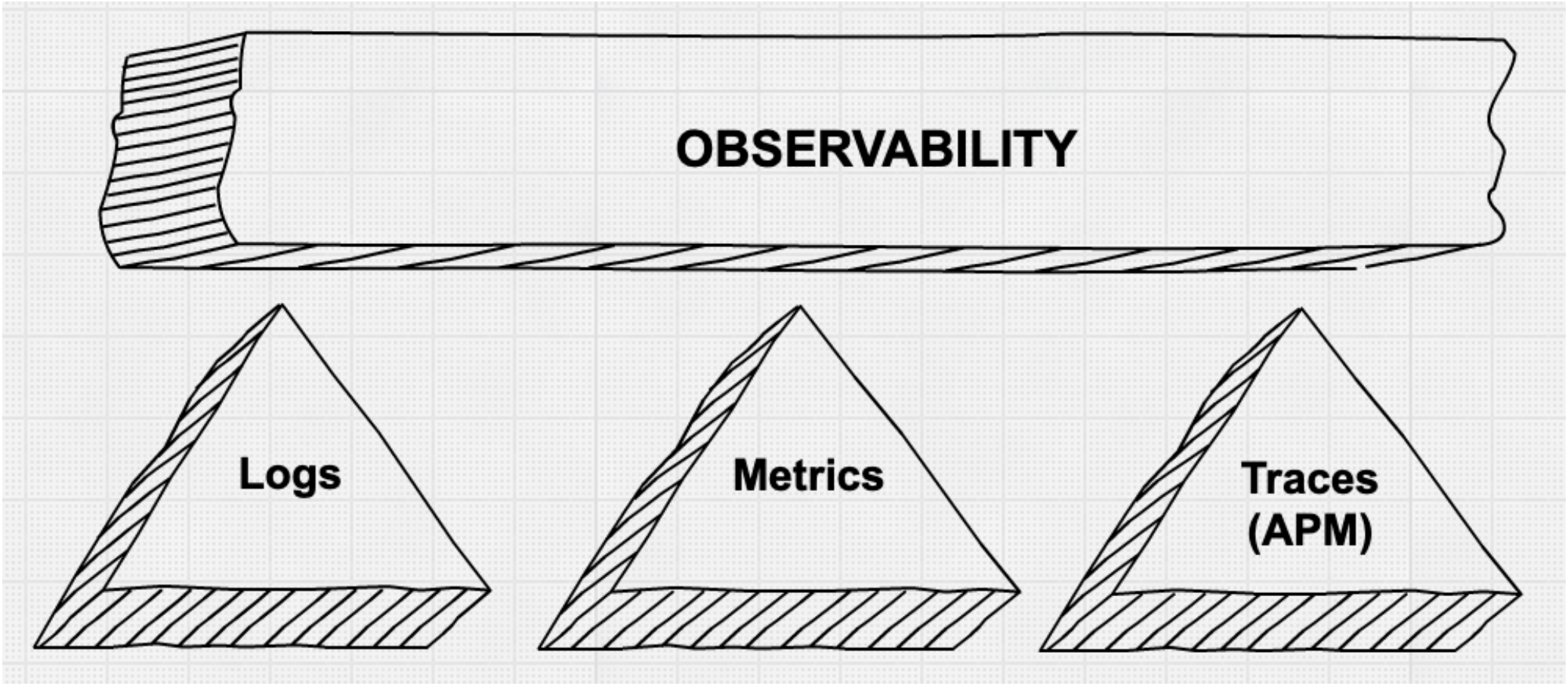
elastic

ElasticsearchとKibanaによるオブザバービリティハンズオン

Jun Ohtani @ Elastic

The world's most popular enterprise open source products for real-time search, logging, analytics, and more

オブザバビリティ(Observability)



https://www.elastic.co/jp/blog/observability-with-the-elastic-stack

elastic

elastic


TH-
THIS IS NOT FINE!!
OH MY GOD EVERY THINGS ON FIRE
WHAT THE HELL IS MY PROBLEM

elastic

マイクロサービス？？？

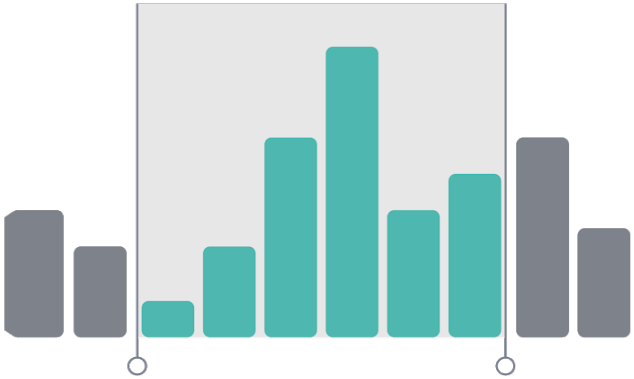
elastic

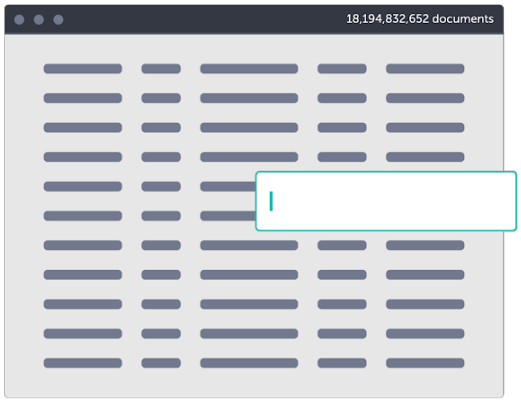
Elastic は **search company**

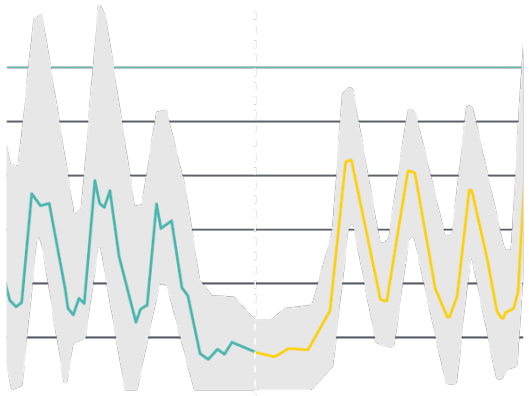
Elasticsearch は検索の技術

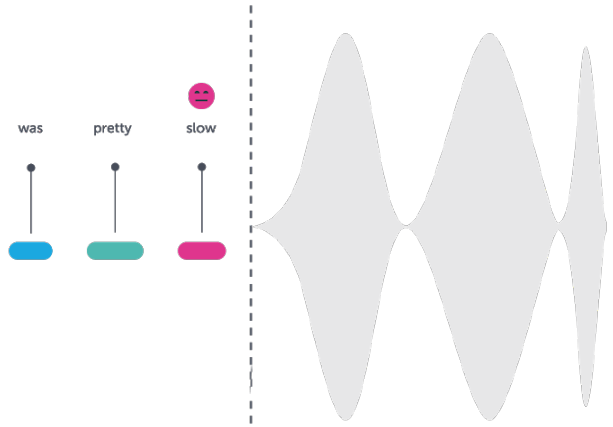
検索は**基礎技術**

.54 seconds | 1,000,000,000 records









技術による**差別化**

SCALE

分散システム

SPEED

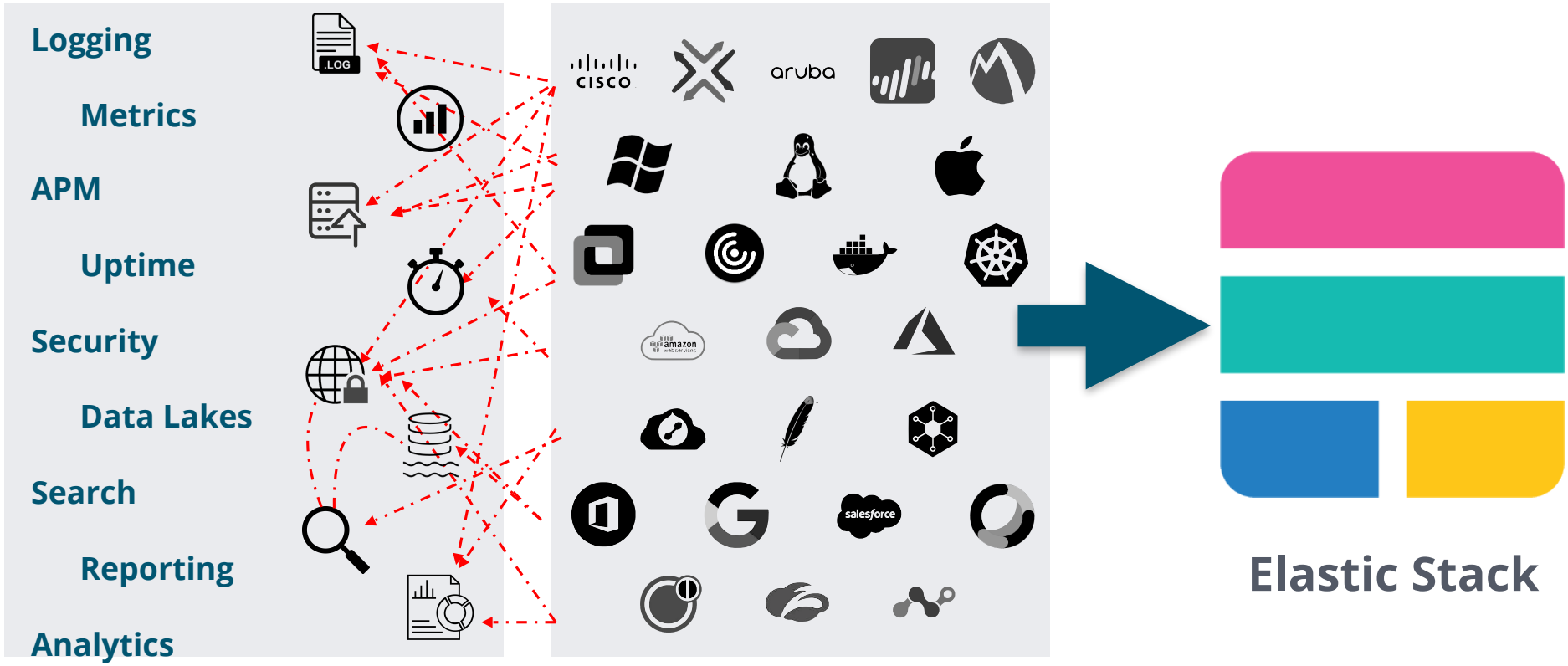
検索結果をすばやく取得

RELEVANCE

関連度の高い結果

elastic

複雑さを減らしましょう



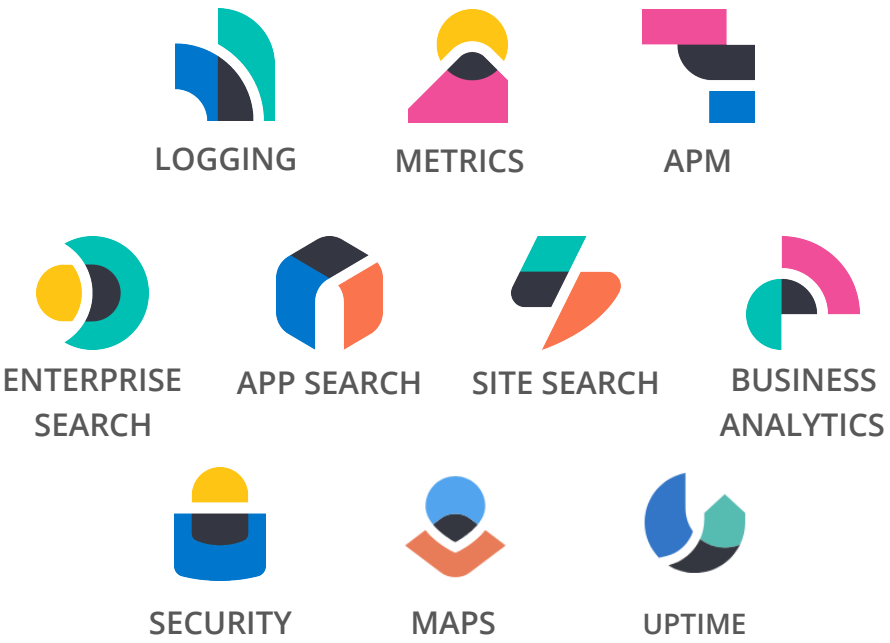
elastic

ROIを最大化

別のソリューションを使うと、2つか3つの
ビジネスチャレンジには対応可能

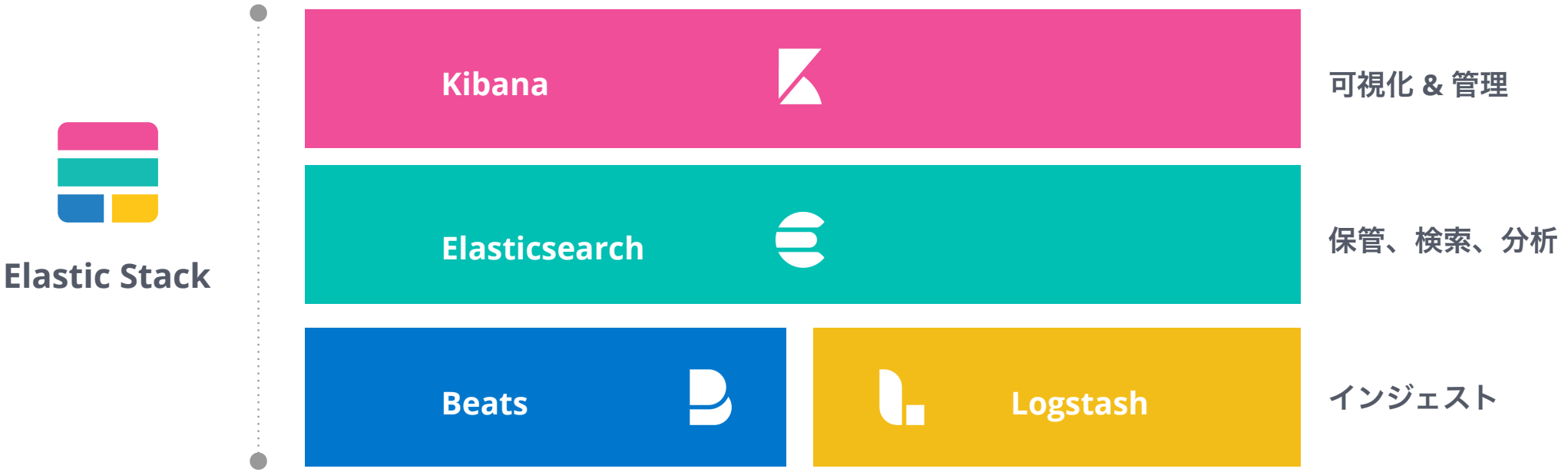
- App 1: Logging, Security, Metrics
- App 2: APM, RUM
- App 3: Network Metrics
- App 4: Site Search, App Search
- App 5: Business Analytics

Elasticを利用するとこれらの
全てに対応可能



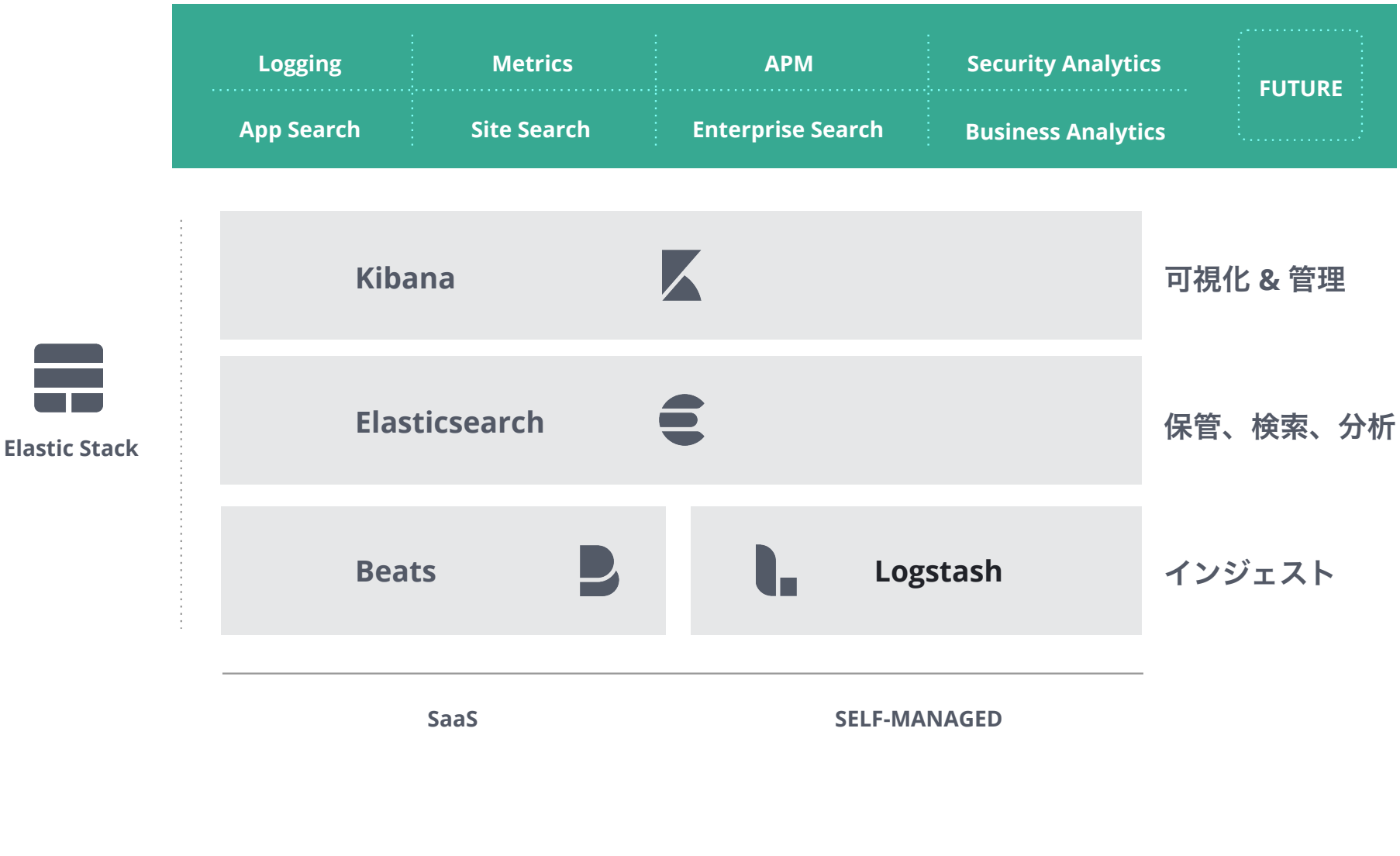
elastic

Elastic **Stack**



elastic

ソリューション

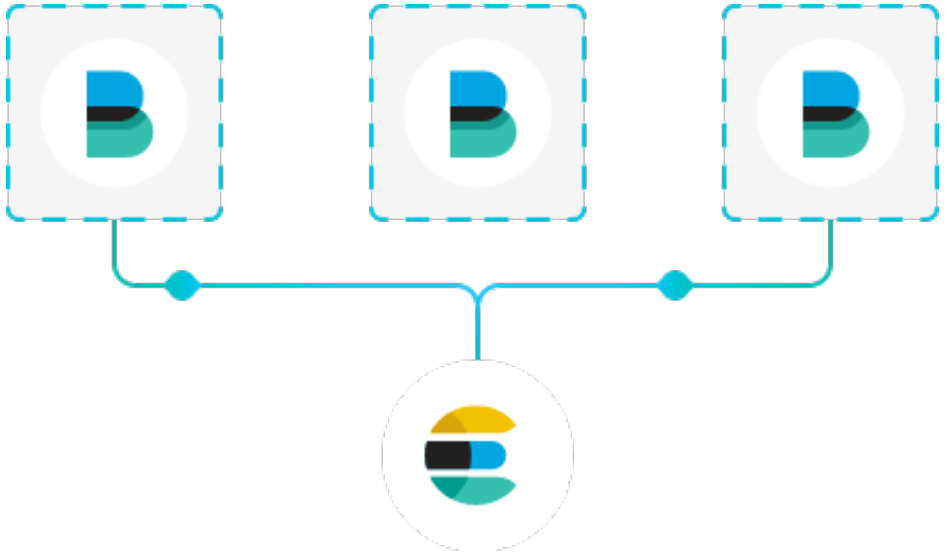


elastic

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

Beats family

Packetbeat

Network data

Metricbeat

Metrics

Winlogbeat

Windows Event Logs

Functionbeat

Serverless Shipper

Auditbeat

Audit data

Filebeat

Log files

Heartbeat

Uptime monitoring

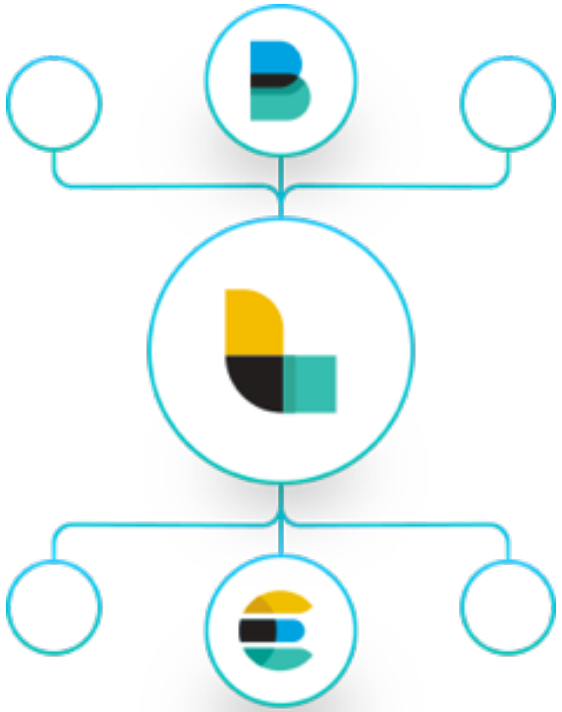
90+ community Beats

elastic

logstash

Logstash

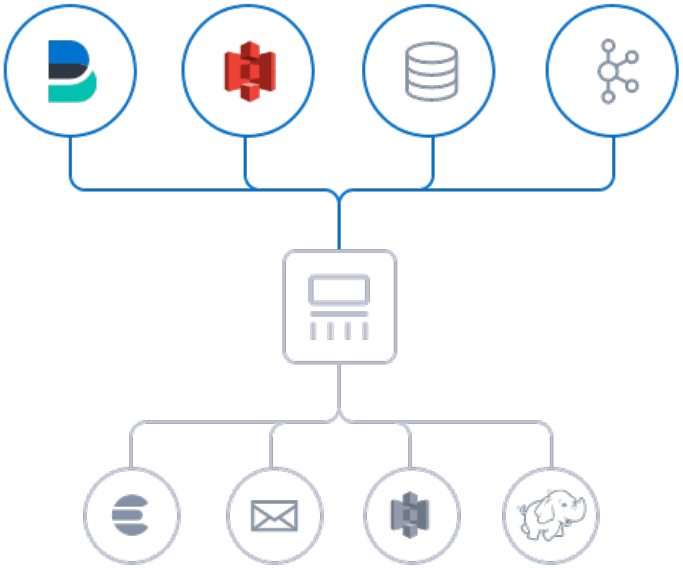
データ加工パイプライン



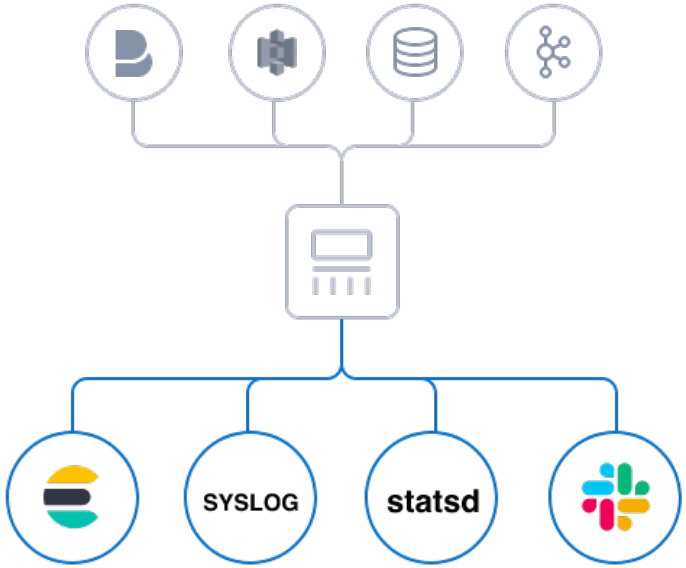
全ての形式、サイズとデータソースの投入	パースと動的なデータ変換	あらゆる出力にデータ転送
安全で暗号化されたデータ入力	独自のパイプライン処理の作成	200以上のプラグイン

