaや他では得られない機能と共に容易に展開します。

製品概要

今すぐトライ

Elastic App Search Service

アプリケーションにスケーラブルな検索機能を実装するために、ものの数分で展開します。

製品概要

今すぐトライ

Elastic Site Search Service

パワフルな検索体験をあなたのウェブサイトで提供できます。特別な学習は必要ではありません。

製品概要

今すぐトライ

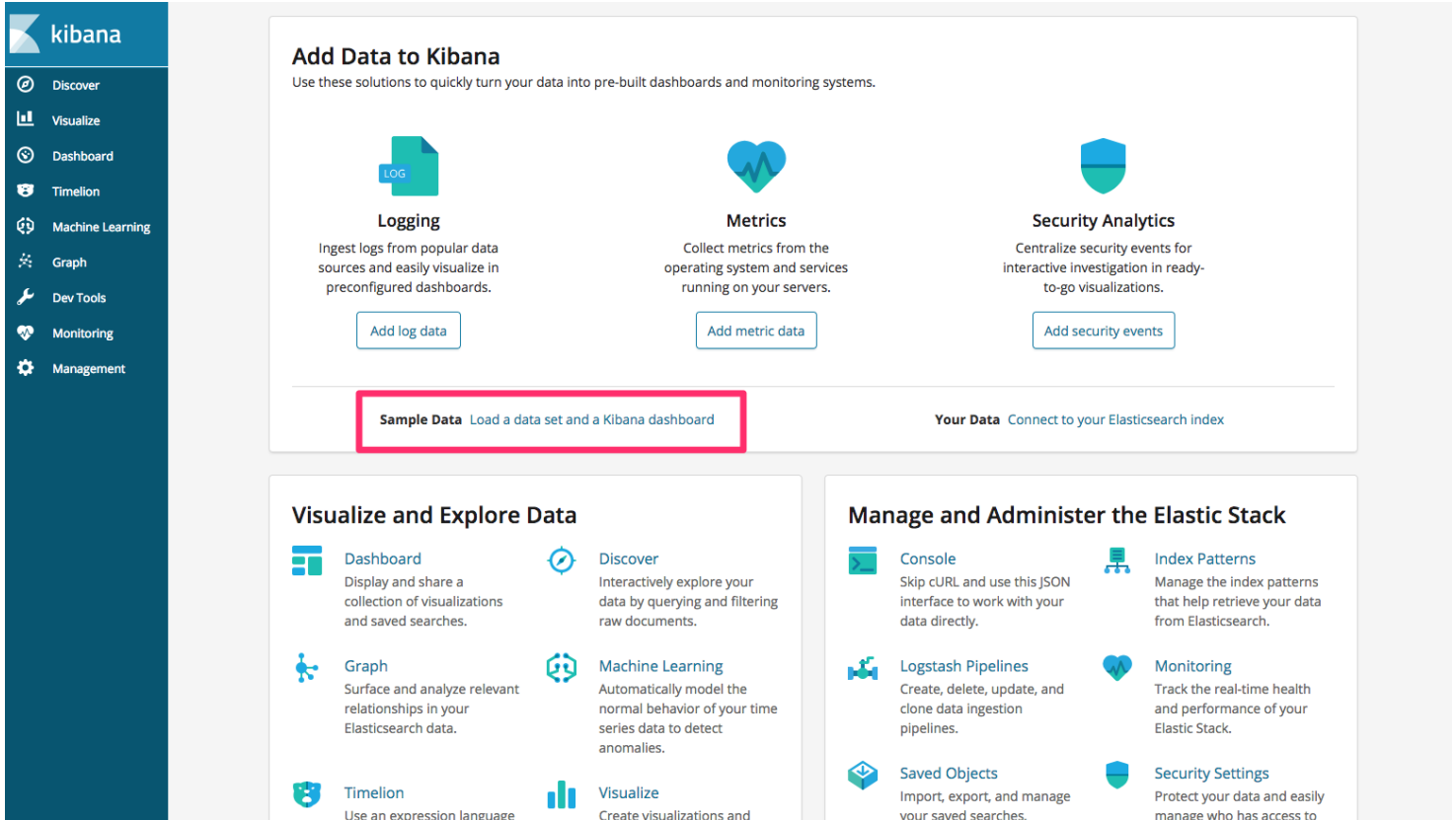
lastic

その他の使い方

データの登録方法

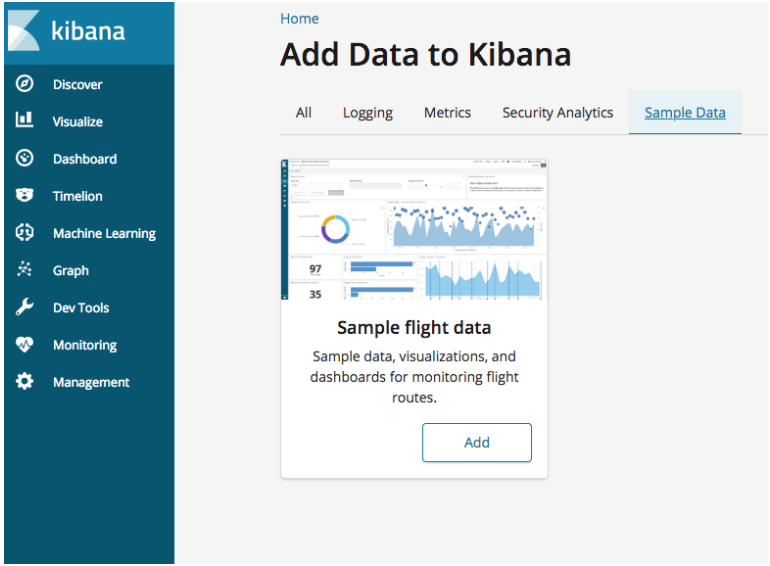
- Kibanaのサンプルデータ（6.4から）
- LogstashでJDBC input
- LogstashでCSV
- Filebeatでアクセスログ
- Metricbeatでメトリック
- PacketbeatでMySQL/PostgreSQLのパケット解析