多種多様な入出力

さまざまな入力プラグイン

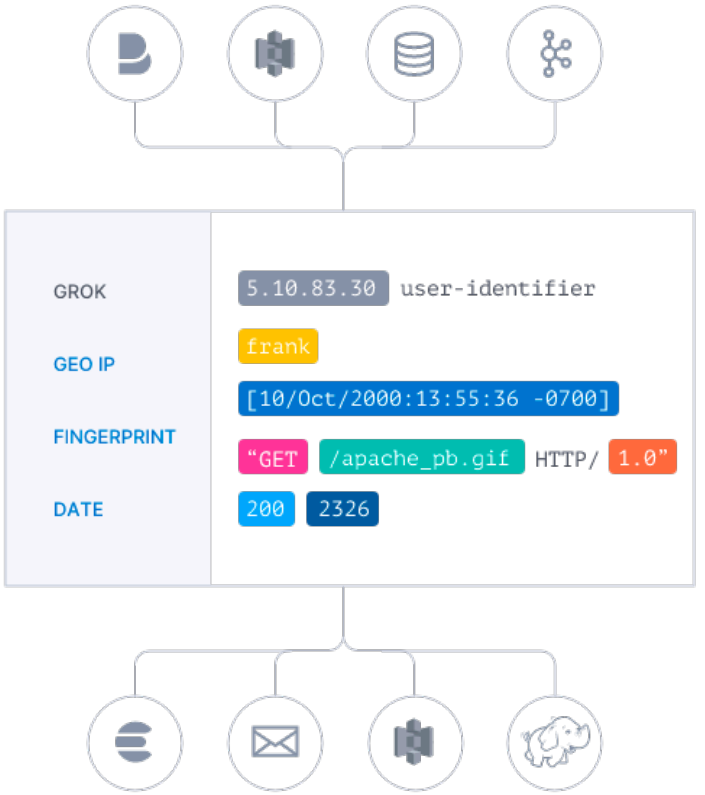


さまざまな出力プラグイン



データの解析と変換

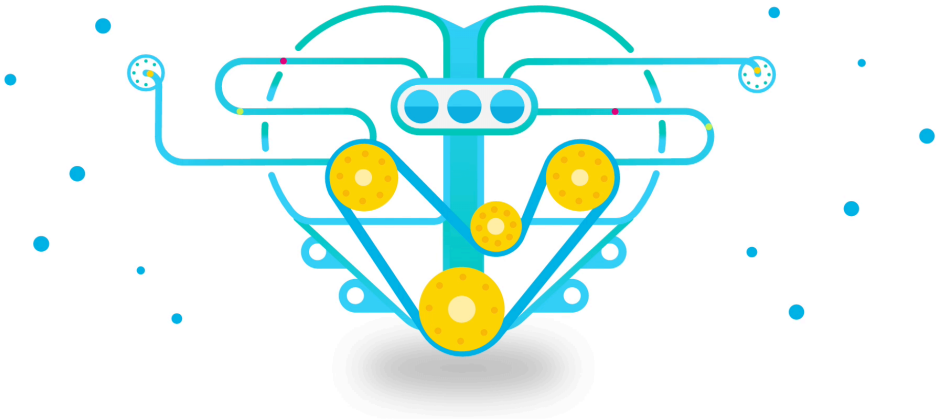
多種多様なフィルタを
使用したデータの変換
が可能



elasticsearch

Elasticsearch

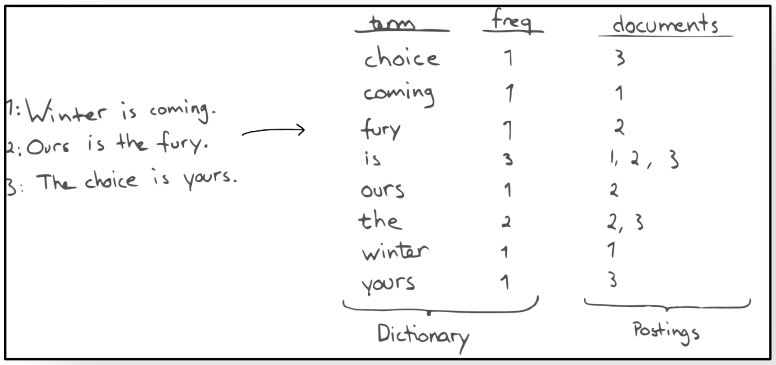
Heart of the Elastic Stack



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 の検索や数値分析のための機能

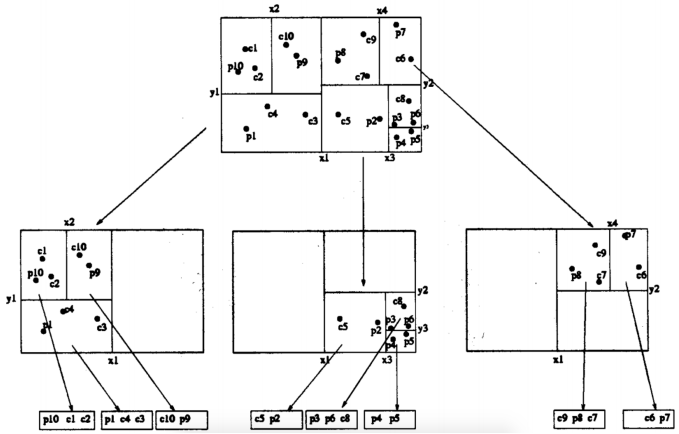
全文検索用の転置インデックス



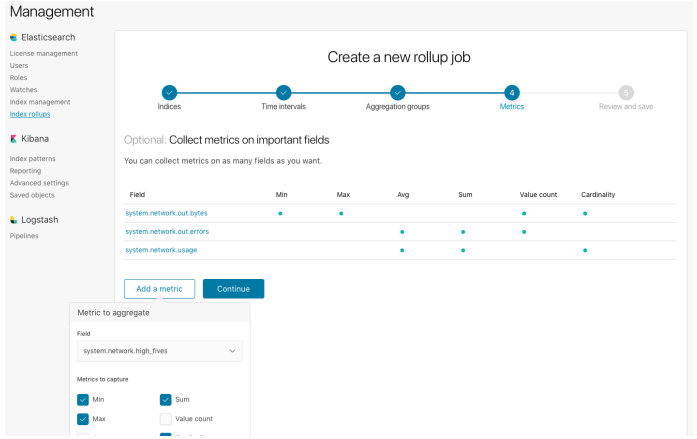
構造化データのためのカラム型データ構造

usernid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrice	Jill	Amy	Rice		
mt123	Jeff		Twain	Toledo	Ohio
sadams	Sue		Adams		
adoe	Amy		Doe	Miami	Florida

数値に強いBKD Tree



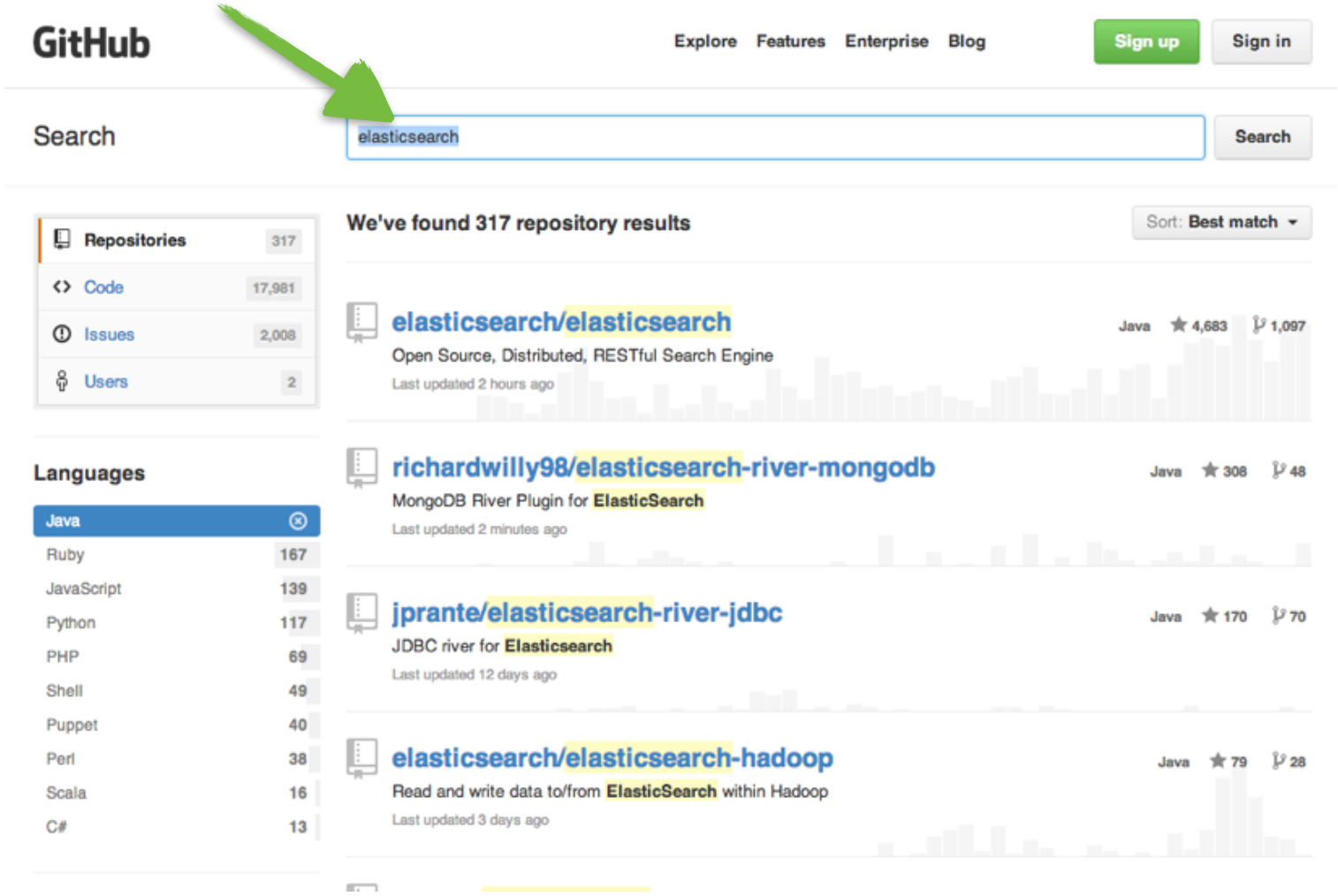
ロールアップ



elastic

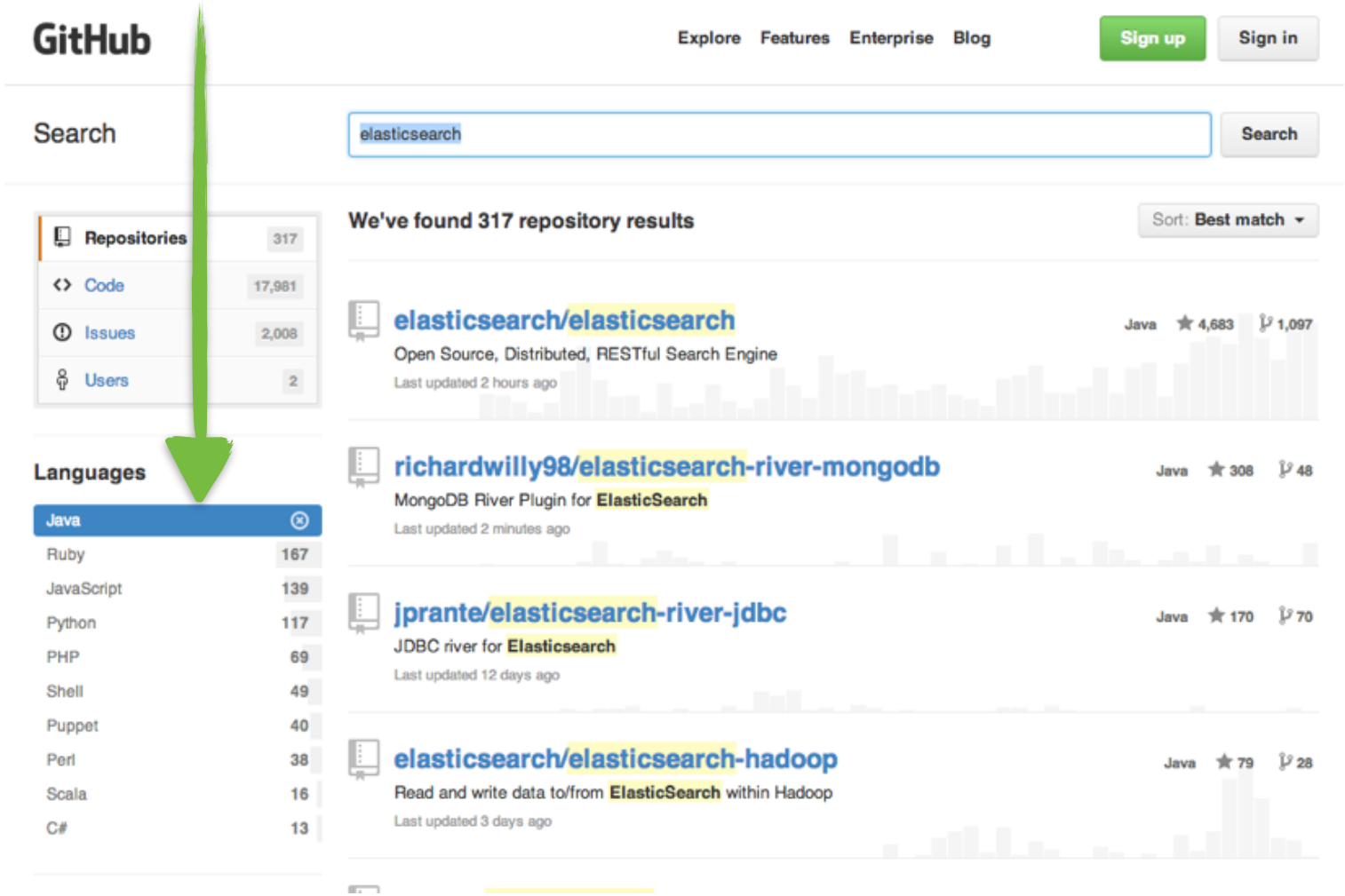
Elasticsearchとは？

フリーワード検索



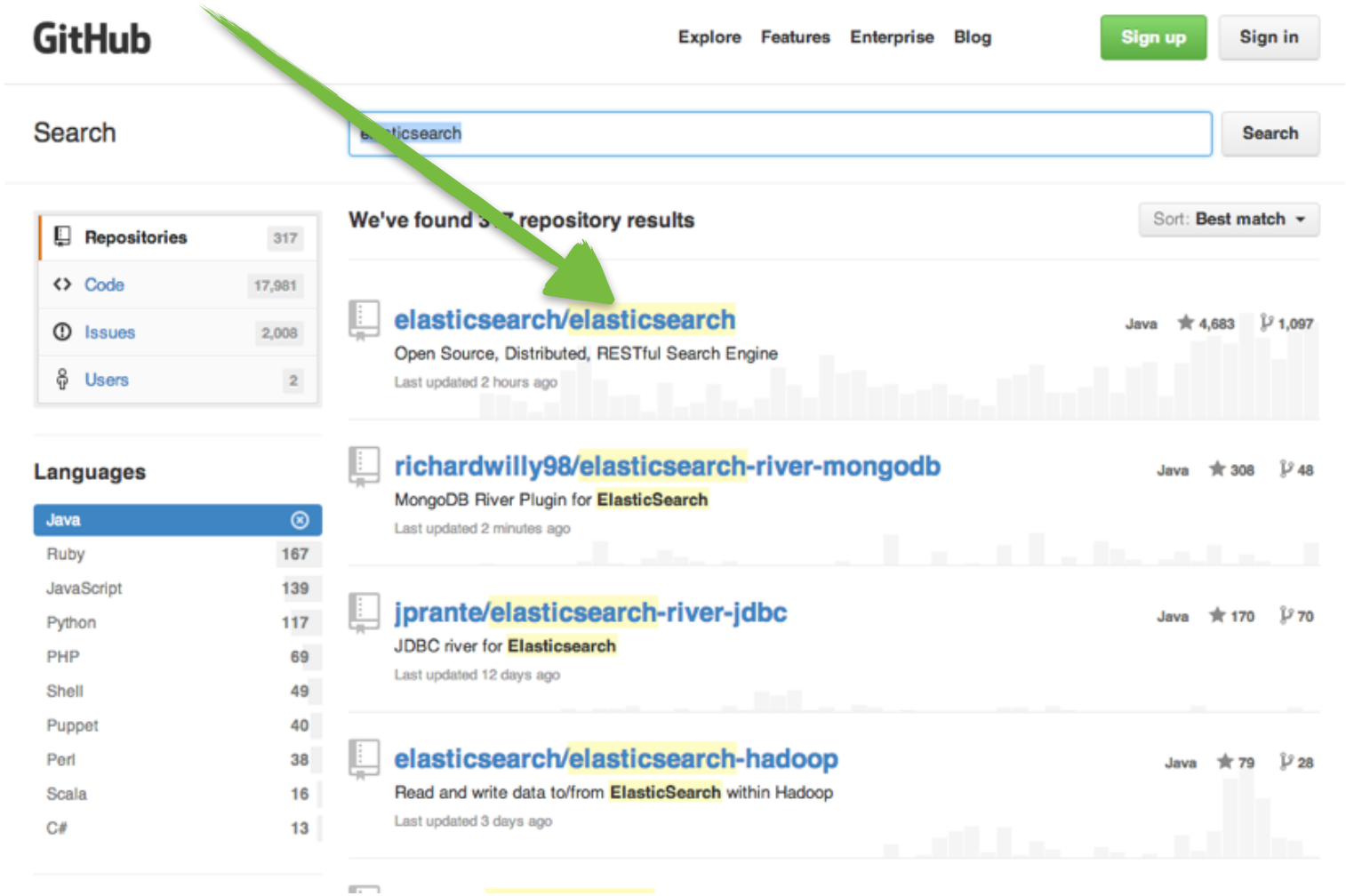
elastic

絞り込み



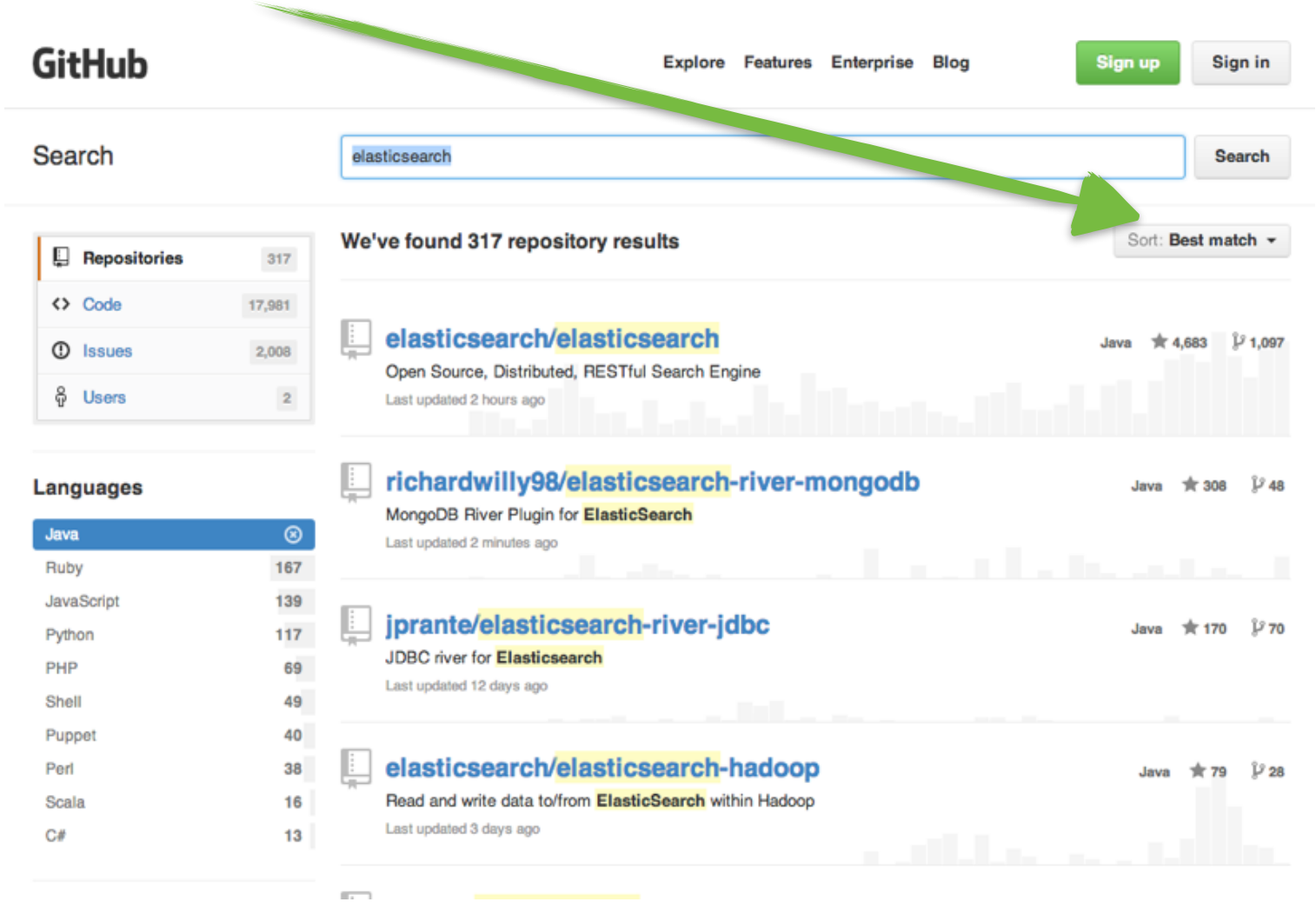
elastic

ハイライト



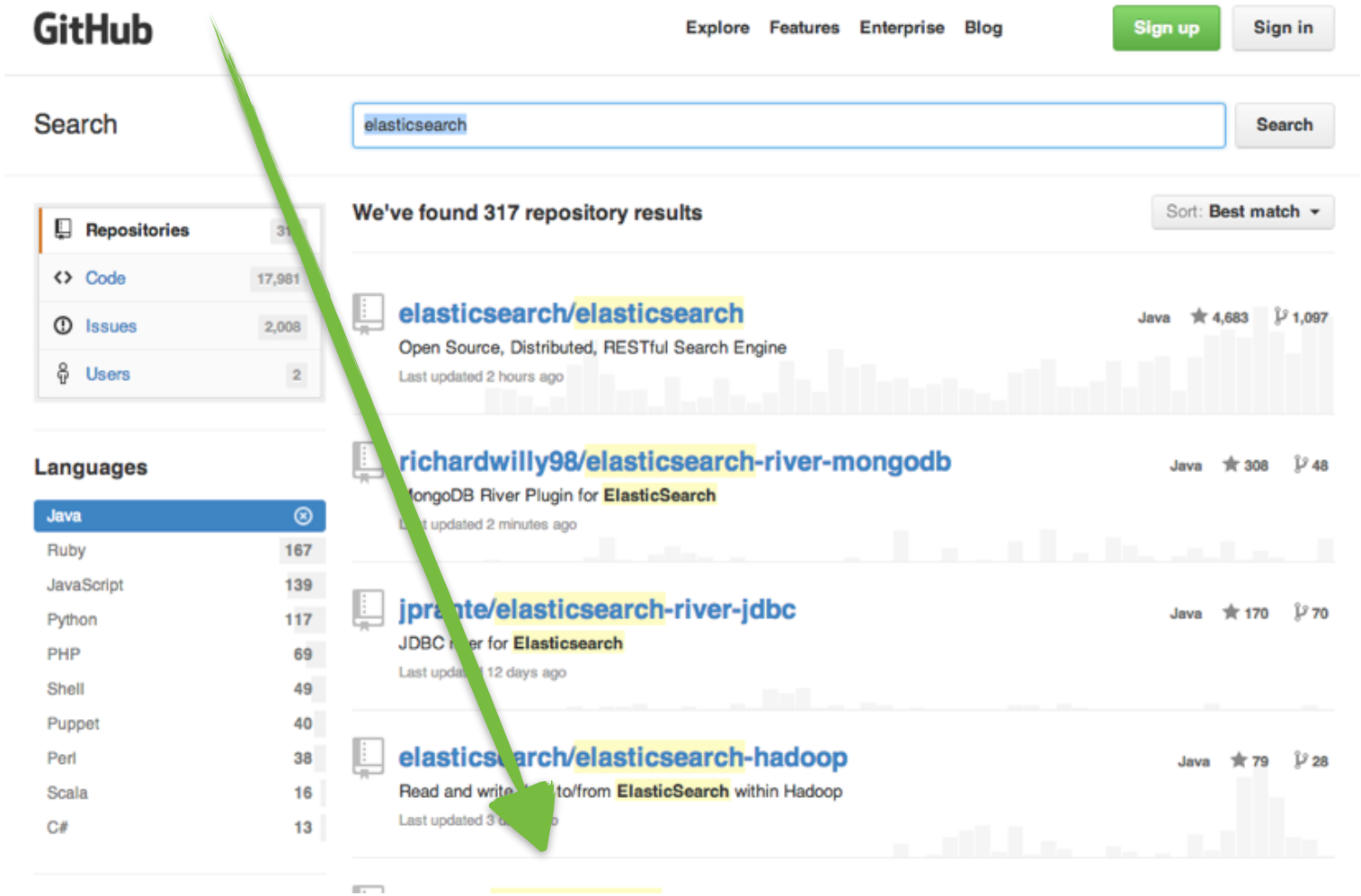
elastic

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
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

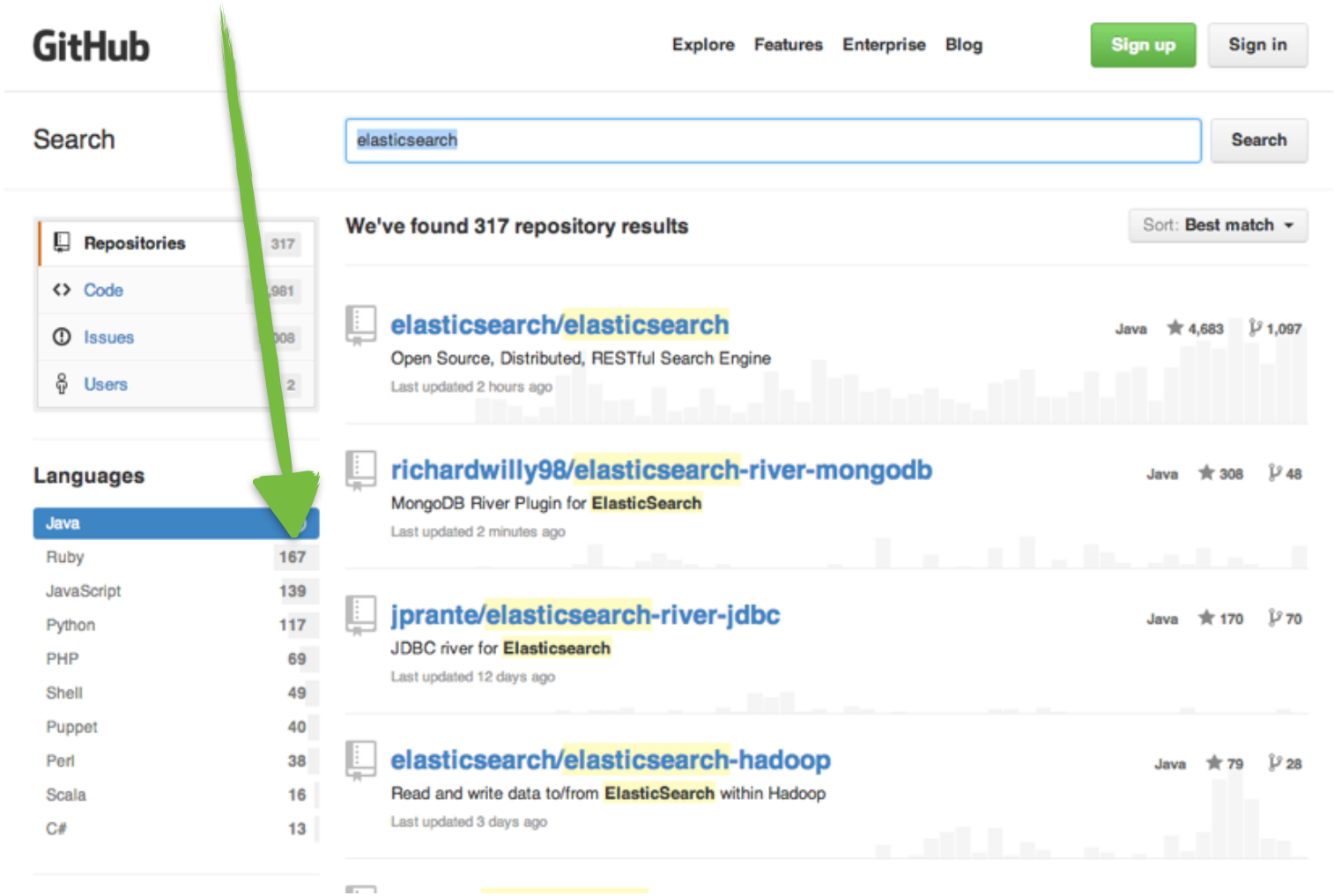
elastic

ページング



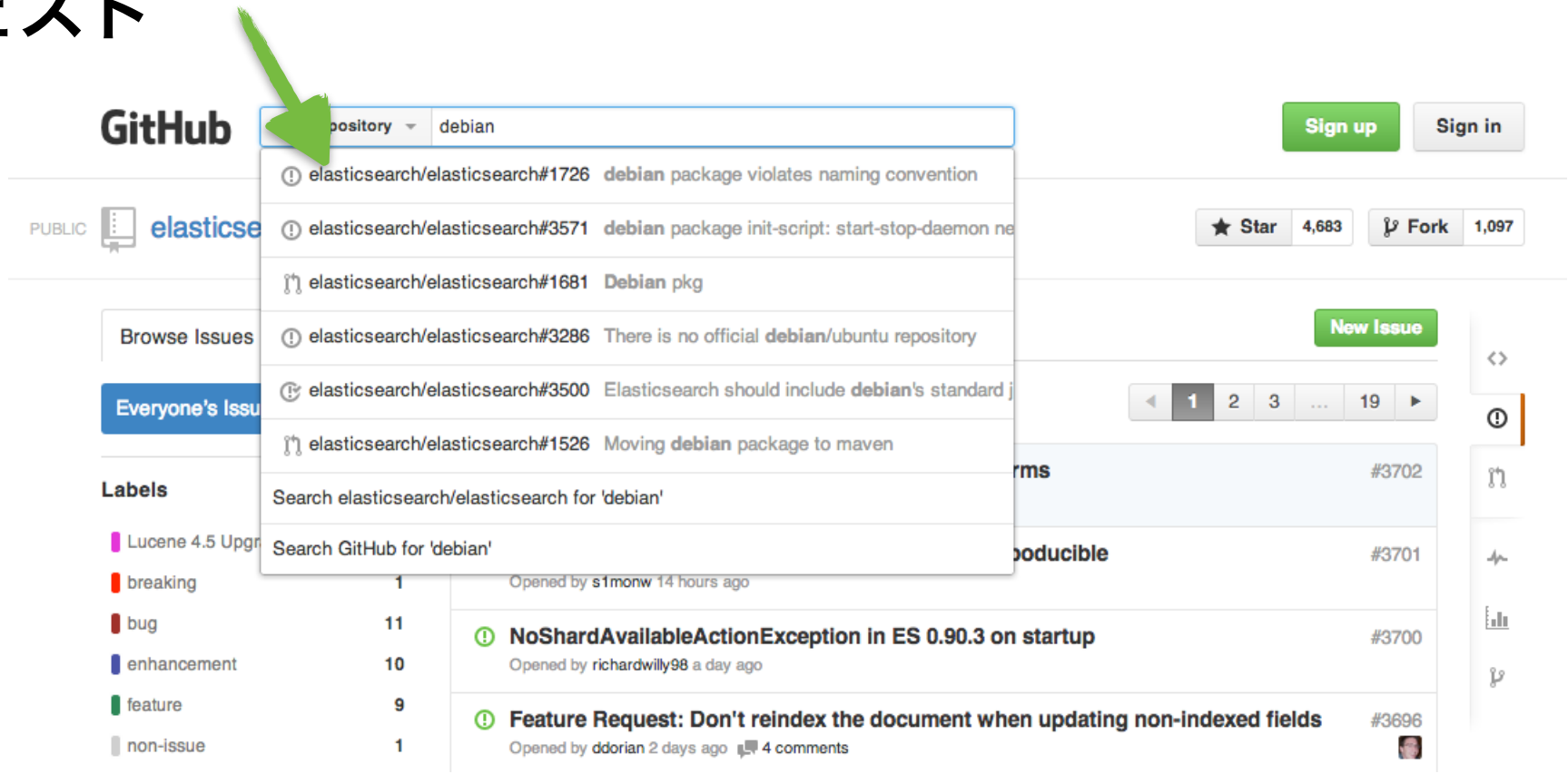
elastic

集計


GitHub
Explore
Features
Enterprise
Blog
Sign up
Sign in
Search
elasticsearch
Search
Repositories 317
Code 981
Issues 908
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
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

REST API + JSON

```
curl -X GET "localhost:9200/accounts/_search?pretty" -H
'Content-Type: application/json' -d'
{
    "query" : {
        "term" : { "firstname" : “Michael" }
    }
}
'
```

REST API + JSON

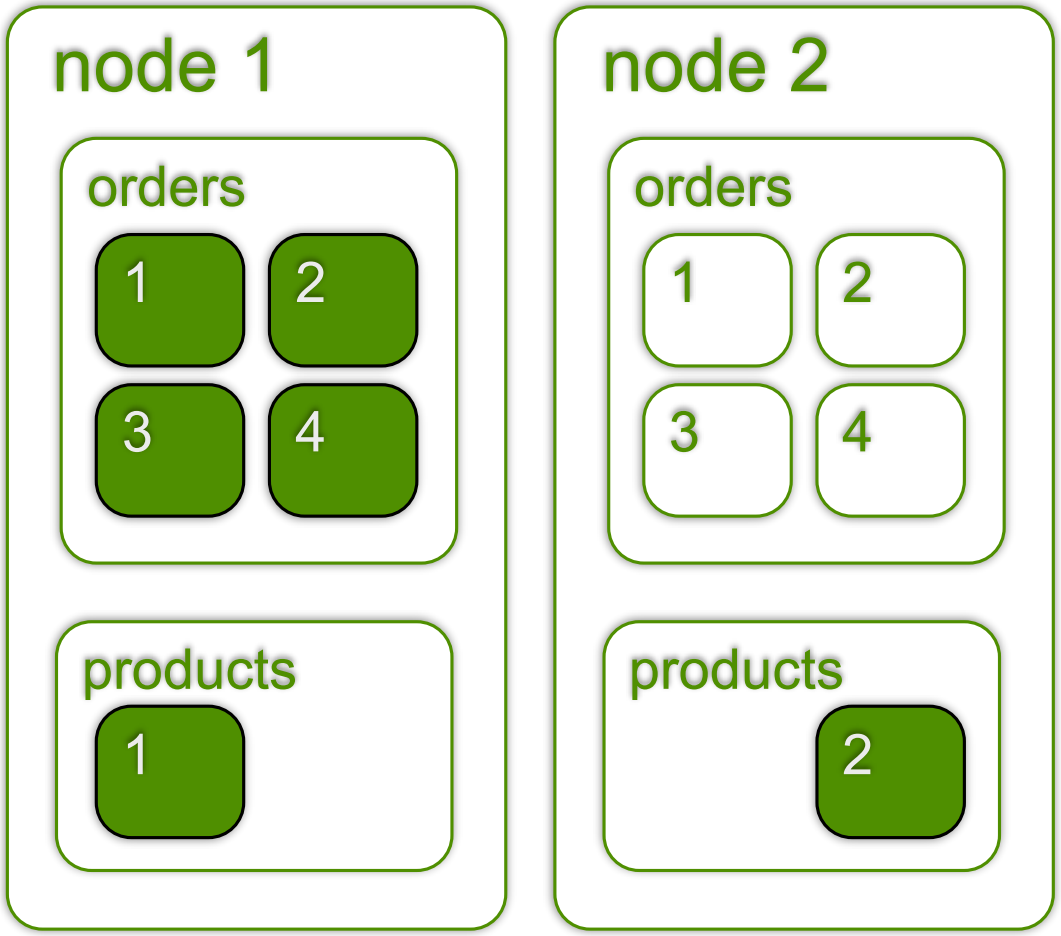

```
{
  "took" : 0,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 2,
      "relation" : "eq"
    },
    "max_score" : 5.992464,
    "hits" : [
      {
        "_index" : "accounts",
        "_type" : "_doc",
        "_id" : "606",
        "_score" : 5.992464,
        "_source" : {
          "account_number" : 606,
          "balance" : 28770,
          "firstname" : "Michael",
          "lastname" : "Bray",
          "age" : 31,
          "gender" : "M",
          "address" : "935 Lake Place",
          "employer" : "Telepark",
          "email" : "michaelbray@telepark.com",
          "city" : "Lemoyne",
          "state" : "CT"
        }
      },
```

分散構成、スケール

自動的な分散

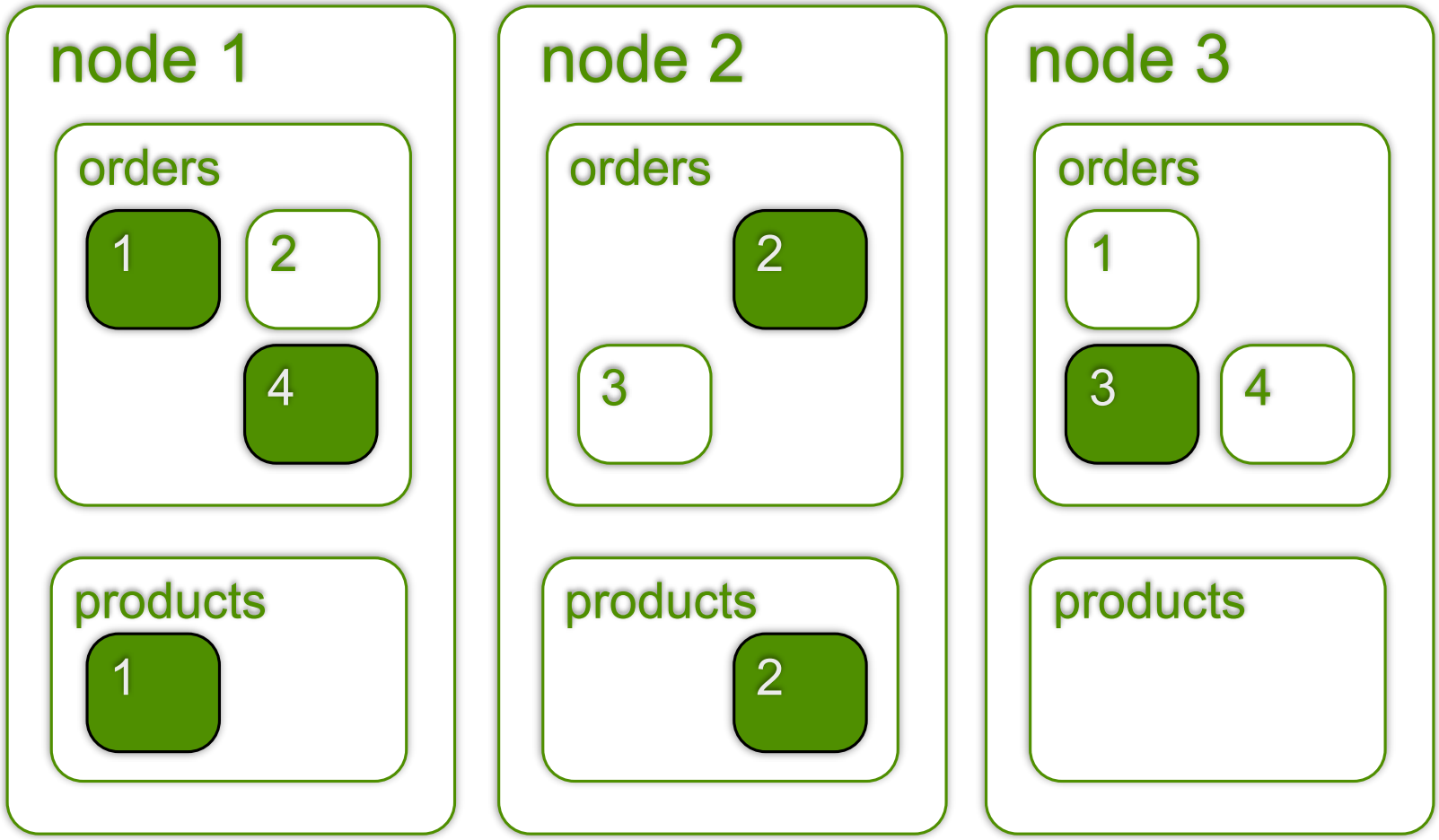
elastic

自動的な分散



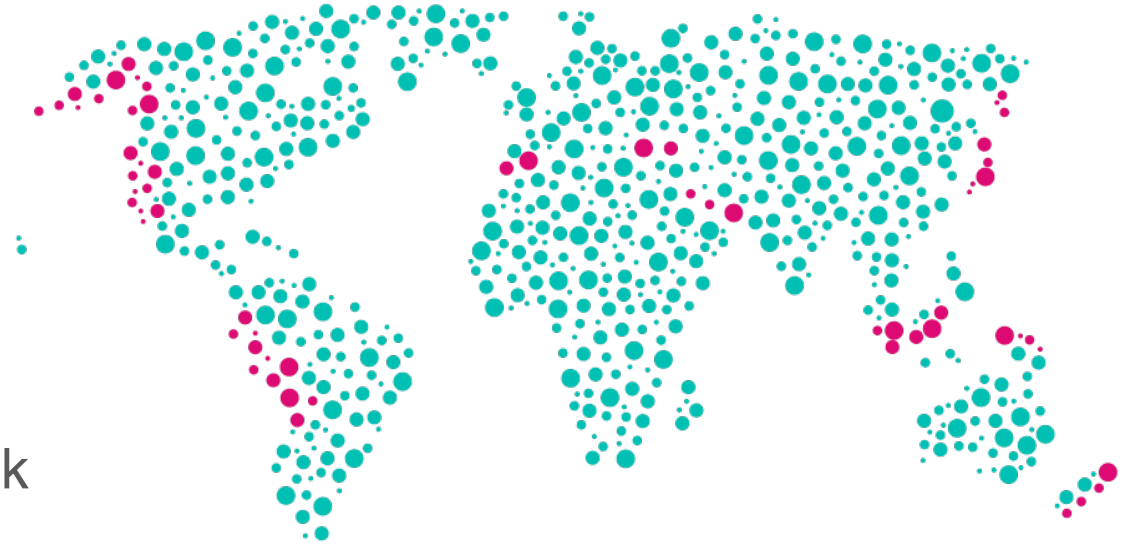
elastic

自動的な分散



elastic


kibana

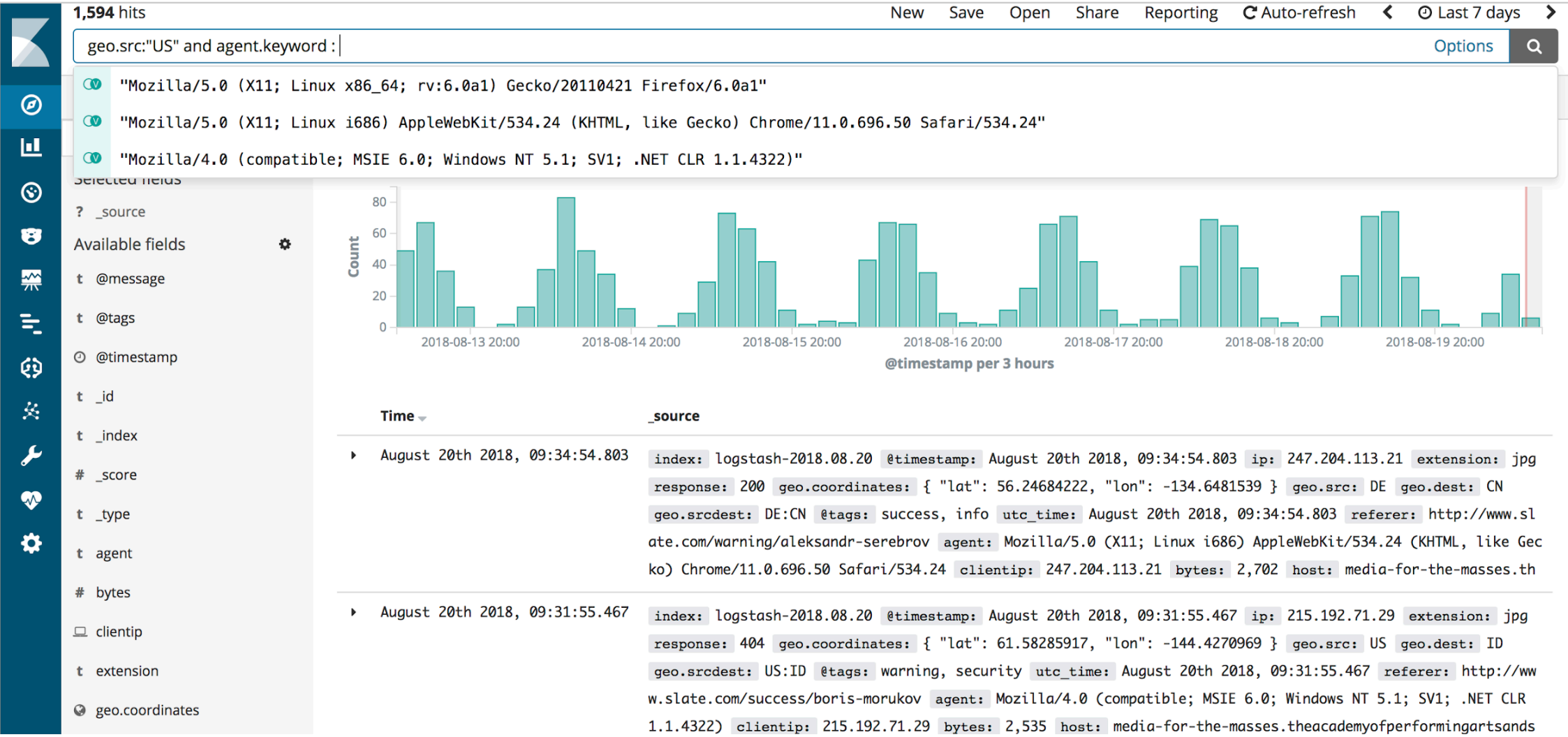


Kibana

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

検索、スクロール、探索、データを分析



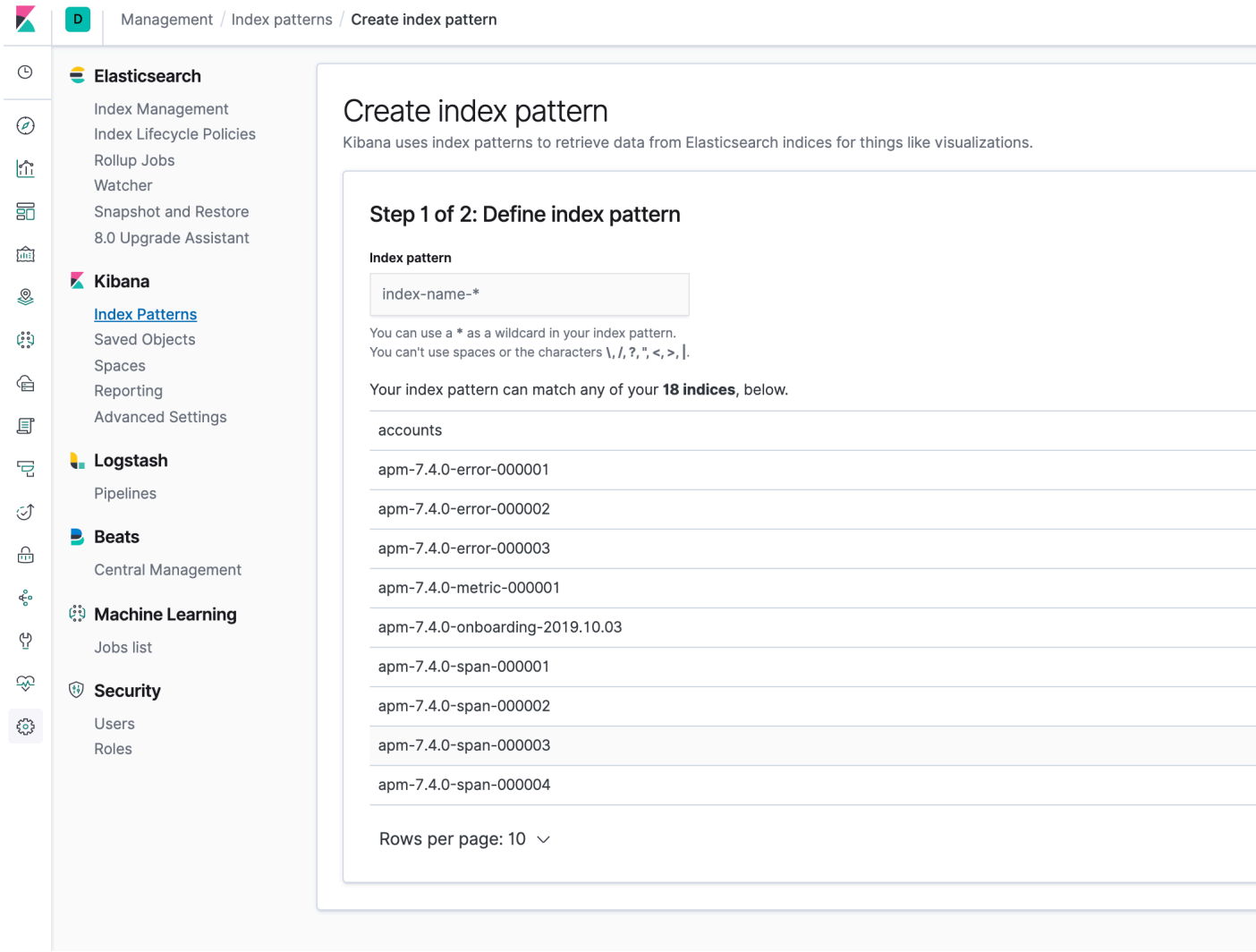
KIbanaの簡単な説明と最短手順

1. Index Pattern
    - 対象とするデータの取得先を定義
2. Discover
    - ざっくりデータを探索する
3. Visualize
    - グラフの作成
4. Dashboard
    - 複数のグラフを1つの画面で