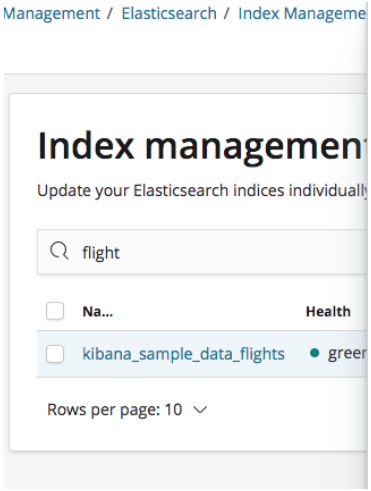
Kibanaのサンプルデータ（>= 6.4.0）

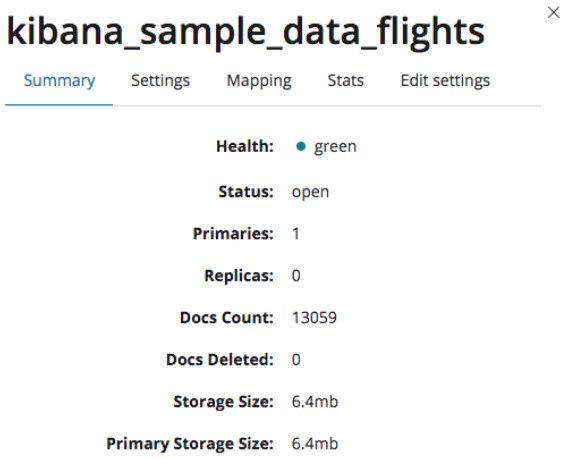


elastic

ワンクリックでデータ登録

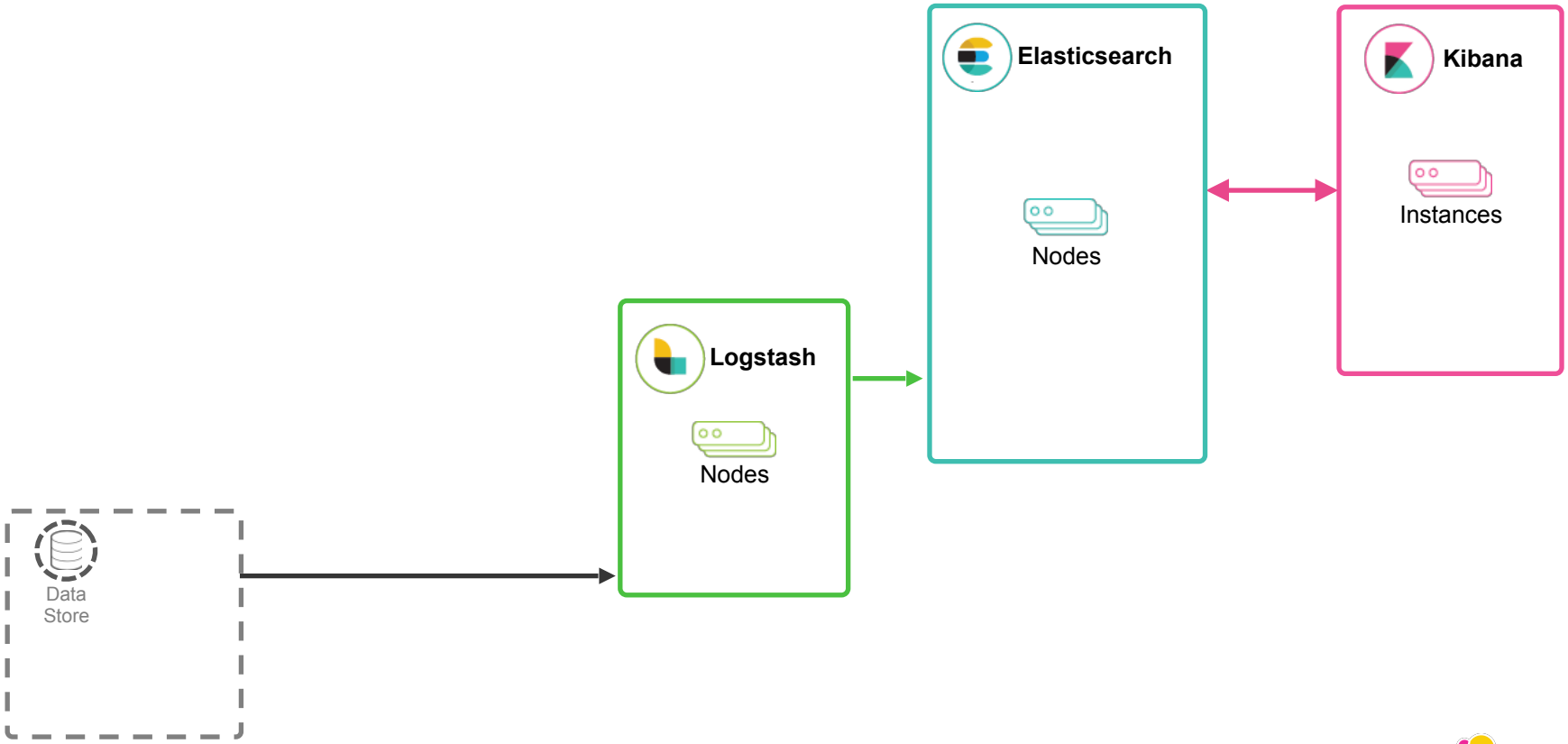






elastic

LogstashでJDBC Input



elastic

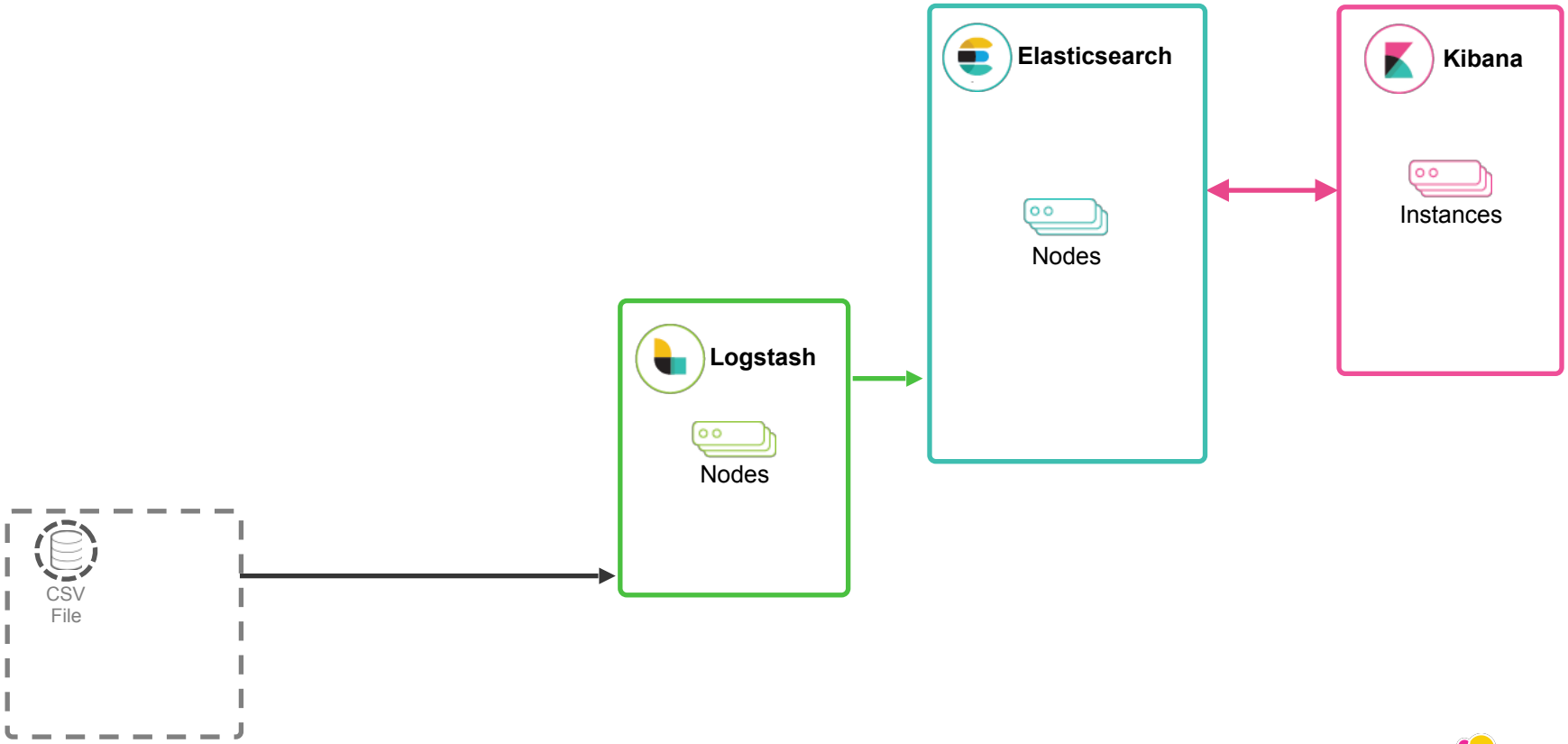
JDBC Input

```
input {
  jdbc {
    jdbc_connection_string => "jdbc:postgresql://db_server:5432/"
    jdbc_driver_class => "org.postgresql.Driver"
    jdbc_driver_library => "/home/elastic/postgresql-9.1-901-1.jdbc4.jar"
    jdbc_user => "postgres"
    jdbc_password => "password"
    statement => "SELECT * from blogs"
  }
}

filter {
  mutate {
    remove_field => ["@version", "host", "message", "@timestamp", "id", "tags"]
  }
}

output {
  stdout { codec => "dots"}
  elasticsearch {
    index => "blogs"
    document_type => "_doc"
  }
}
```