elastic

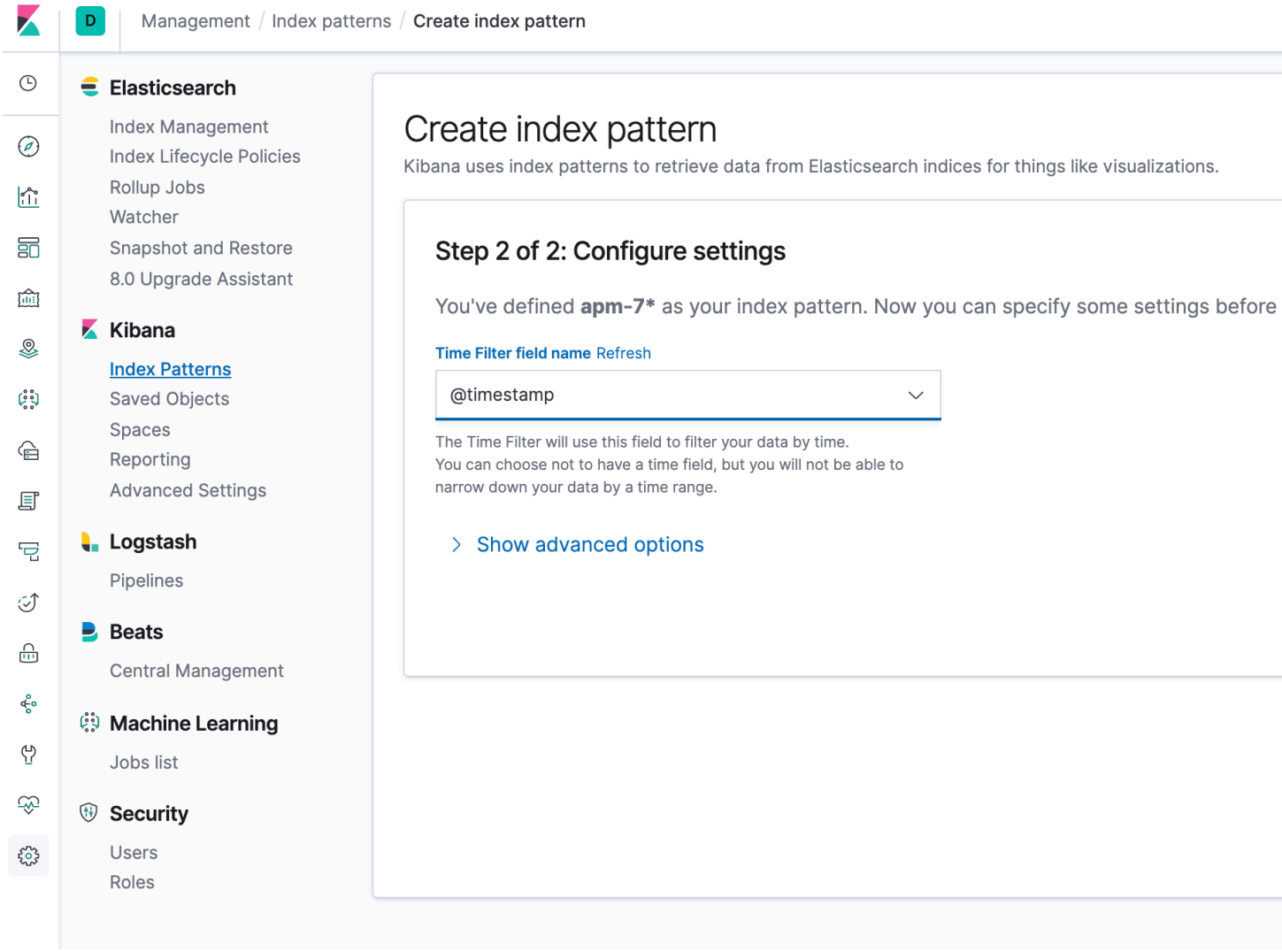
Index Pattern

- データ取得先の設定
- 取得するインデックスの「パターン」を定義



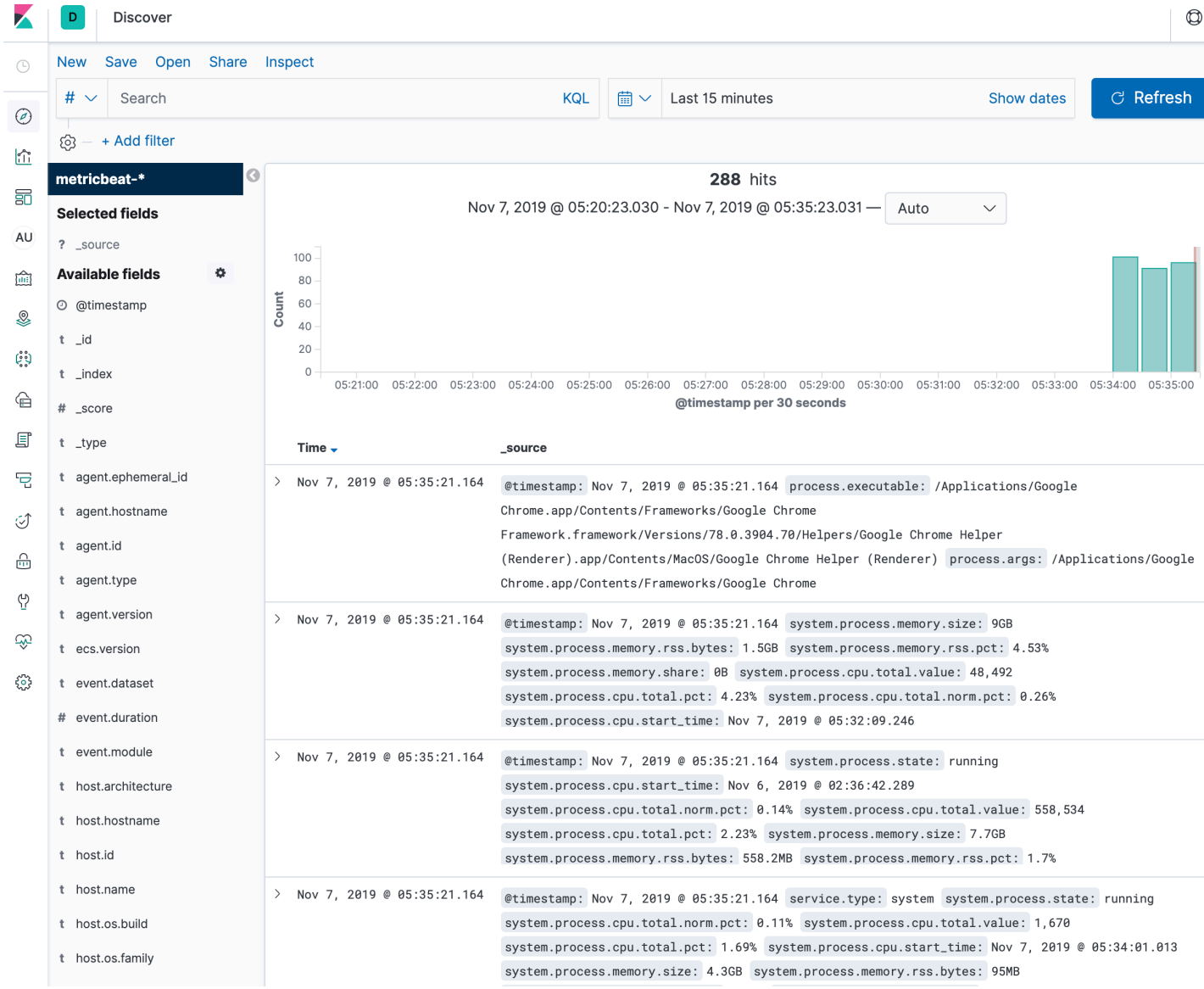
Index Pattern

- 日時のフィールドを指定



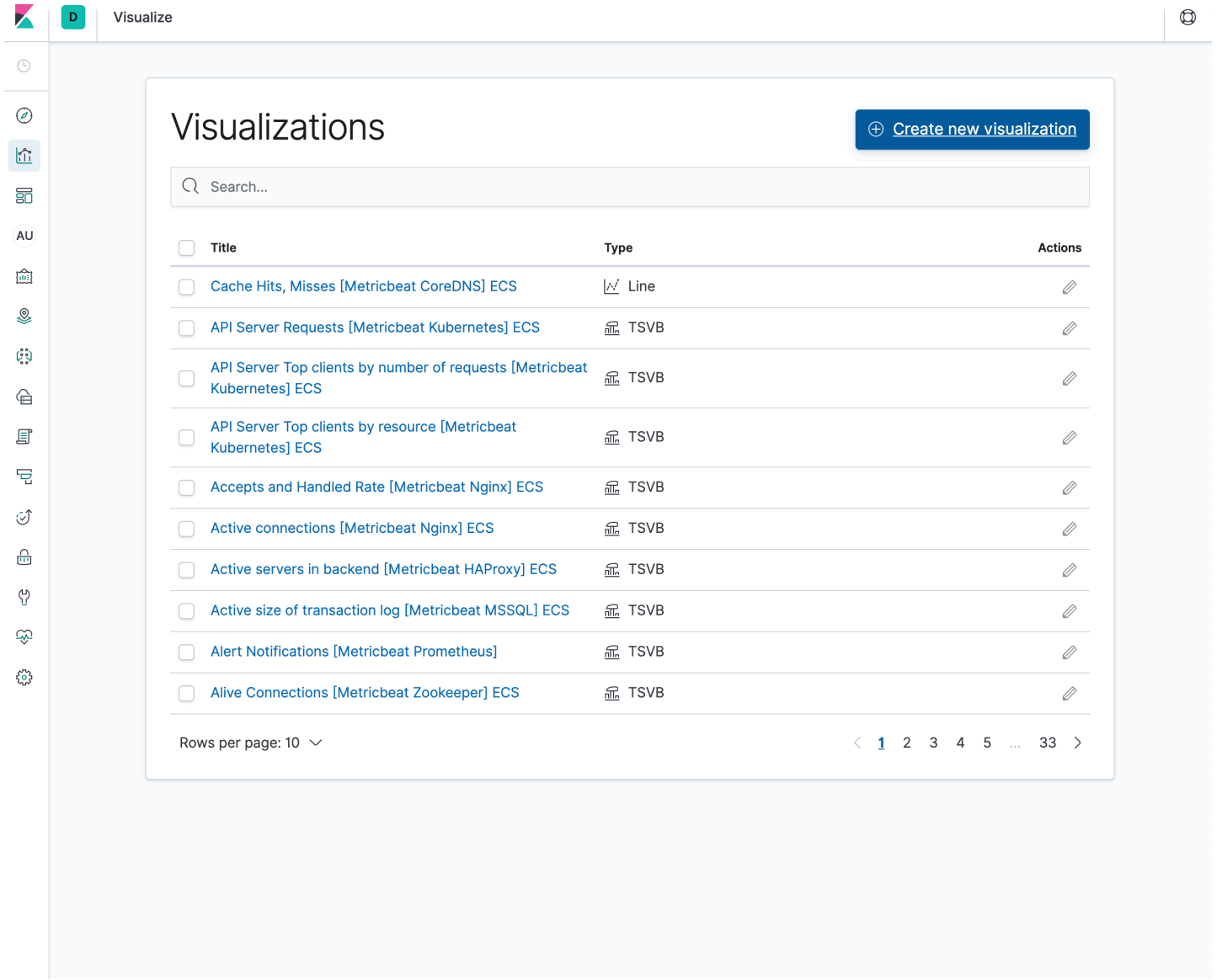
Discover

- データの概観をつかむ



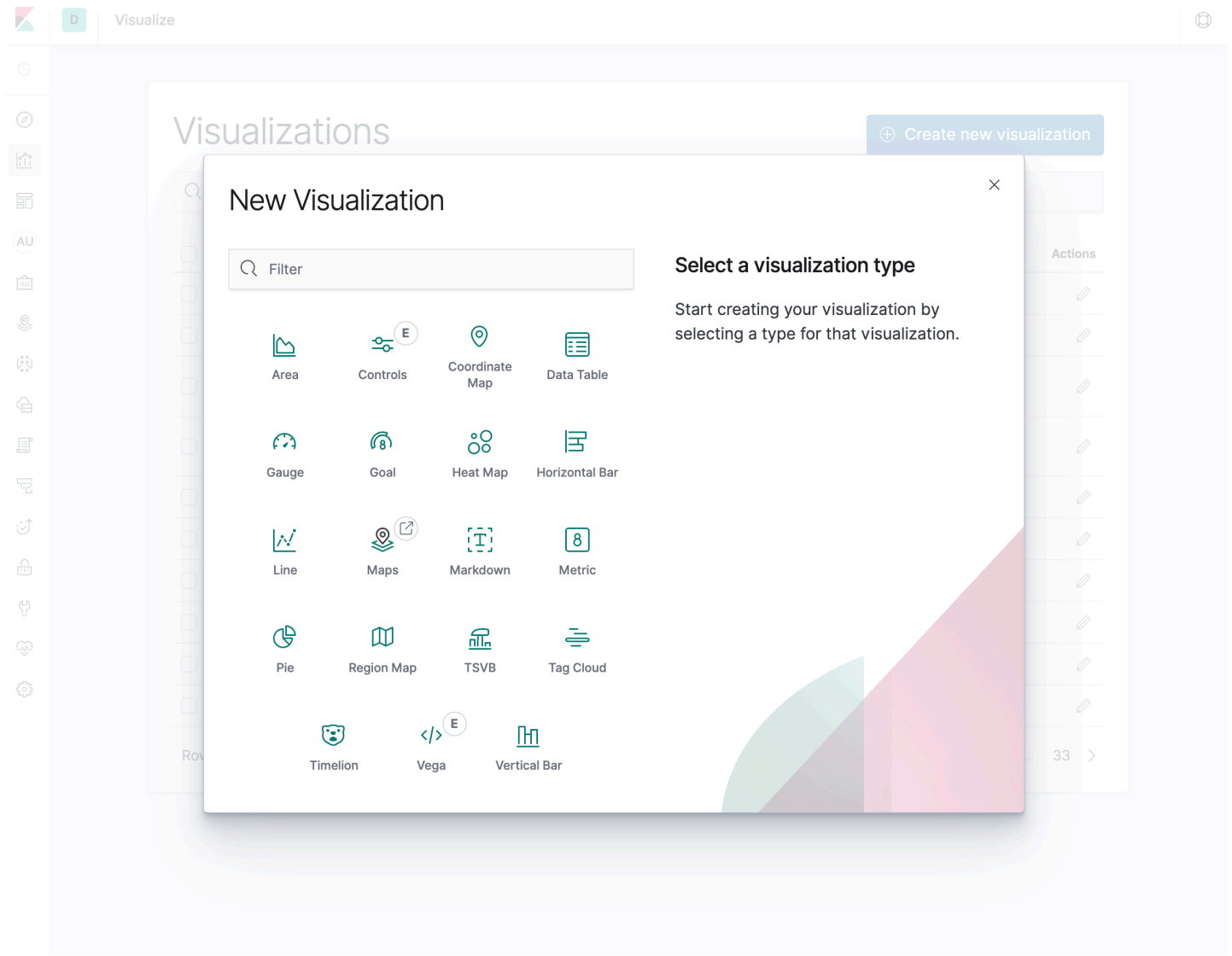
Visualize

- グラフをつくる



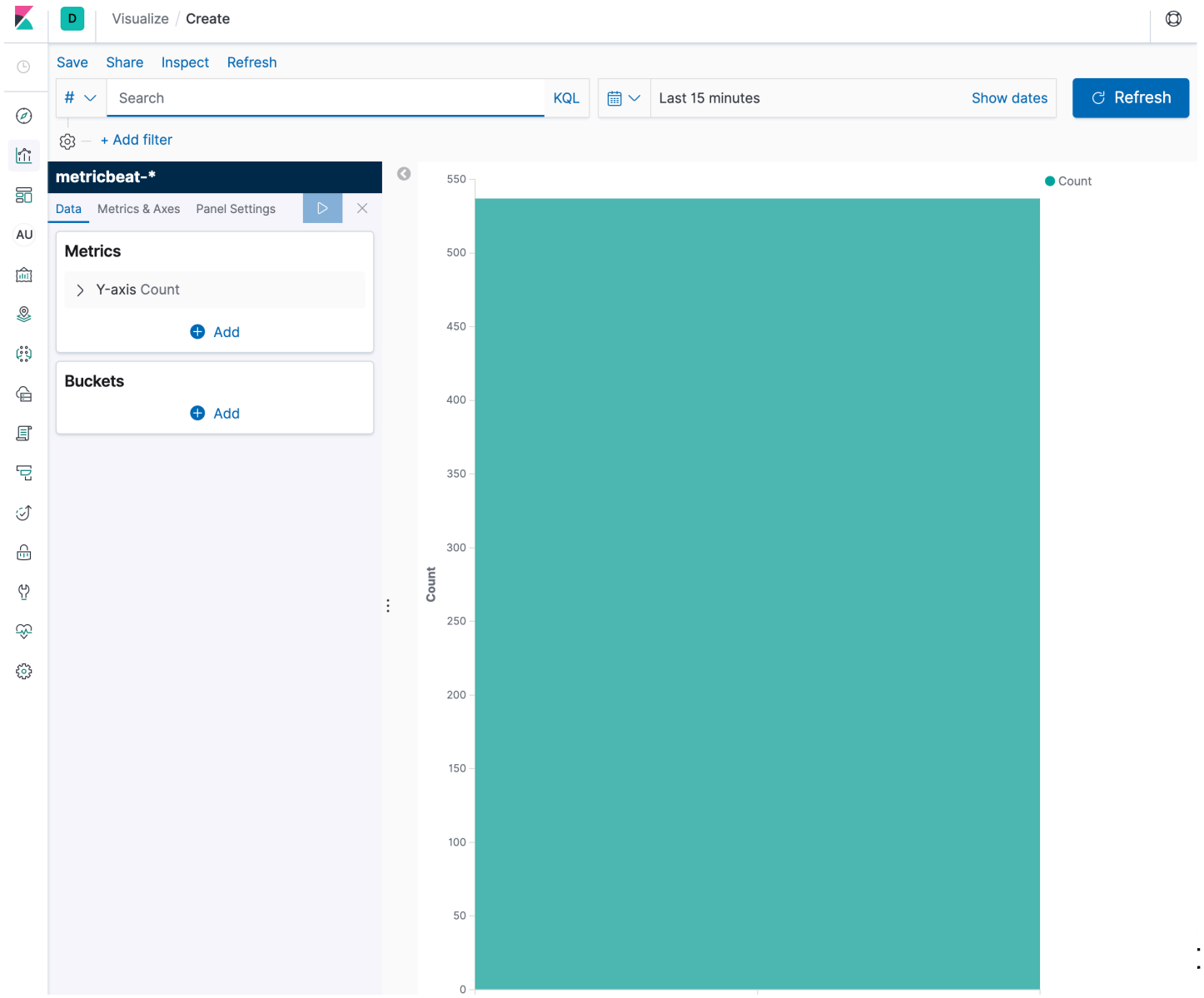
Visualize

- グラフをつくる
- 様々な種類のグラフ



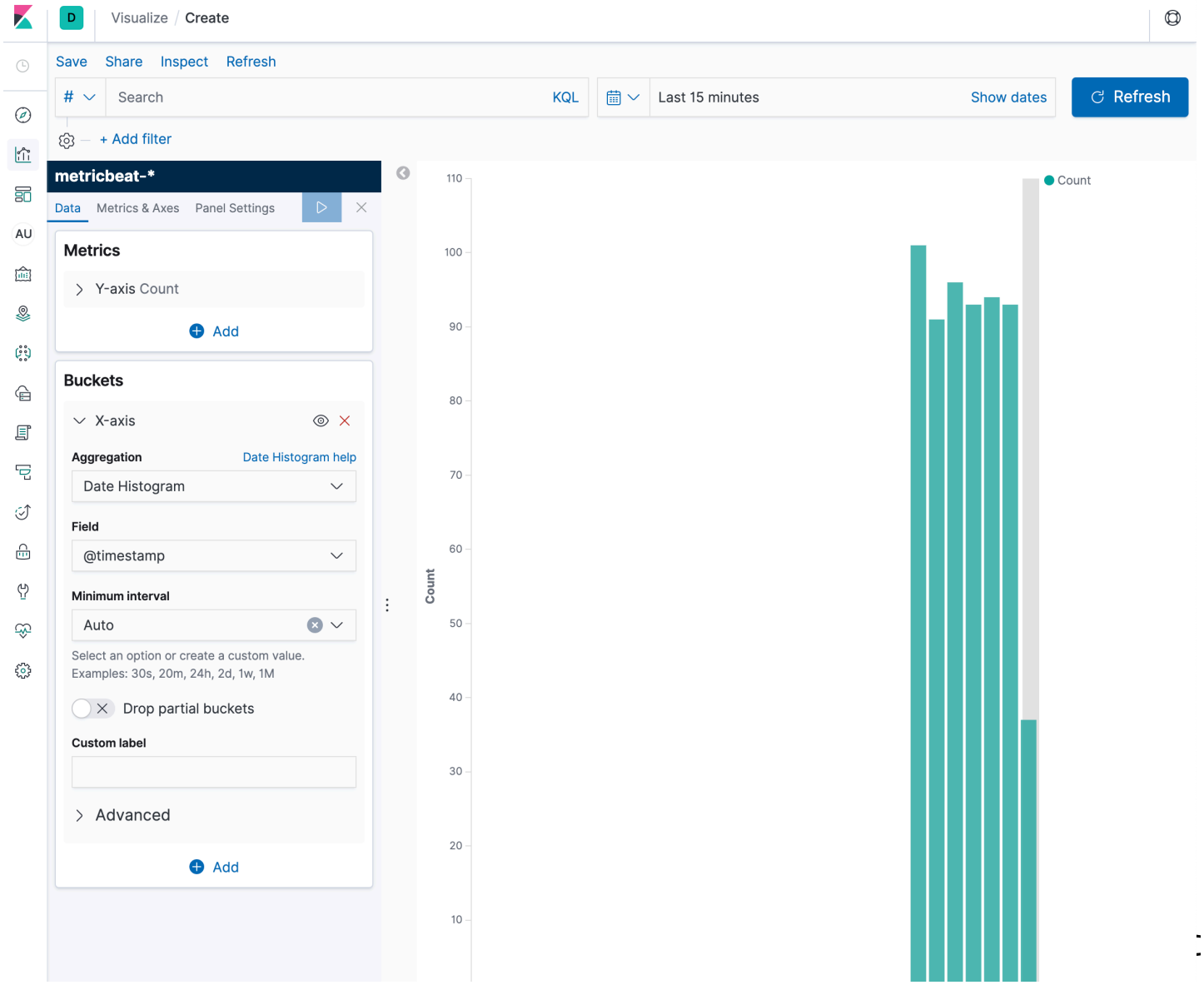
Visualize

- グラフをつくる
- 様々な種類のグラフ



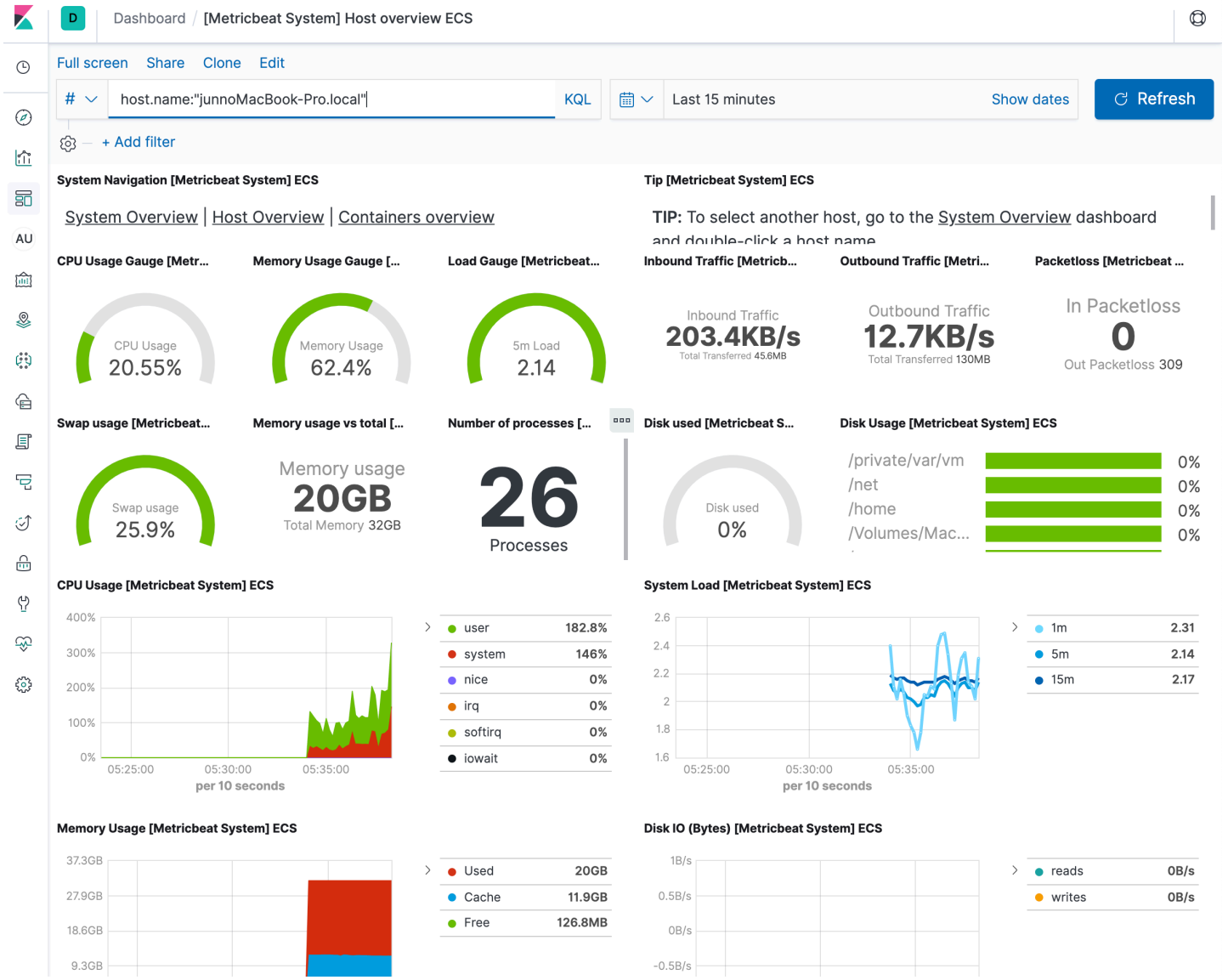
Visualize

- グラフをつくる
- 様々な種類のグラフ



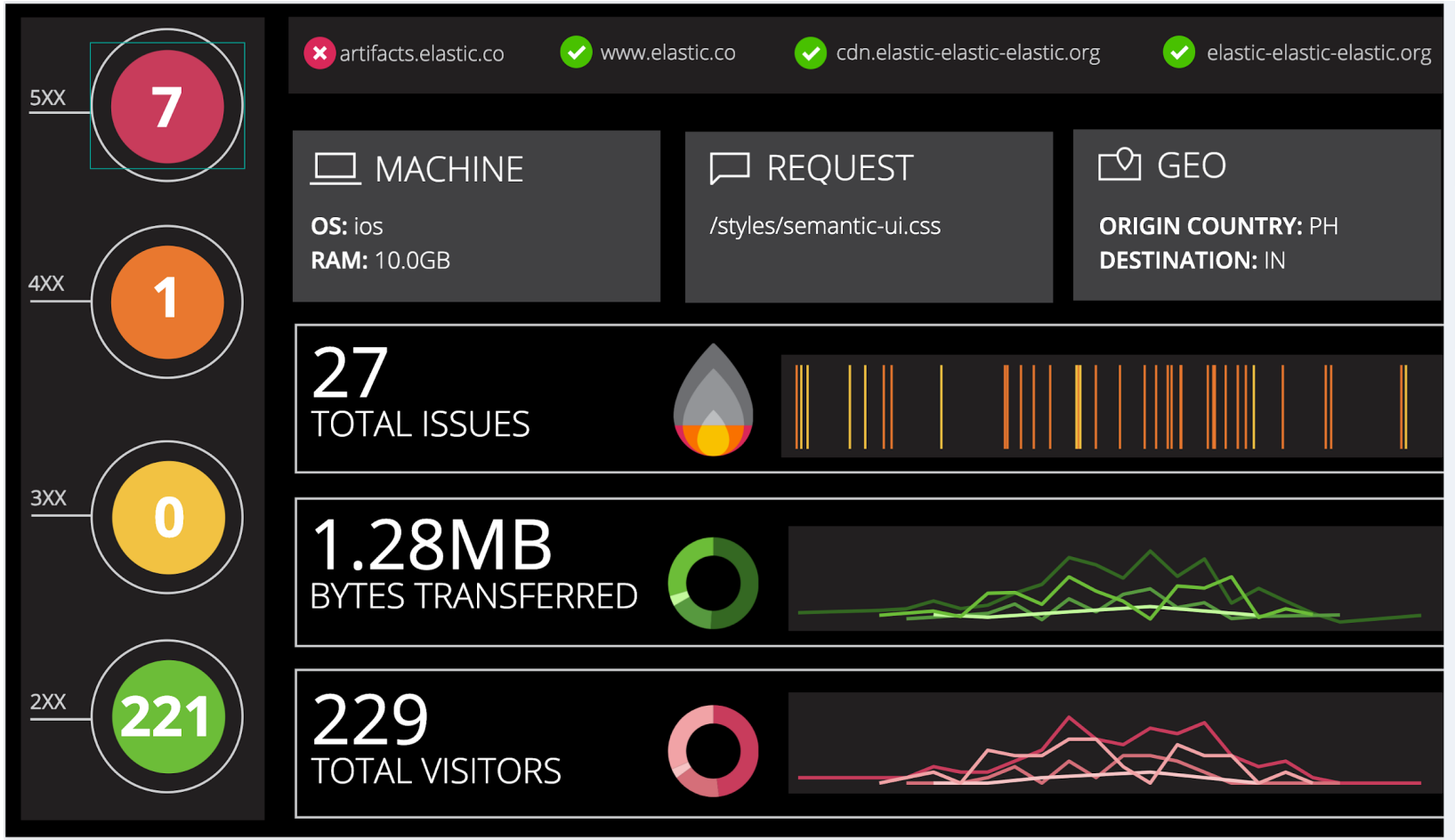
Dashboard

- グラフを並べる
- ダッシュボードをシェア



Canvas: Create live pixel-perfect presentations

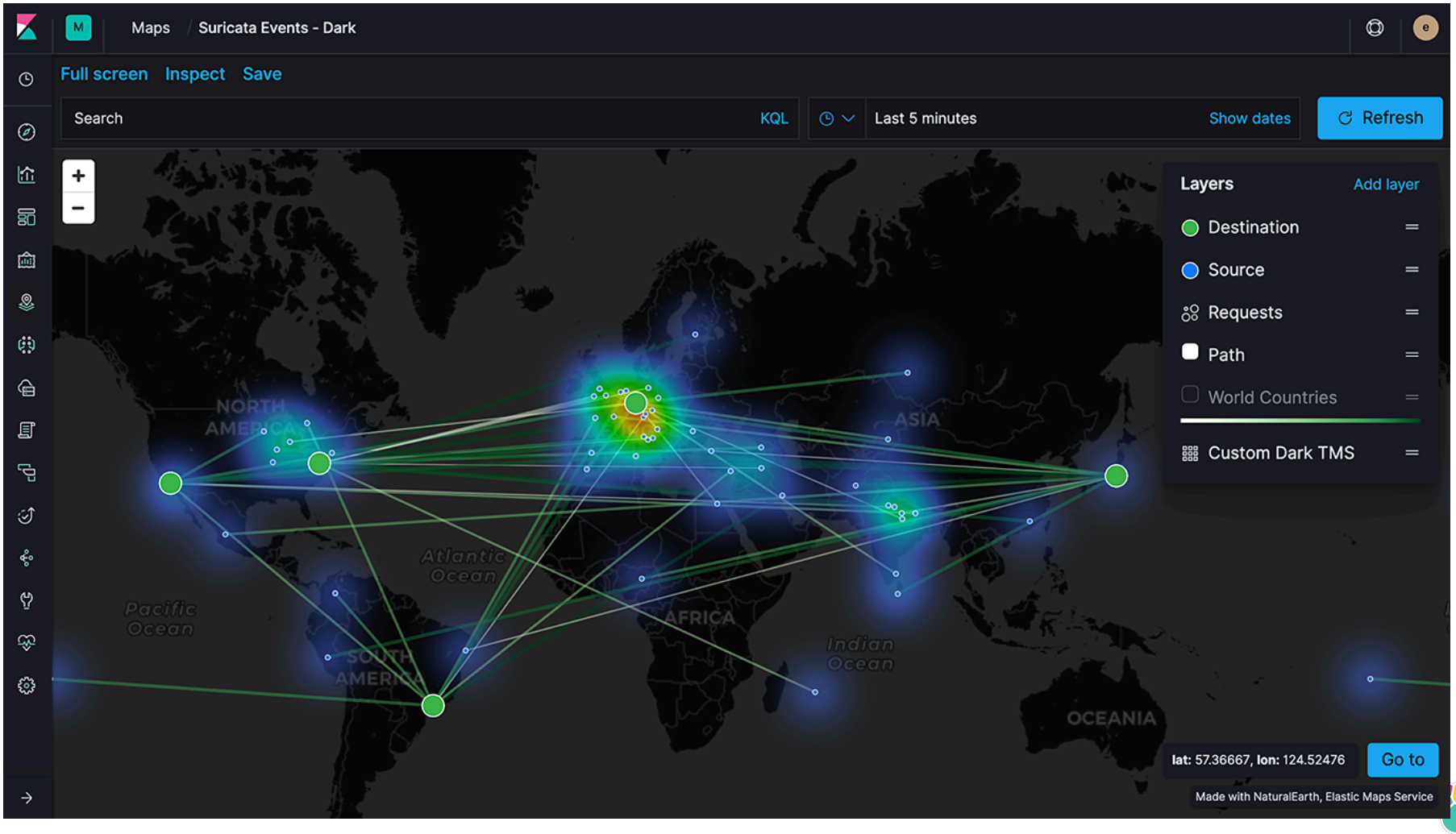
GA | Basic (free)



elastic

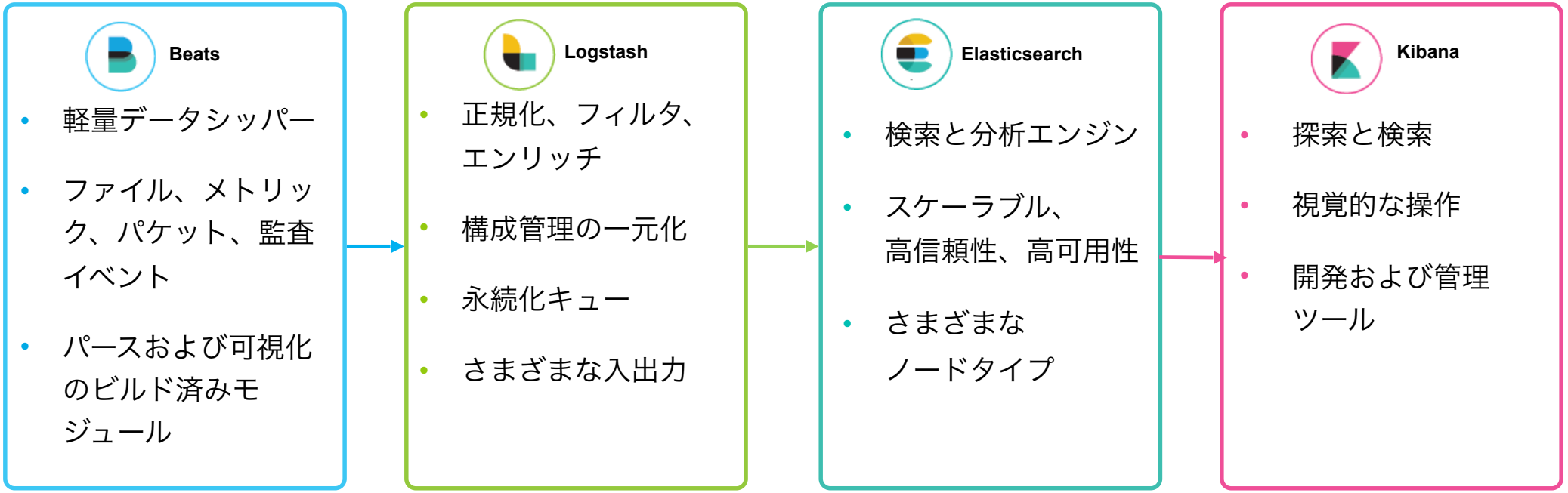
Maps: A new way to explore & visualize geospatial data in Kibana

GA | Basic (free)



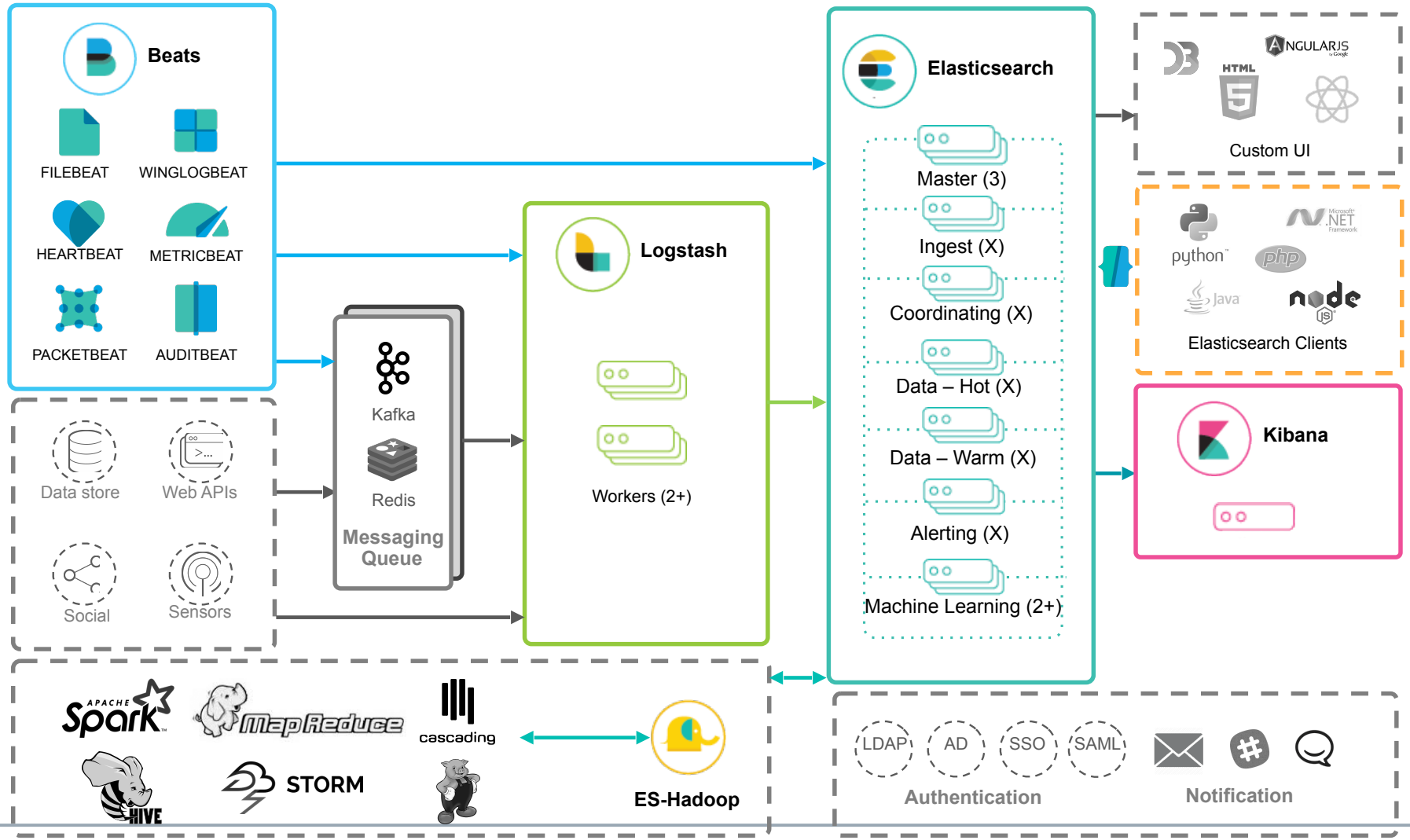
elastic

論理的な処理のパイプライン



elastic

ログやメトリックのためのElastic Stackの構成



elastic

デプロイの**選択肢**

ソリューション

Elastic Stack

Kibana	可視化 & 管理
Elasticsearch	保管、検索、分析
Beats / Logstash	インジェスト

SaaS

Elastic Cloud

SELF-MANAGED

Elastic Cloud Enterprise

Standalone

Elasticsearch Service

No one hosts the stack better

Cluster management made easy

One-click deploy and upgrade

Scale up / down with sliders

Auto backup every 30 minutes

Any use case. Any size.

Predefined deployment templates

Hot-warm + index curation

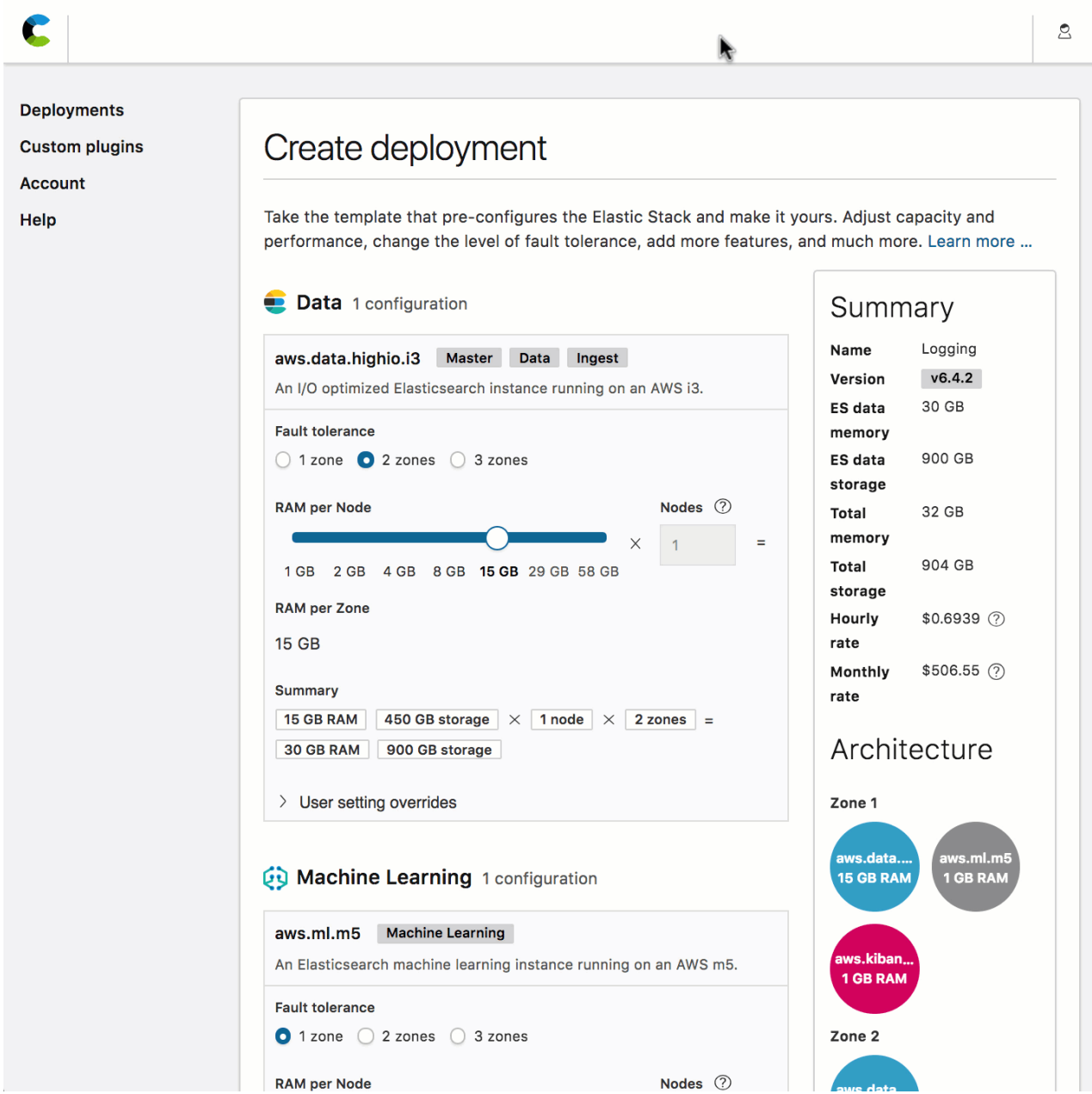
Dedicated master nodes

Exclusive Elastic Stack features

Canvas, Elasticsearch SQL, Rollups

Graph, Machine Learning, Security,

Alerting, Monitoring, and growing.



Elastic Cloud Enterprise

Productizing years of SaaS expertise

Manage deployments @ scale

Deploy anywhere

Easy deploy, scale up, upgrade

Auto backup every 30 minutes

Any use case. Any size.

Customizable deployment templates

Hot-warm + index curation

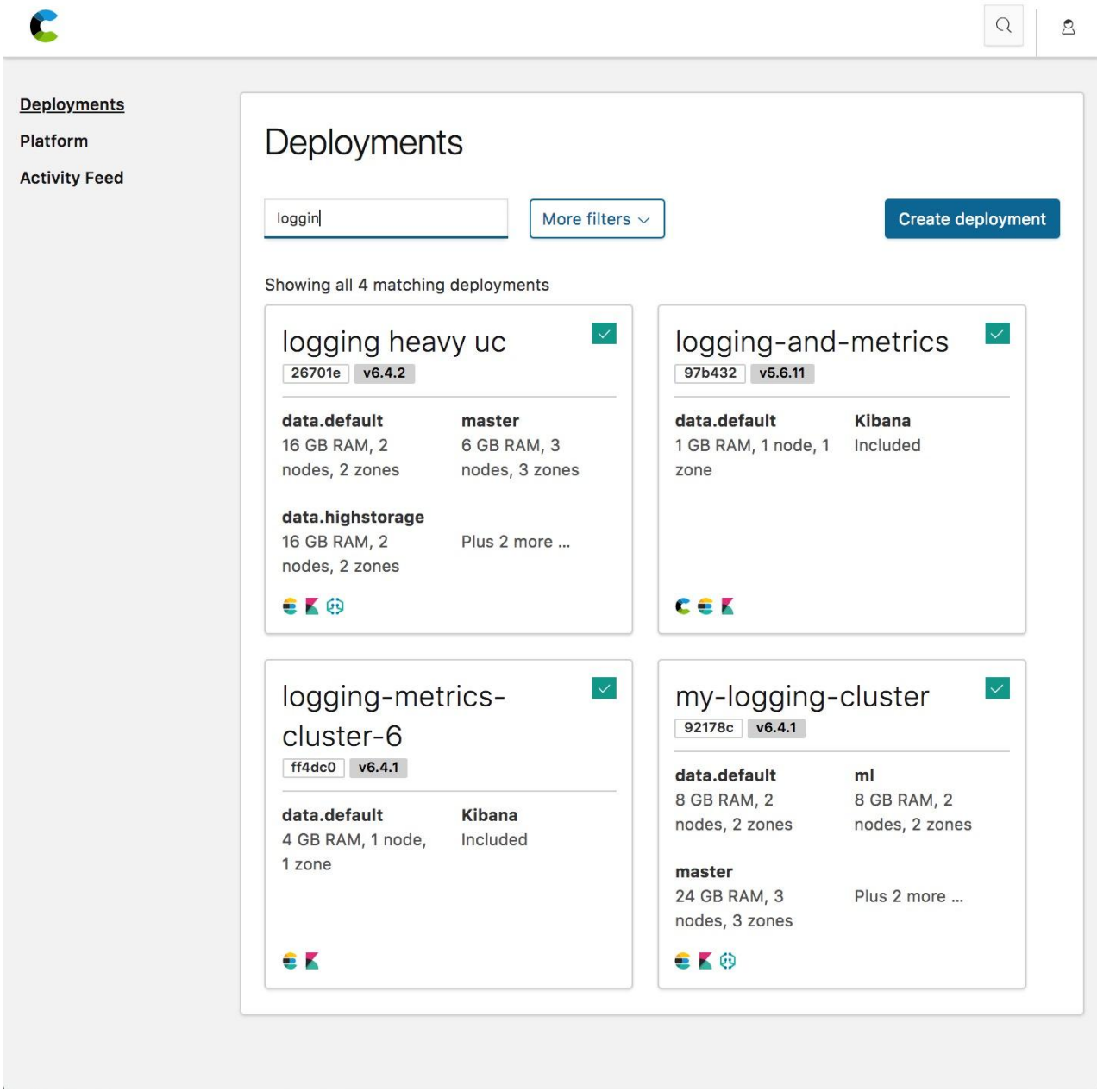
Dedicated master nodes

Elastic Stack features

Canvas, Elasticsearch SQL, Rollups

Graph, Machine Learning, Security,

Alerting, Monitoring, and growing.