LogstashでCSV

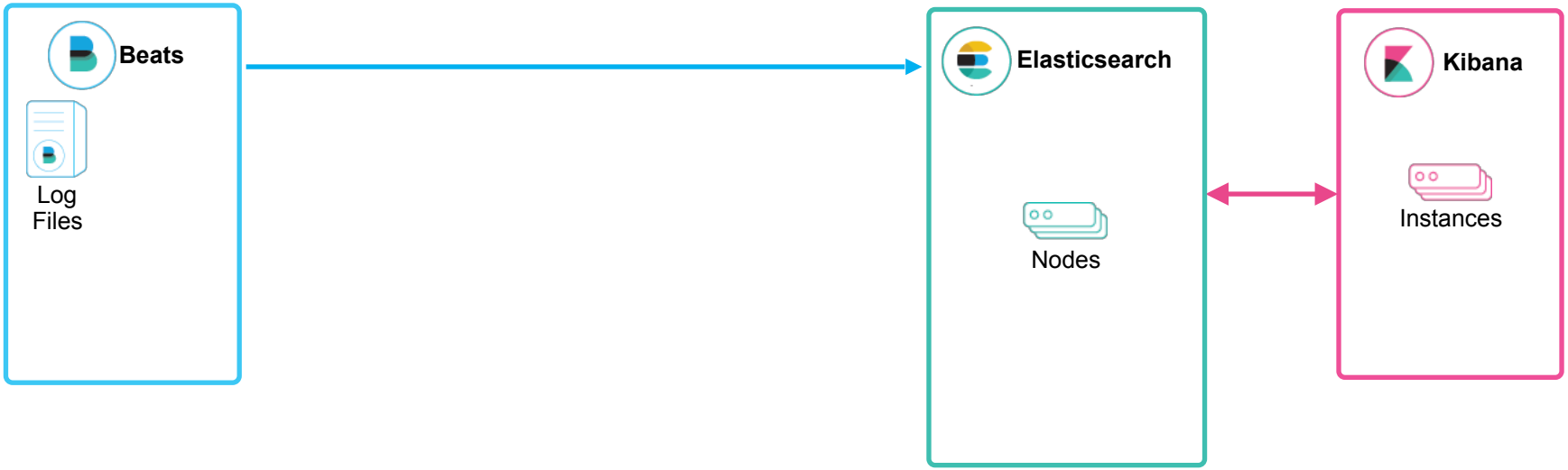


elastic

CSV filter

```
input {
  stdin { type => "${EVENT:earthquake}" }
}
filter {
  csv {
    columns => ["timestamp","latitude","longitude","depth","mag","magType","nst","gap","dmin","rms","source","event_id"]
    convert => {"latitude" => "float"}
    convert => {"longitude" => "float"}
    convert => {"depth" => "float"}
    convert => {"mag" => "float"}
    convert => {"dmin" => "float"}
    convert => {"rms" => "float"}
    convert => {"gap" => "float"}
  }
  mutate {
    add_field => ["location", "%{latitude}, %{longitude}"]