Standalone

- Tar.gz / Zip
- DEB / RPM
- Homebrew
- Windows Installer

Kubernetes?

Docker @ Elastic

先ほど紹介した4つのプロダクトについてDockerのイメージを配布

https://www.docker.elastic.co/

Elastic Cloud on Kubernetes

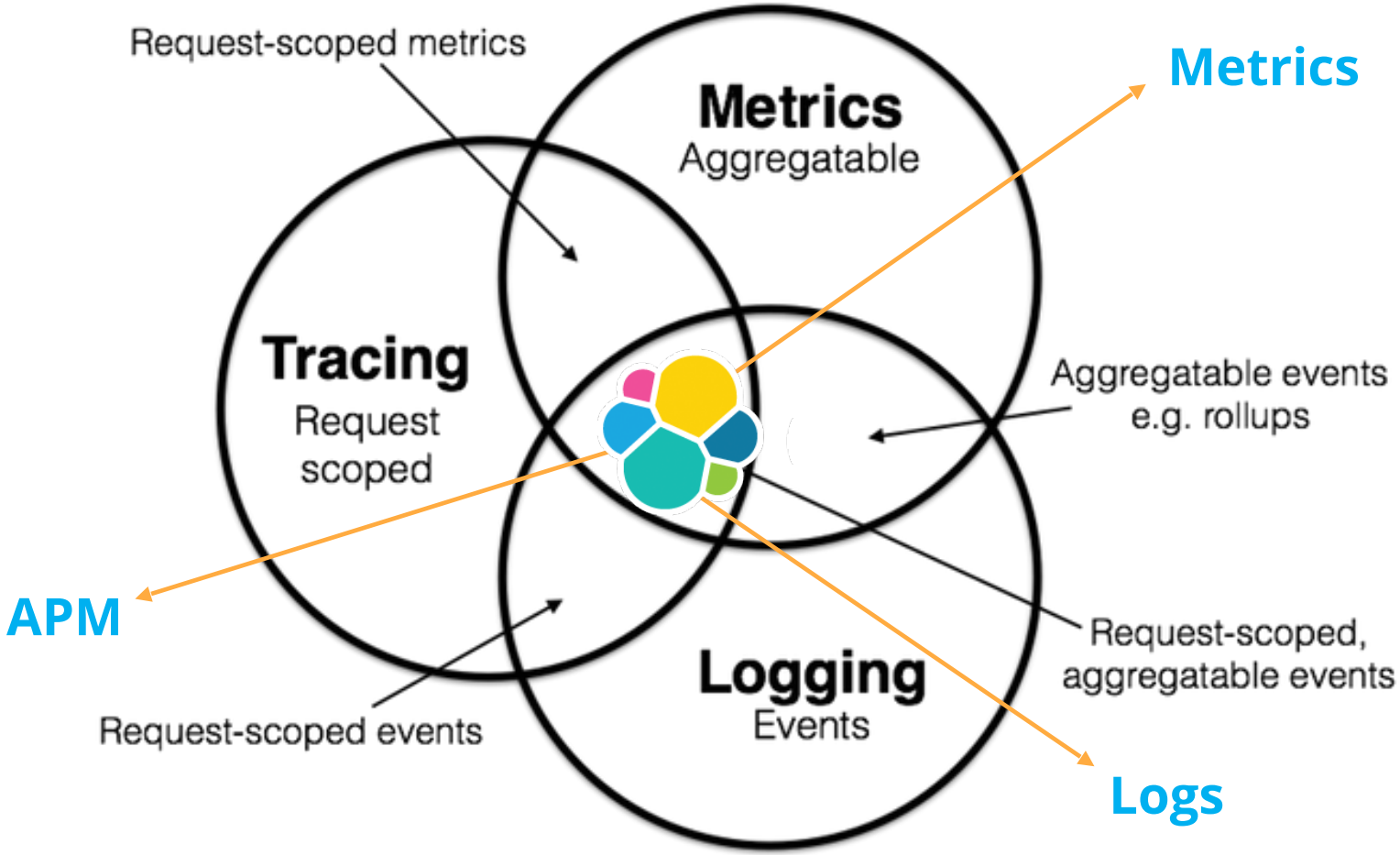
ElasticsearchとKibanaのoperatorを公式にサポート(ECK):

1. 利用方法 : `kubectl apply -f https://download.elastic.co/downloads/eck/0.8.1/all-in-one.yaml`

elastic

Observability は検索のユースケース

オブザバビリティの三要素 : Logging、 Metrics、 APM



検索と探索

相関

異常値検知

アラート

ダッシュボード

レポート

Reference : Peter Bourgon https://peter.bourgon.org/blog/2017/02/21/metrics-tracing-and-logging.html:

elastic

効果的なオブザバビリティ

さまざまなものを測定しなにが重要か

- エコシステムの健全性を示す相関的なデータに基づいた明確で意味のあるハイレベルなメトリックを測定

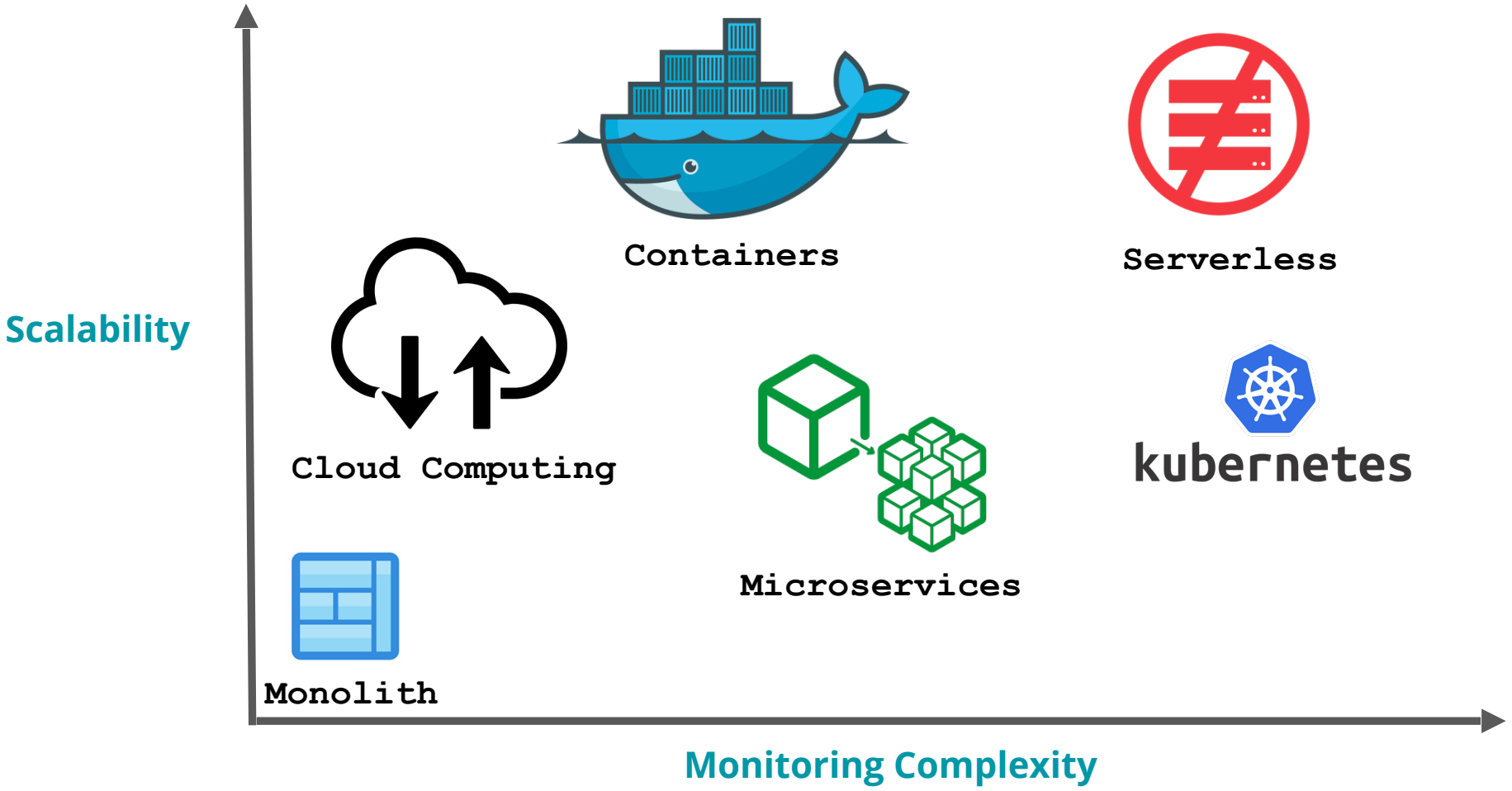
- リアルタイムな探索や重要なイベントをアラートするために異常値を自動で検知

- ハイレベルからディープダイブや、さまざまなデータをいつでも高速かつスケーラブルに関連付け、横断的な探索を可能にし、「何？」や「なぜ？」の答えるを効率よく探す

References:
Google SRE Handbook : https://landing.google.com/sre/sre-book/toc/index.html
Cindy Sridharan : https://medium.com/@copyconstruct/monitoring-and-observability-8417d1952e1c

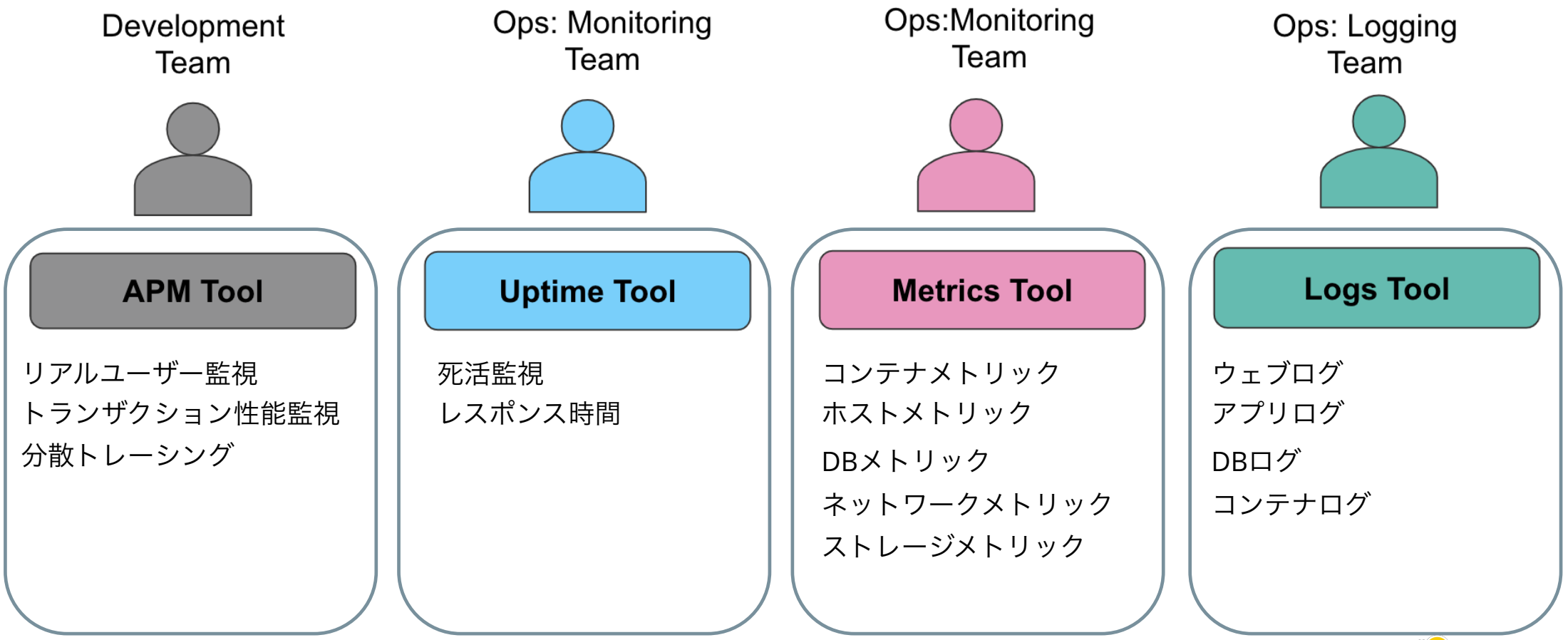
elastic

アーキテクチャの進化に関する監視の観点



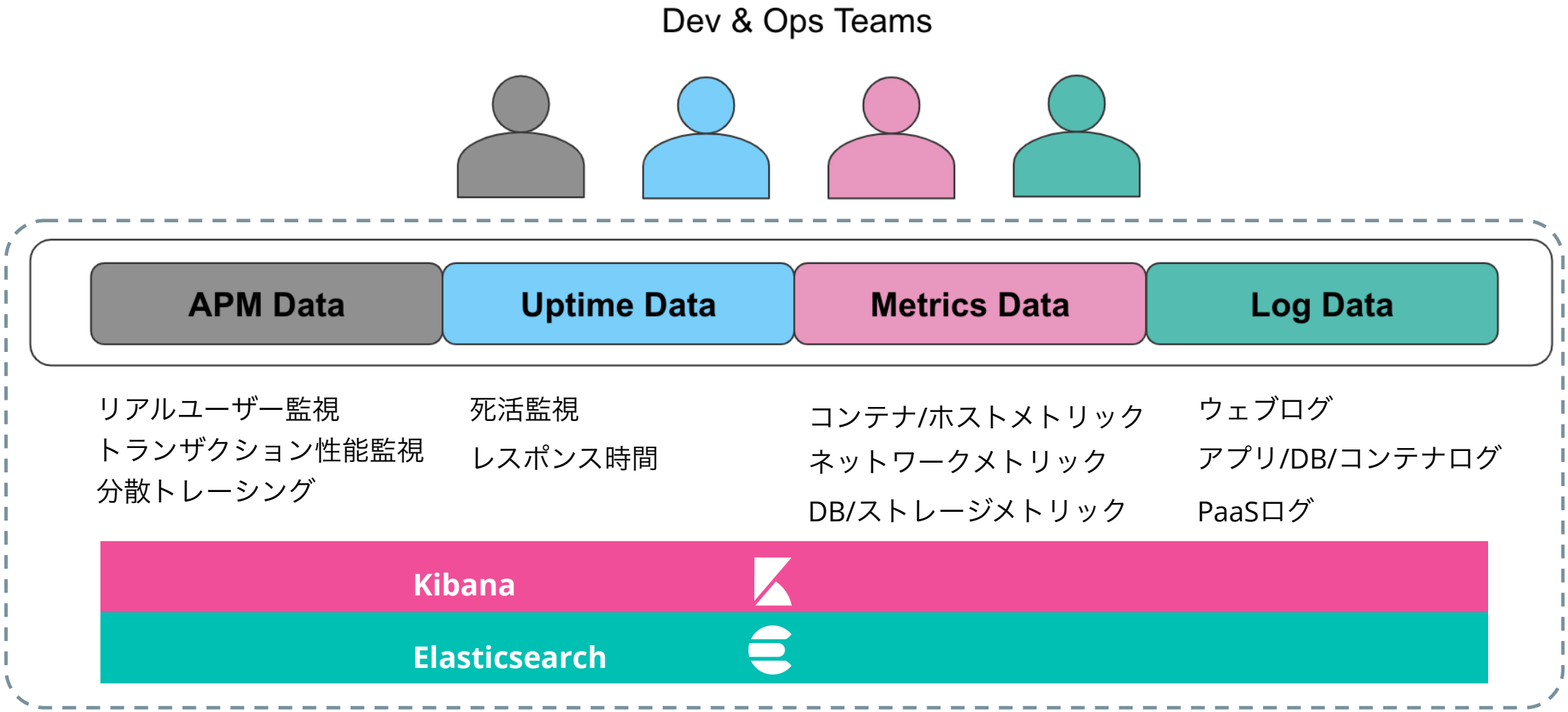
elastic

現状：サイロ化されたツール群



elastic

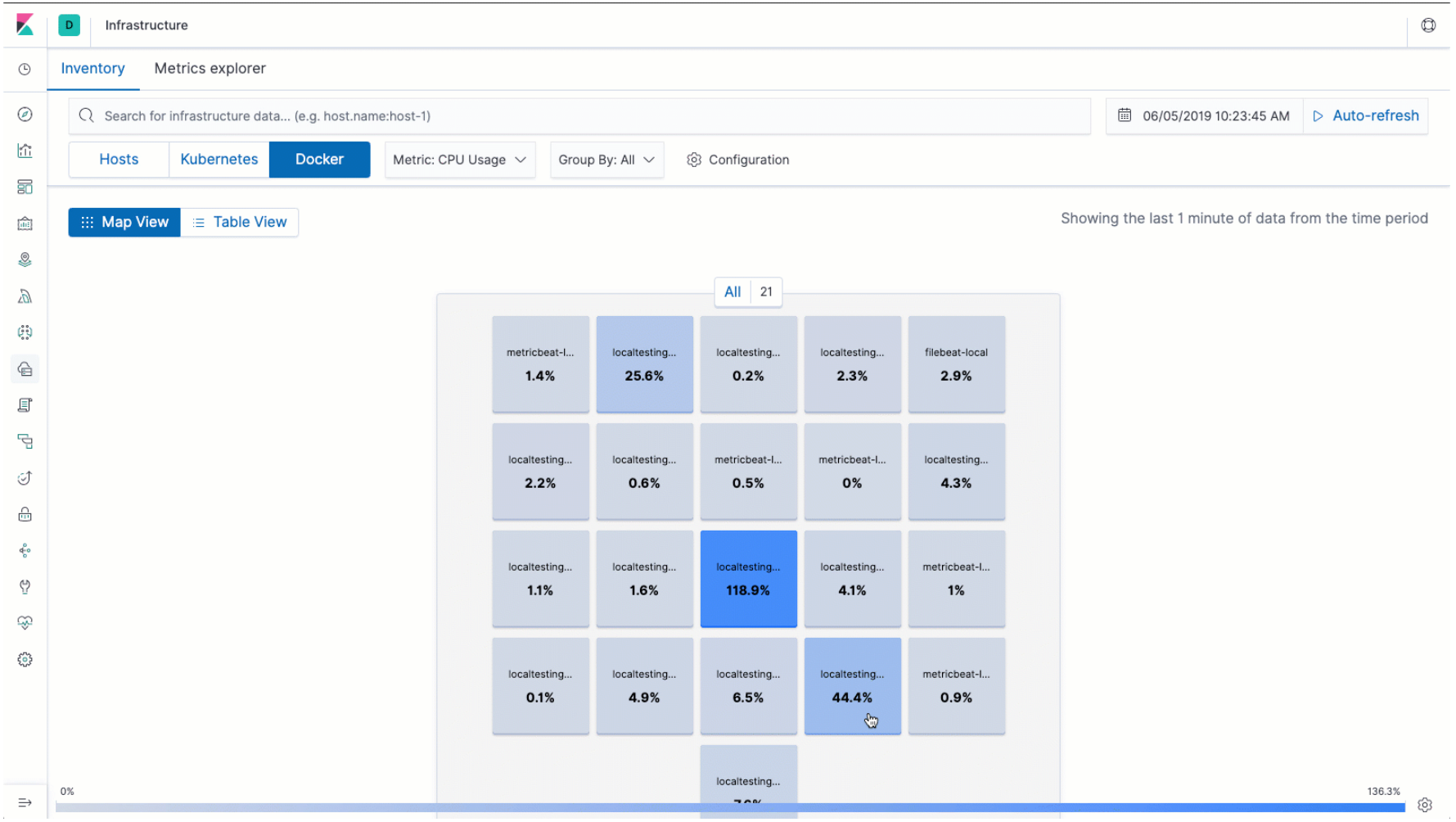
Elastic Stackを利用したオブザバビリティ



elastic

ログ、メトリック、APM、アップタイム間での統一された可視性

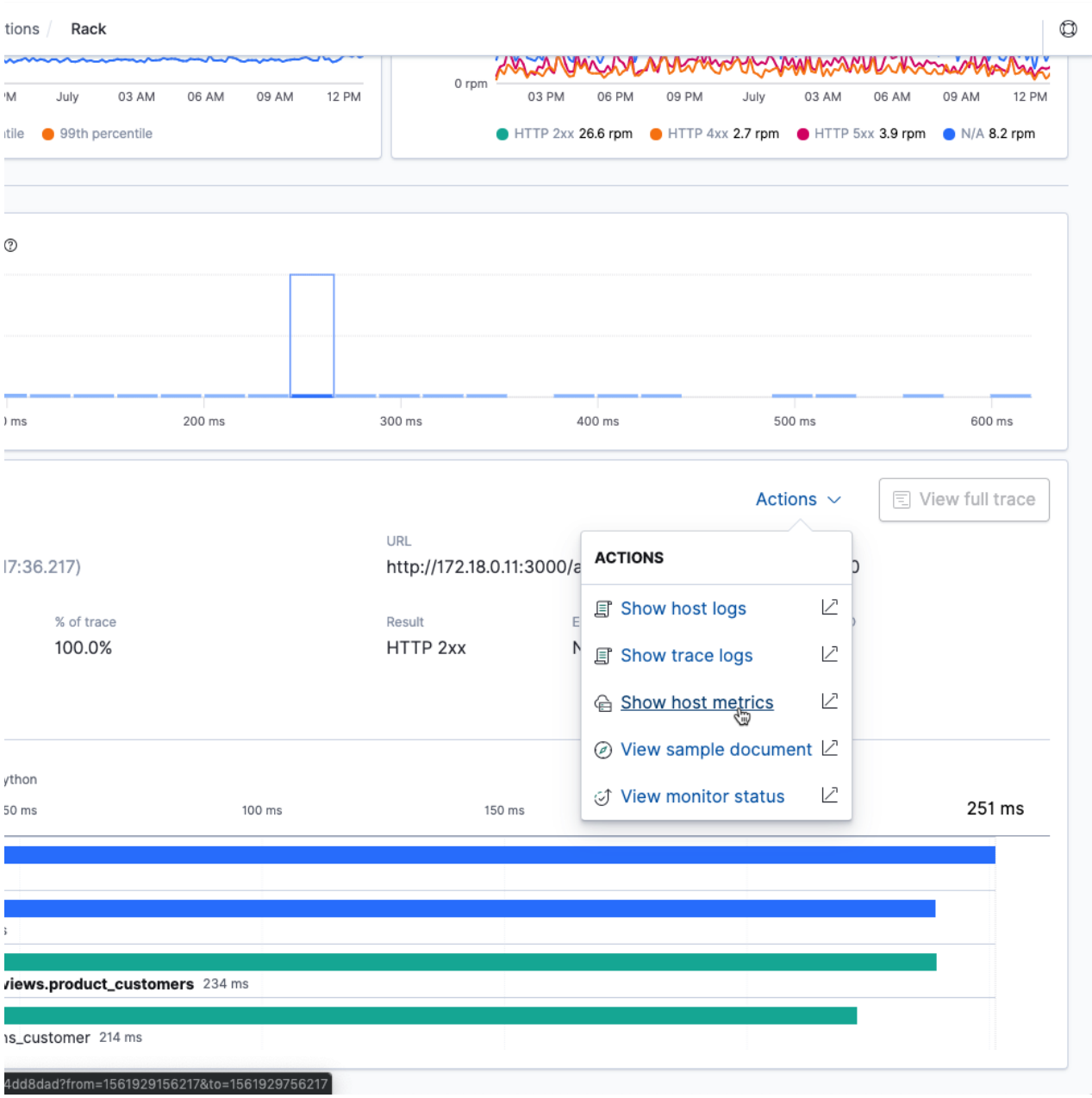
Observabilityのそれぞれの要素をワンクリックで統合



統一されたObservability
なぜ重要なのか？

一枚のガラス

- 合理的な分析ワークフロー
- より素早く問題を解決
- コンテキストを引き継ぐ
- オペレーションコストの削減



ログ、メトリック、APM

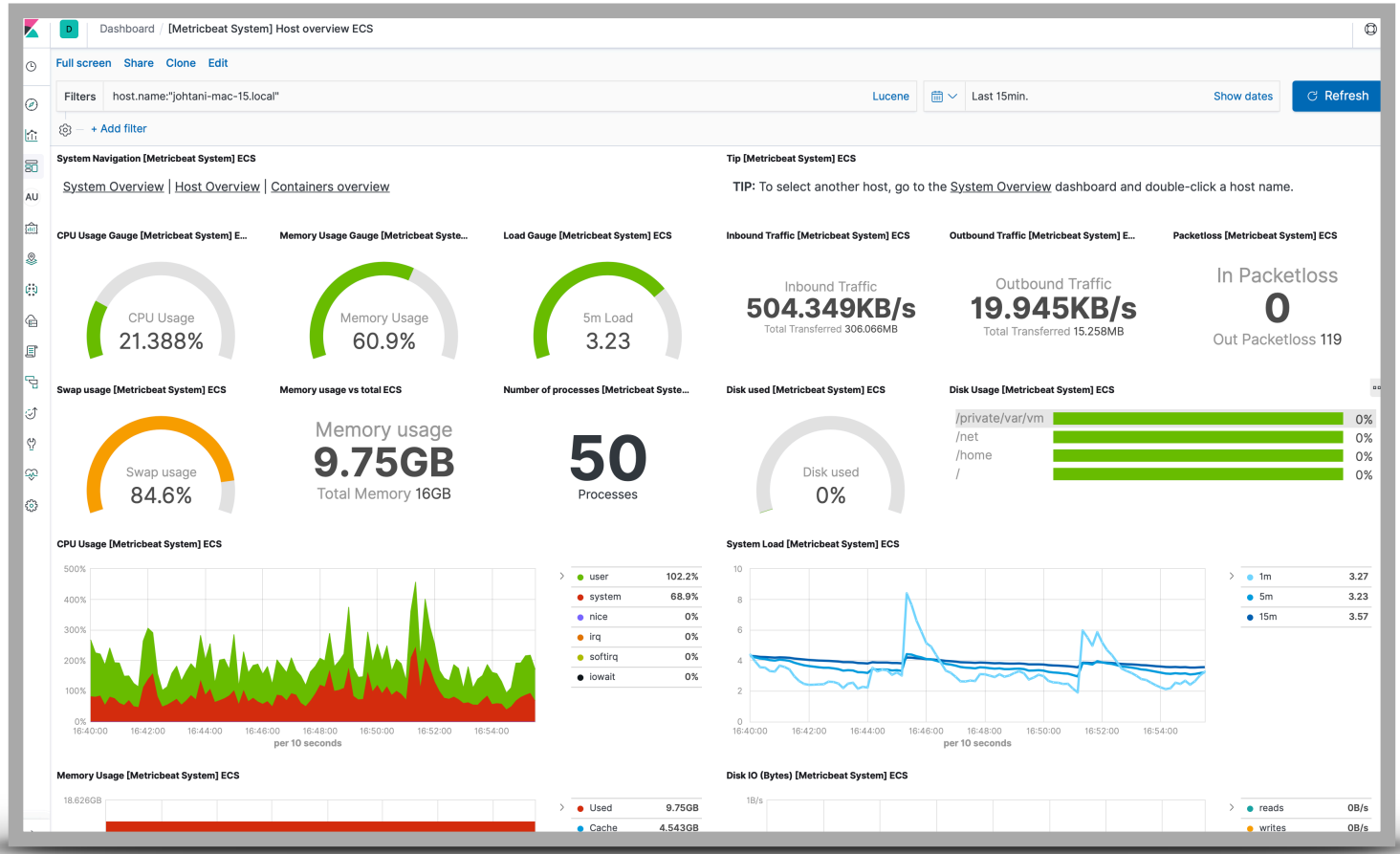
Kibanaひとつですべてをカバー

メトリック

Metricbeat & Heartbeat

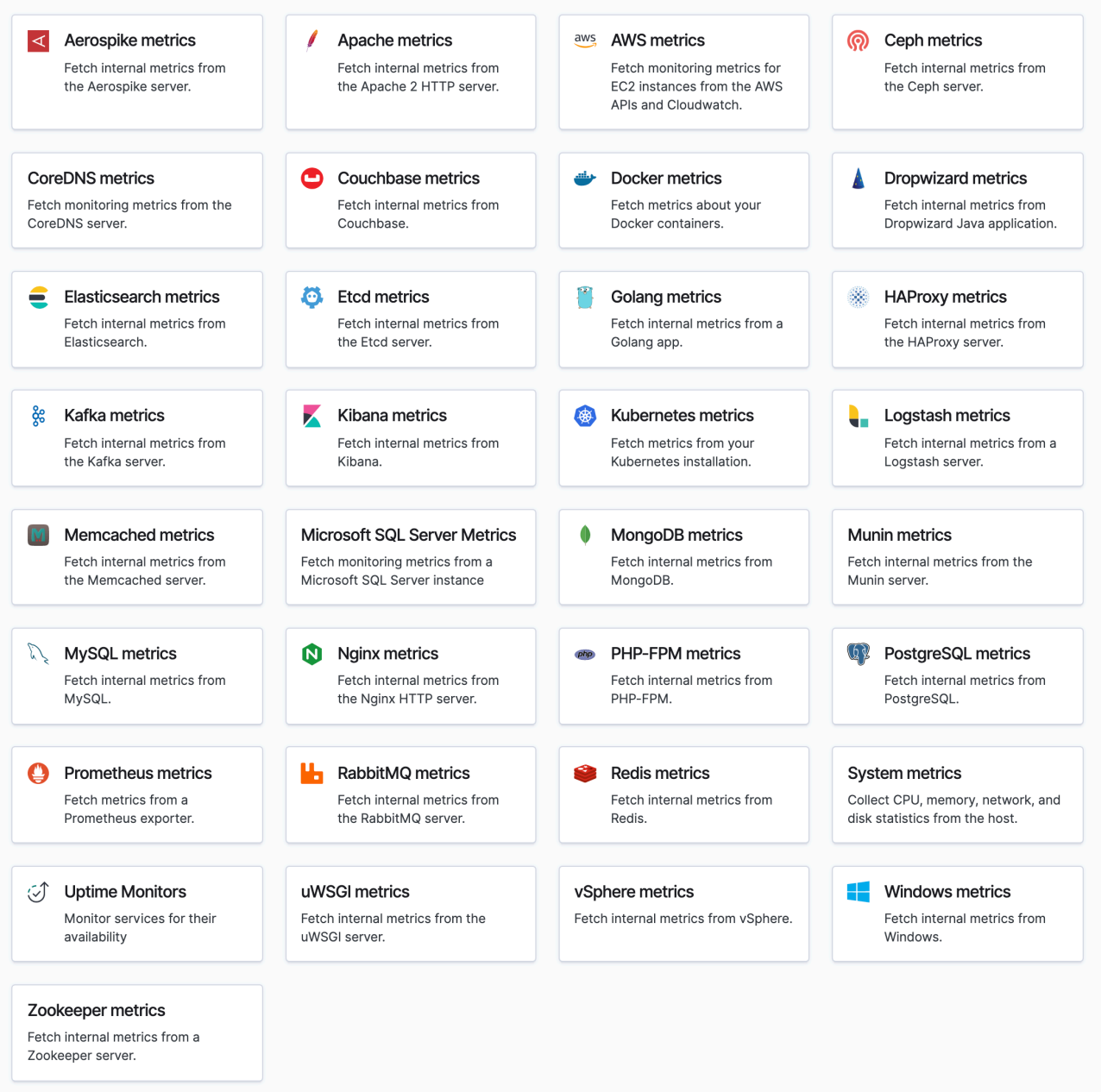
Metricbeat

システムや
アプリの
メトリックを収集

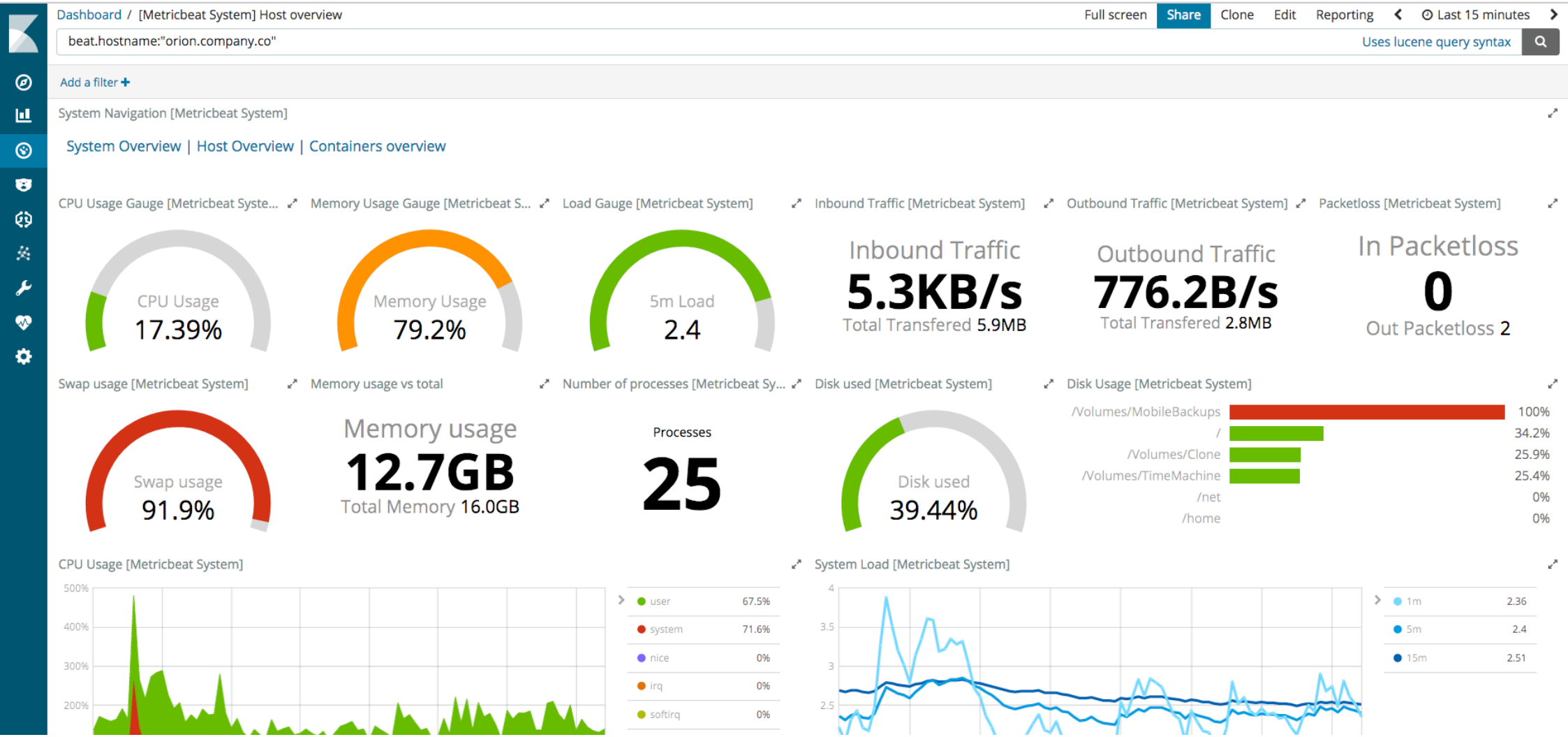


Metricbeat

多くの
モジュール



すぐ使えるダッシュボードとデータソース（増加中）



モジュールとは？

- 手軽にデータの取得から可視化までを提供する仕組み
  - 対象とするシステム、ミドルウェアごとに提供
- 事前に定義された取得データ
  - データソースごとに項目を選別済み、定義
- サンプルとなるグラフおよびダッシュボード
  - Kibanaのグラフ、ダッシュボードも定義済み

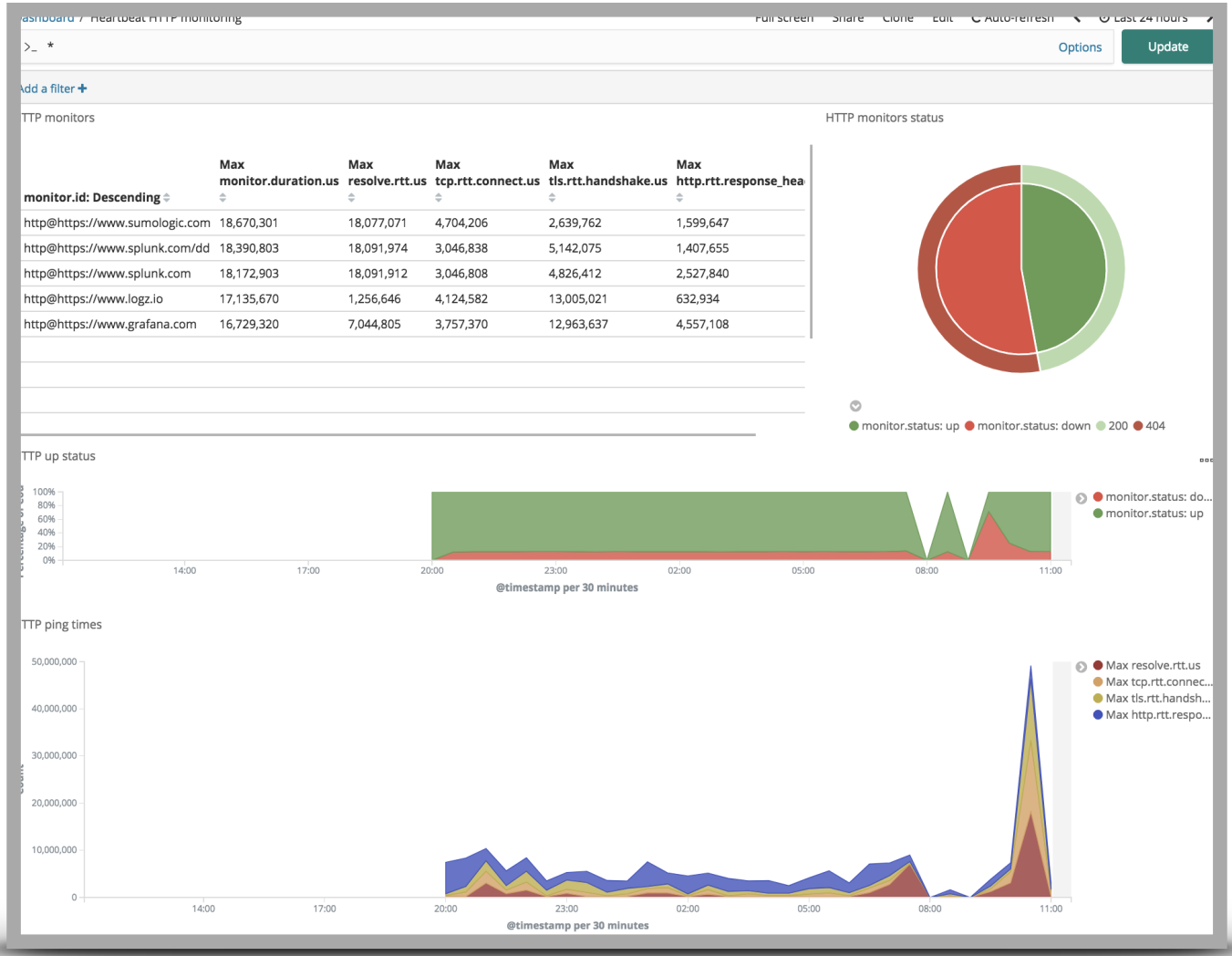
モジュールを構成するもの - Metricbeat

- メトリックセット (Beats)
  - データの名前とデータの型 - 例 : system moduleのCPU metricset
- インデックステンプレート (Elasticsearch)
  - スキーマ定義 - Elasticsearchでのフィールド名と型
- グラフ & ダッシュボード (Kibana)
  - グラフの定義 - どのフィールドでどんなグラフが構成されているか