    remove_field => ["latitude", "longitude"]
  }
  date {
    match => ["timestamp", "yyyy/MM/dd HH:mm:ss.SS", "ISO8601"]
    remove_field => ["timestamp"]
    timezone => "GMT"
  }
}
output {
#  stdout { codec => rubydebug { metadata => true } }
  stdout { codec => dots }
  elasticsearch {
#    hosts => [""]
```

Filebeatでアクセスログ



elastic

Filebeatでアクセスログ

- 2つのElasticsearchプラグインをインストールしてElasticsearchを起動

```
bin/elasticsearch-plugin install ingest-geoip
bin/elasticsearch-plugin install ingest-user-agent
```

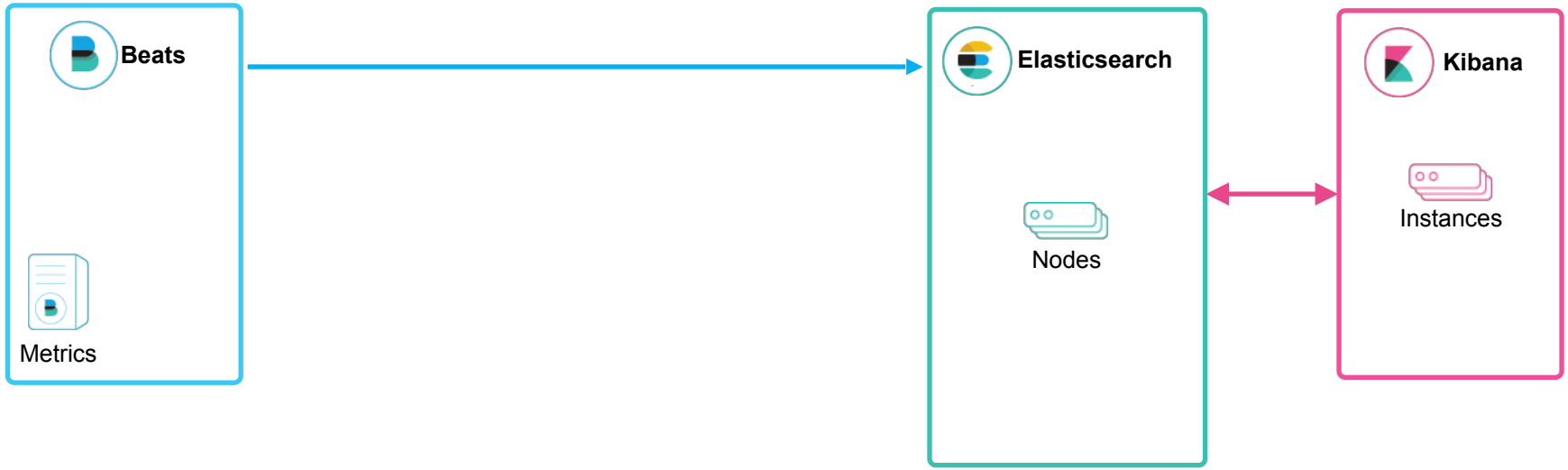
- FilebeatのApache2モジュールを有効化

```
./filebeat modules enable apache2
```

- modules.d/apache2.ymlにアクセスログのパスを設定
- setupコマンドを実行してからFilebeatを起動

```
./filebeat setup
./filebeat -e
```

Metricbeatでメトリック



Metricbeatでメトリック

- MetricbeatのsystemモジュールをEnable

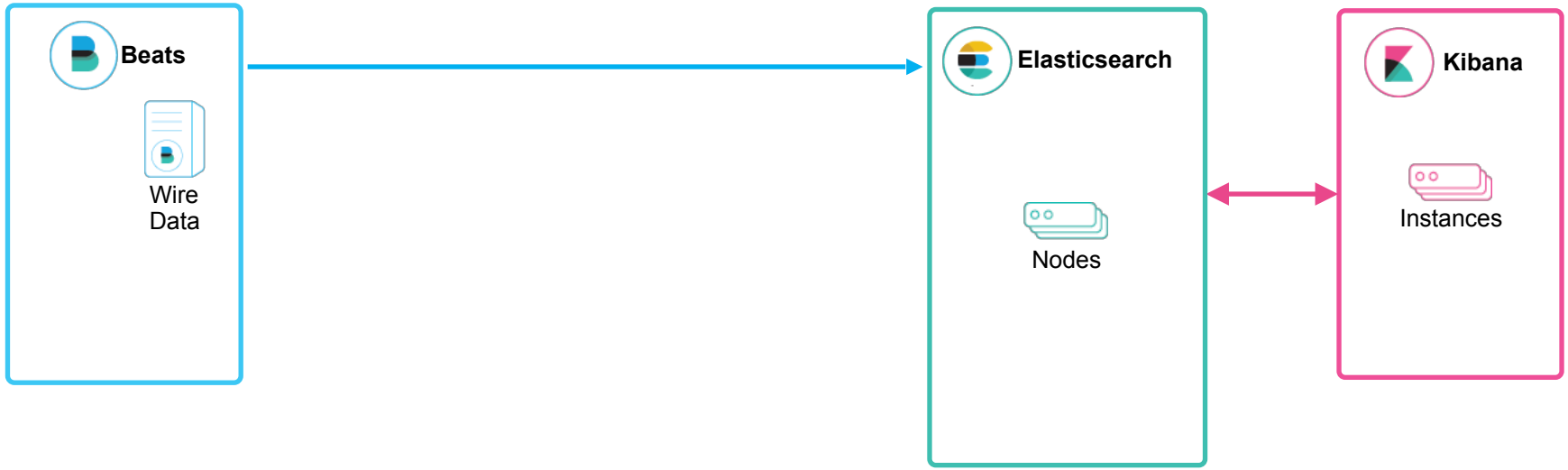
```
./metricbeat modules enable system
```

- setupコマンドを実行してからFilebeatを起動

```
./metricbeat setup
./metricbeat -e
```


elastic

PacketbeatでMySQL、PostgreSQLのパケット解析

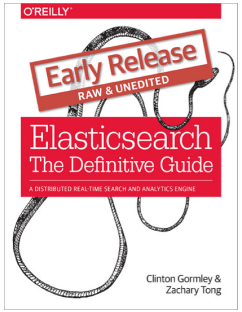


elastic

参考文献

- Elasticsearch - The Definitive guide
  - http://www.elastic.co/guide/en/elasticsearch/guide/current/index.html

- 書籍（日本語）
  - データ分析基盤構築入門
  - Elasticsearch実践ガイド



elastic

参考サイト

- ユースケース
  - https://www.elastic.co/use-cases
- Discuss（Webフォーラム）
  - https://discuss.elastic.co
- Elastic{ON}のビデオと資料
  - https://www.elastic.co/elasticon/videos
- サポートメニュー
  - https://www.elastic.co/subscriptions

elastic

Thank you!

- **Web** : https://www.elastic.co/jp/
- **Forums** : https://discuss.elastic.co/
- **Twitter** : @johtani