Heartbeat

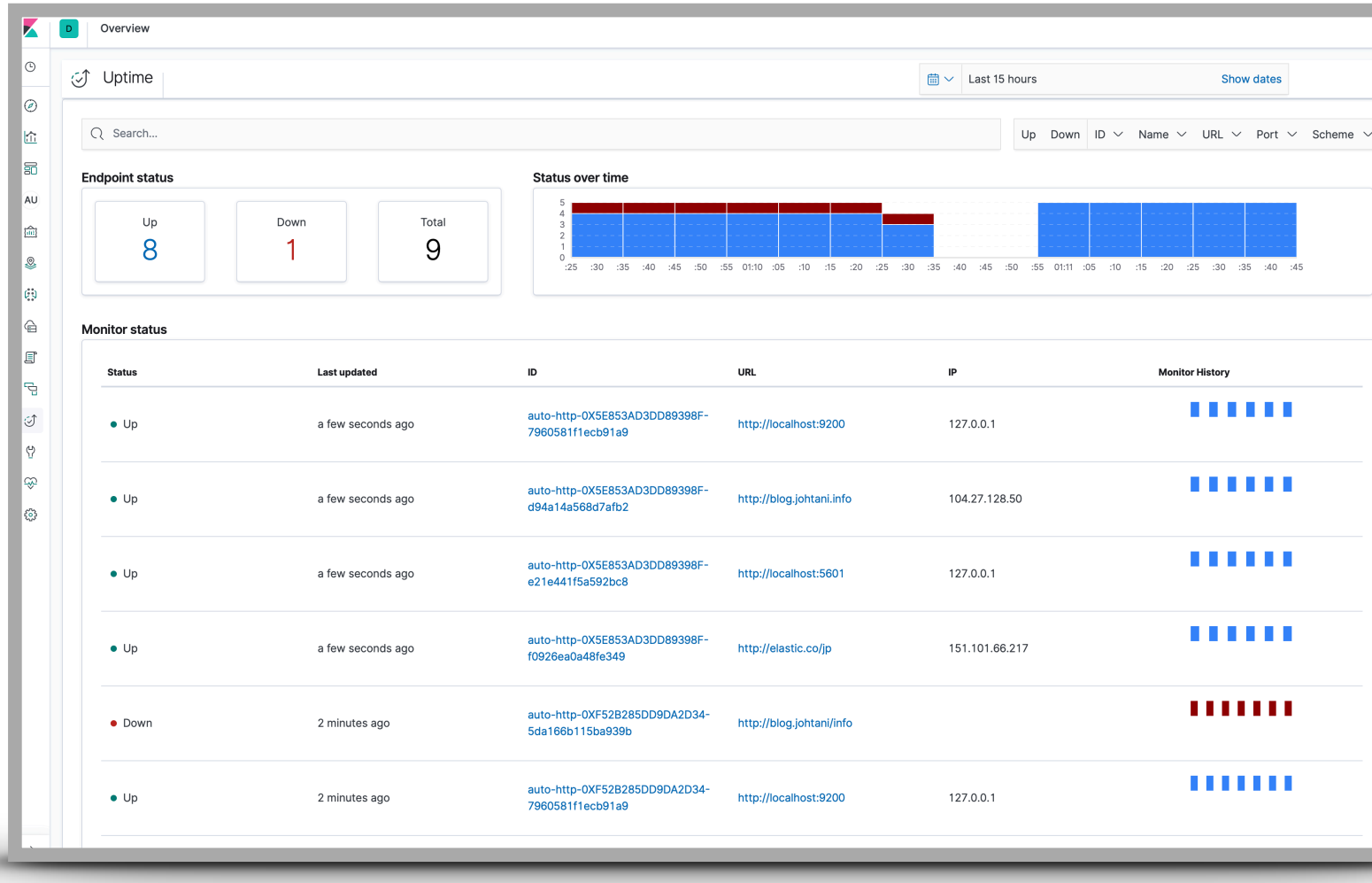
軽量な

外形監視



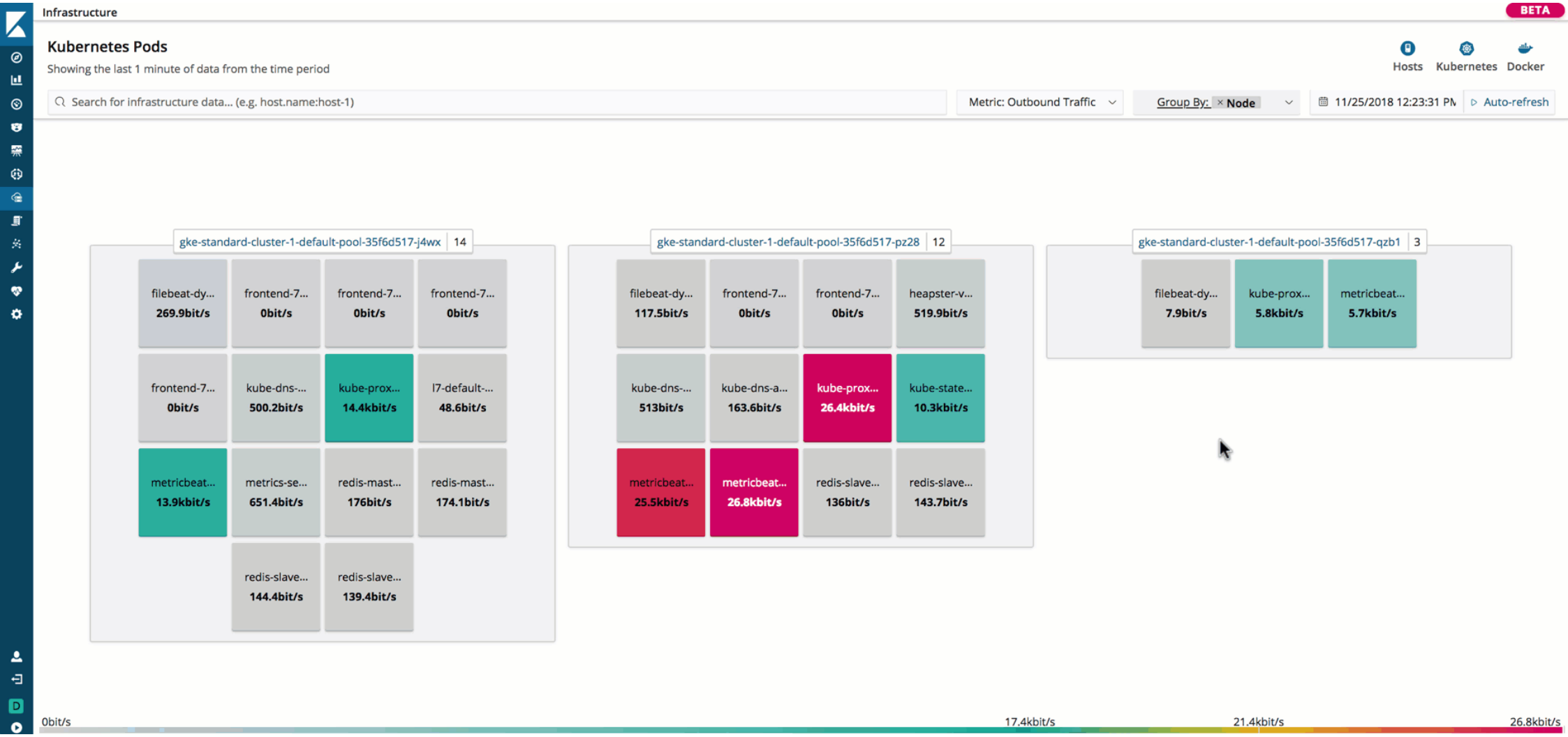
Uptime UI

外形監視の
専用UI



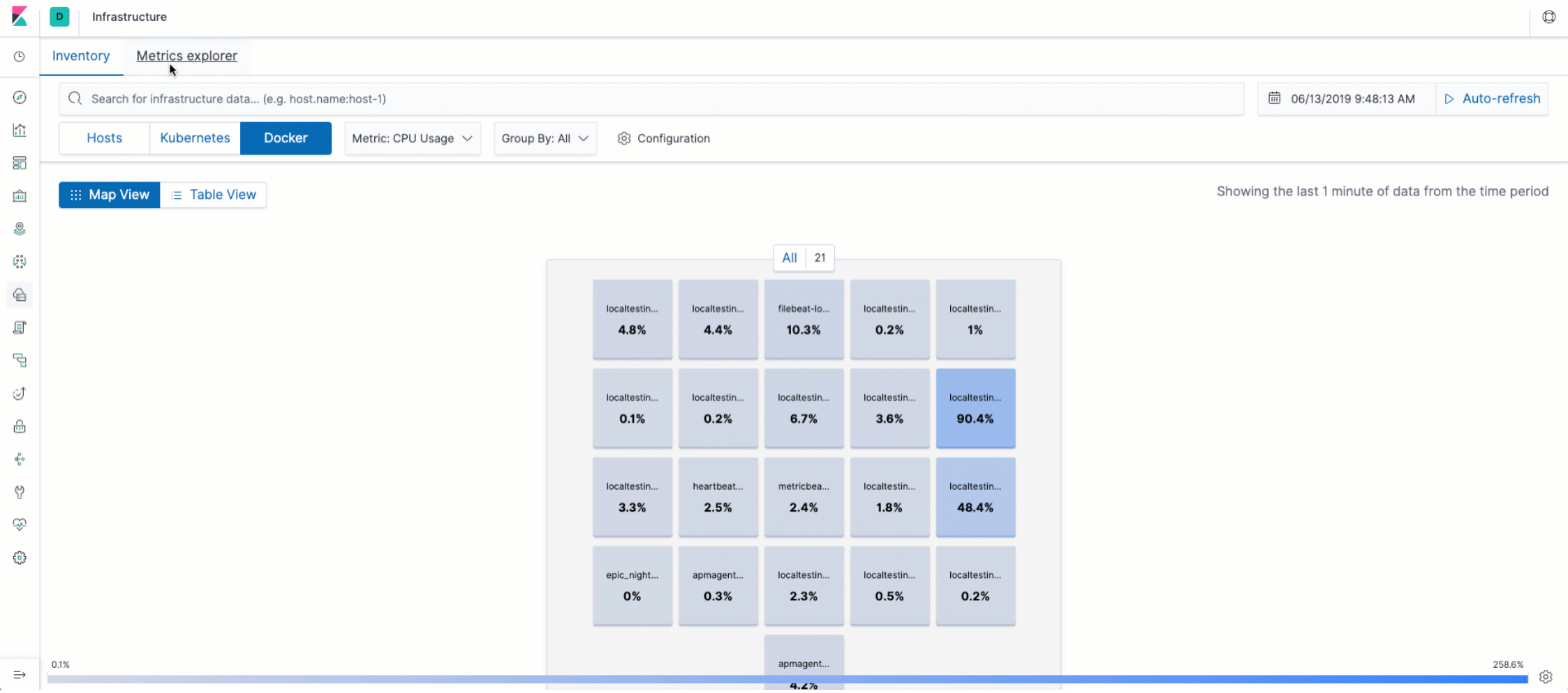
インフラUI

俯瞰的に多くのサーバーを監視



Metrics Explorer

アドホックな時系列の可視化

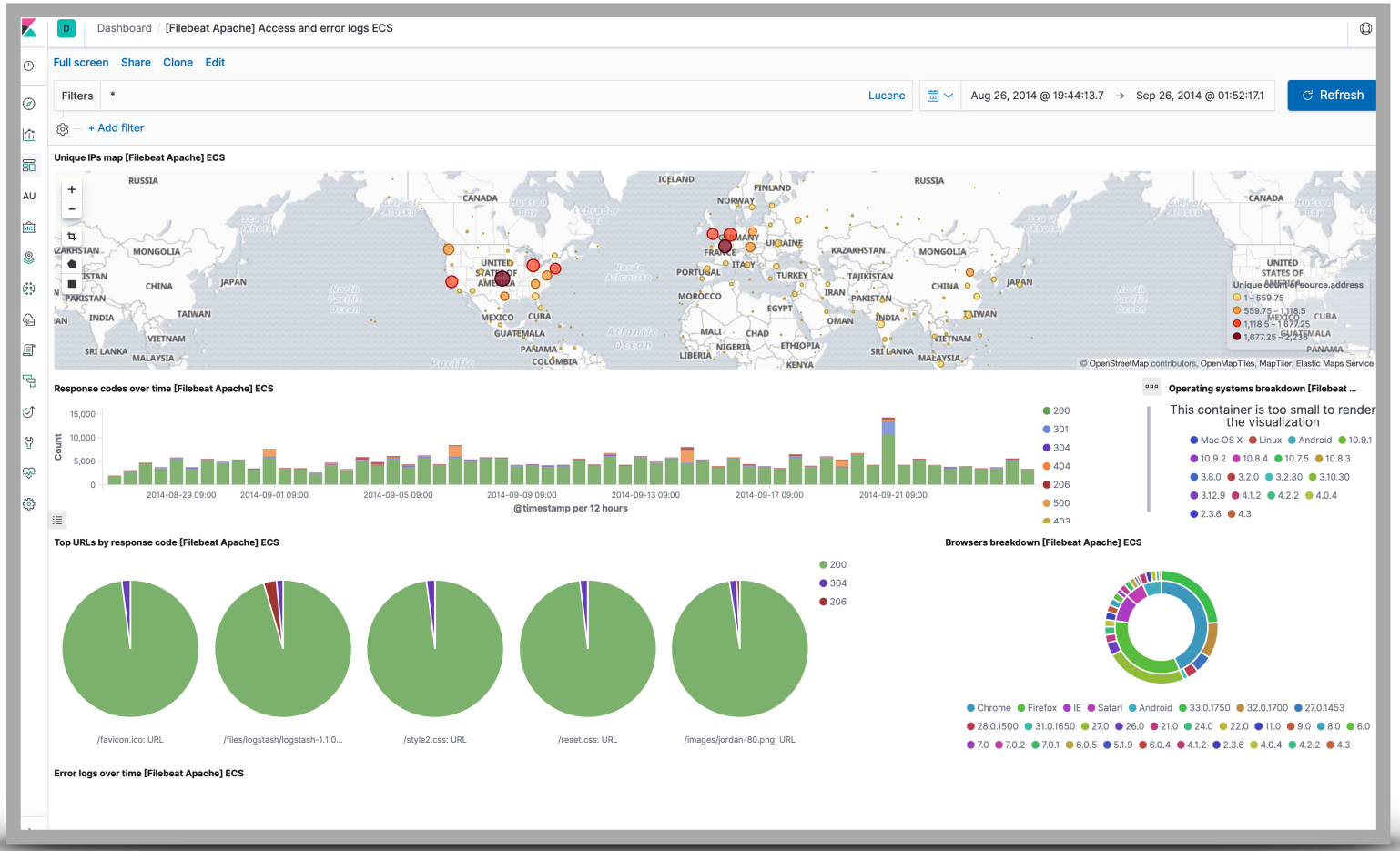


ログ

Filebeat & Auditbeat

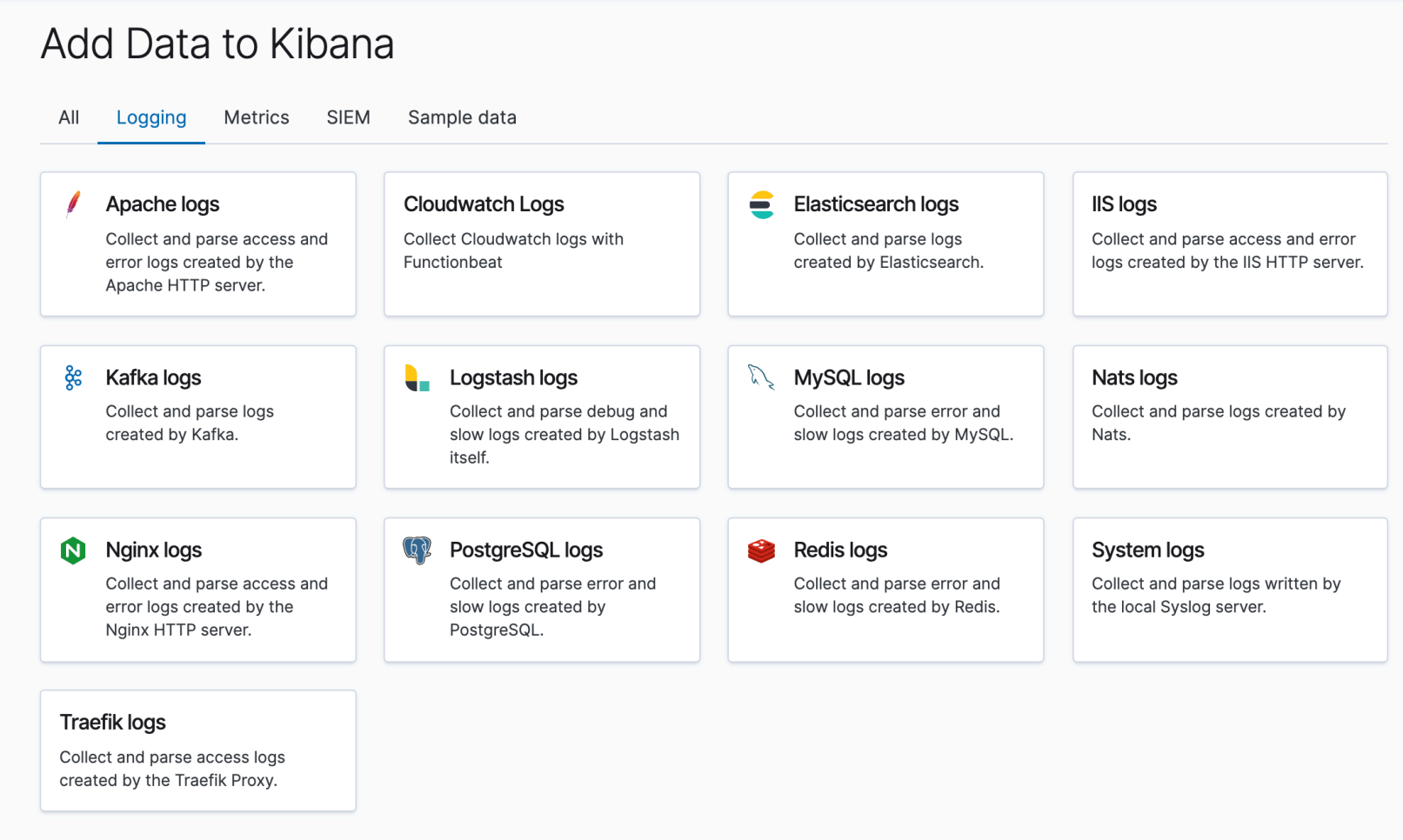
Filebeat

ファイルから
ログを収集



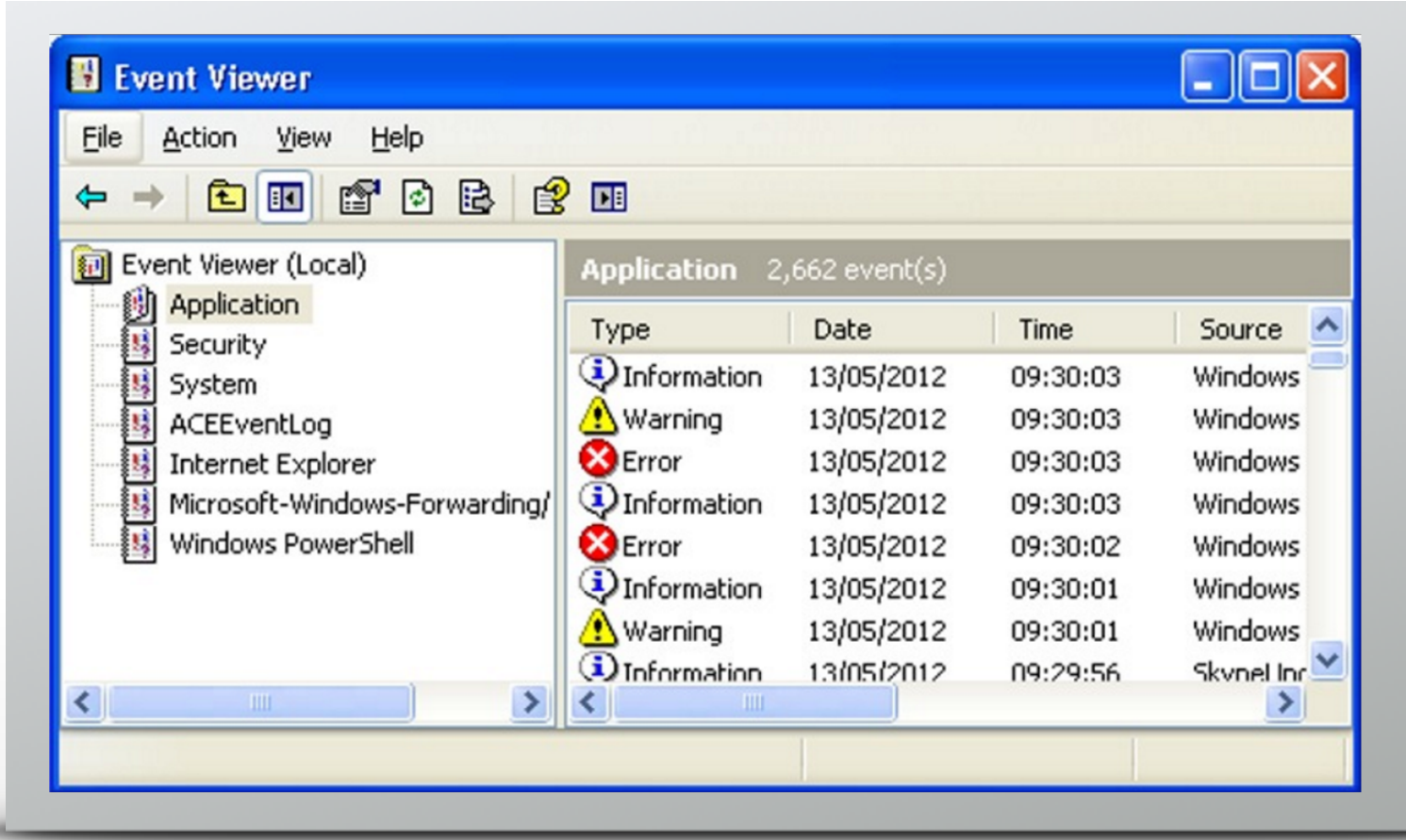
Filebeat

多くの
モジュール



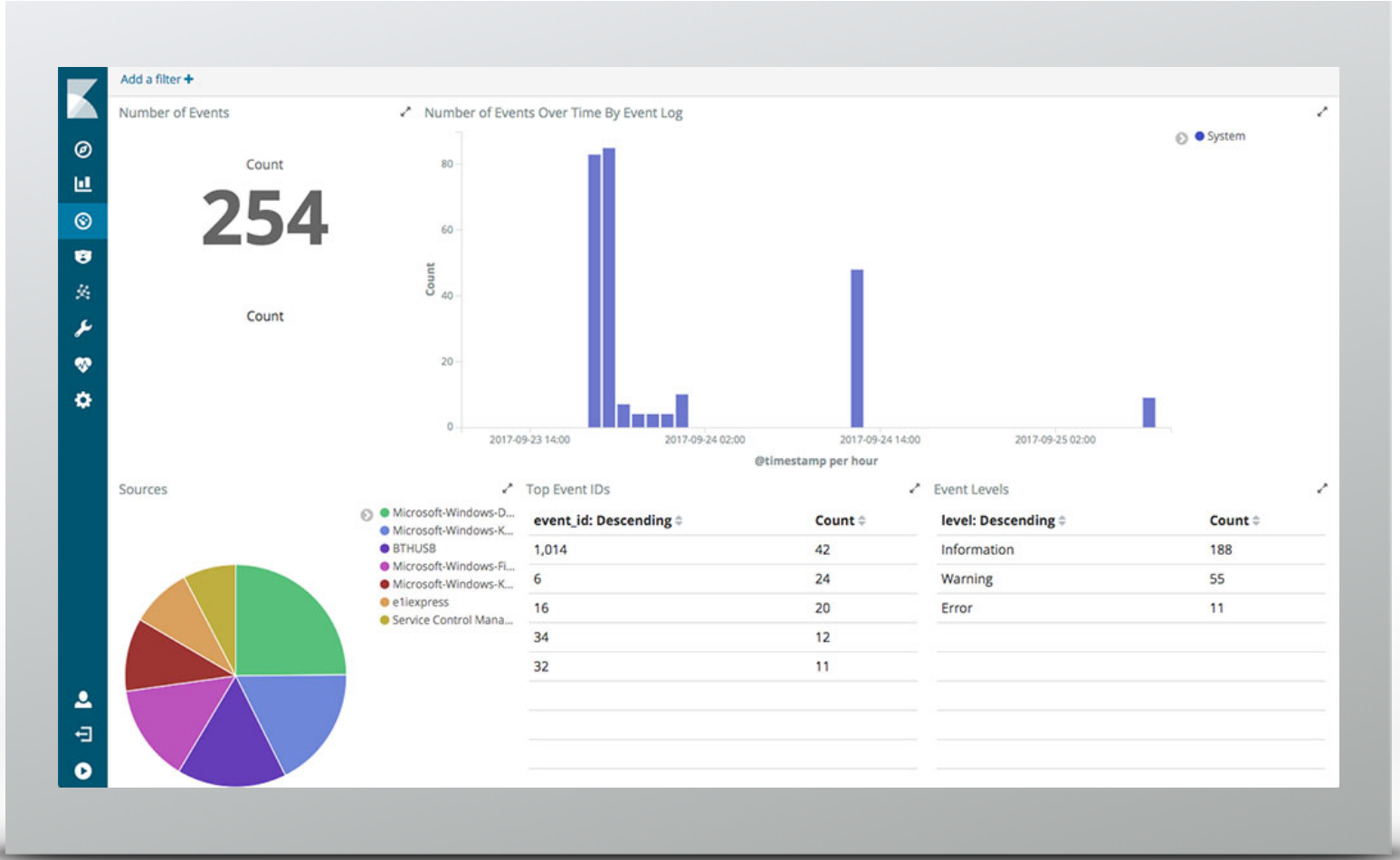
winlogbeat

Welcome to **1998**



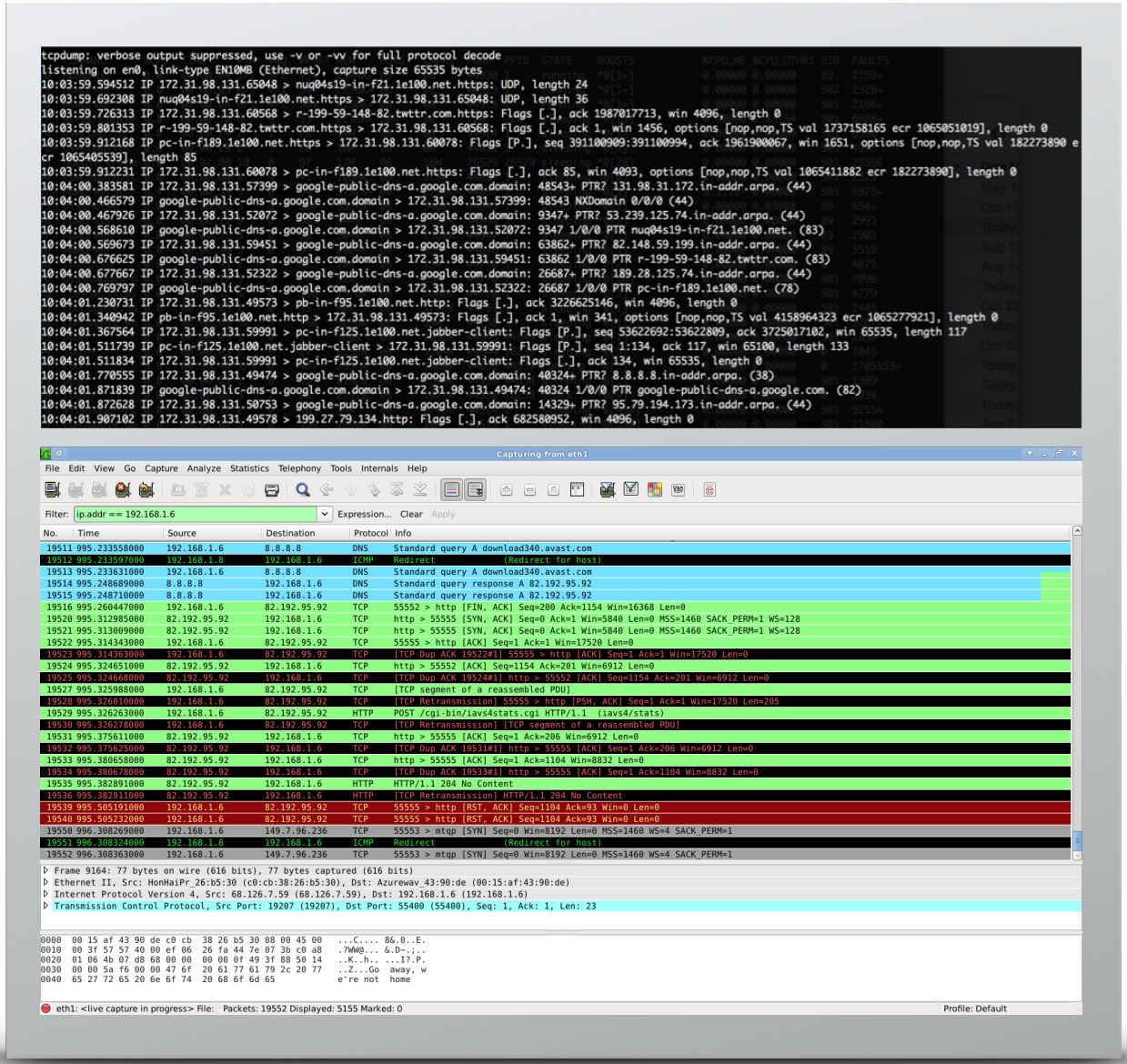
winlogbeat

Now



Packetbeat

Capture the **Packet**



Packetbeat

パケットを
キャプチャ

どういう仕組？

- Filebeatのモジュール
- Filebeatの役割
- Ingest Node / Logstashの役割

モジュールとは？ - Filebeatのモジュール

- 手軽にデータの取得から可視化までを提供する仕組み
  - 対象とするシステム、ミドルウェアごとに提供
- 事前に定義されたパターンでログをパース
  - データソースごとにログをパースして構造化するための定義を用意
- サンプルとなるグラフおよびダッシュボード
  - Kibanaのグラフ、ダッシュボードも定義済み

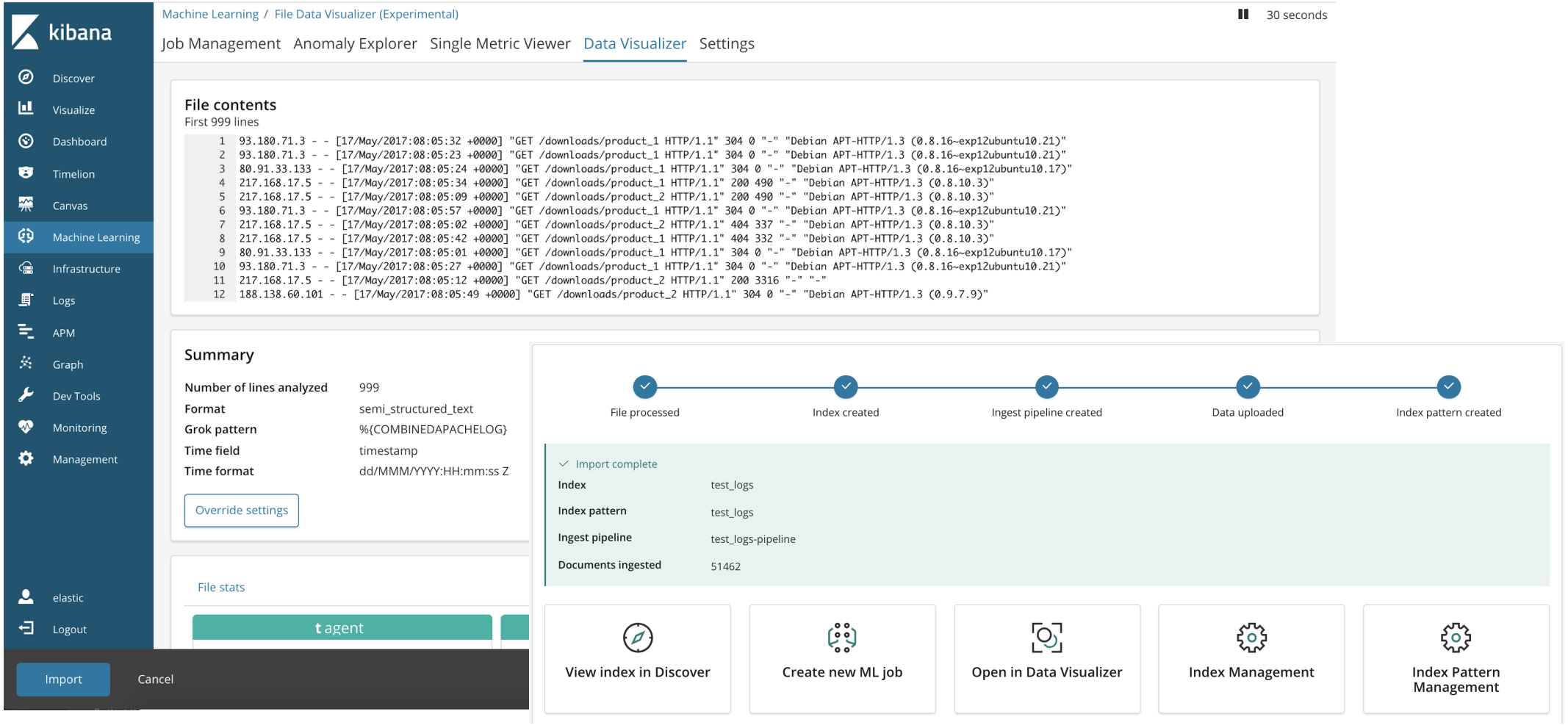
Filebeatの役割

- ファイルを監視し、ログを取り込み
- ファイルごとに読み込み済みの場所を管理
- ログに対してメタデータを付与

Ingest Node / Logstashの役割

- 読み込んだログ文字列を構造化
- 不要なデータの除去
- データのエンリッチ（データの変換、追加）

ログファイルのインポート（簡易版）
自動的な構造解析



Logs Solution

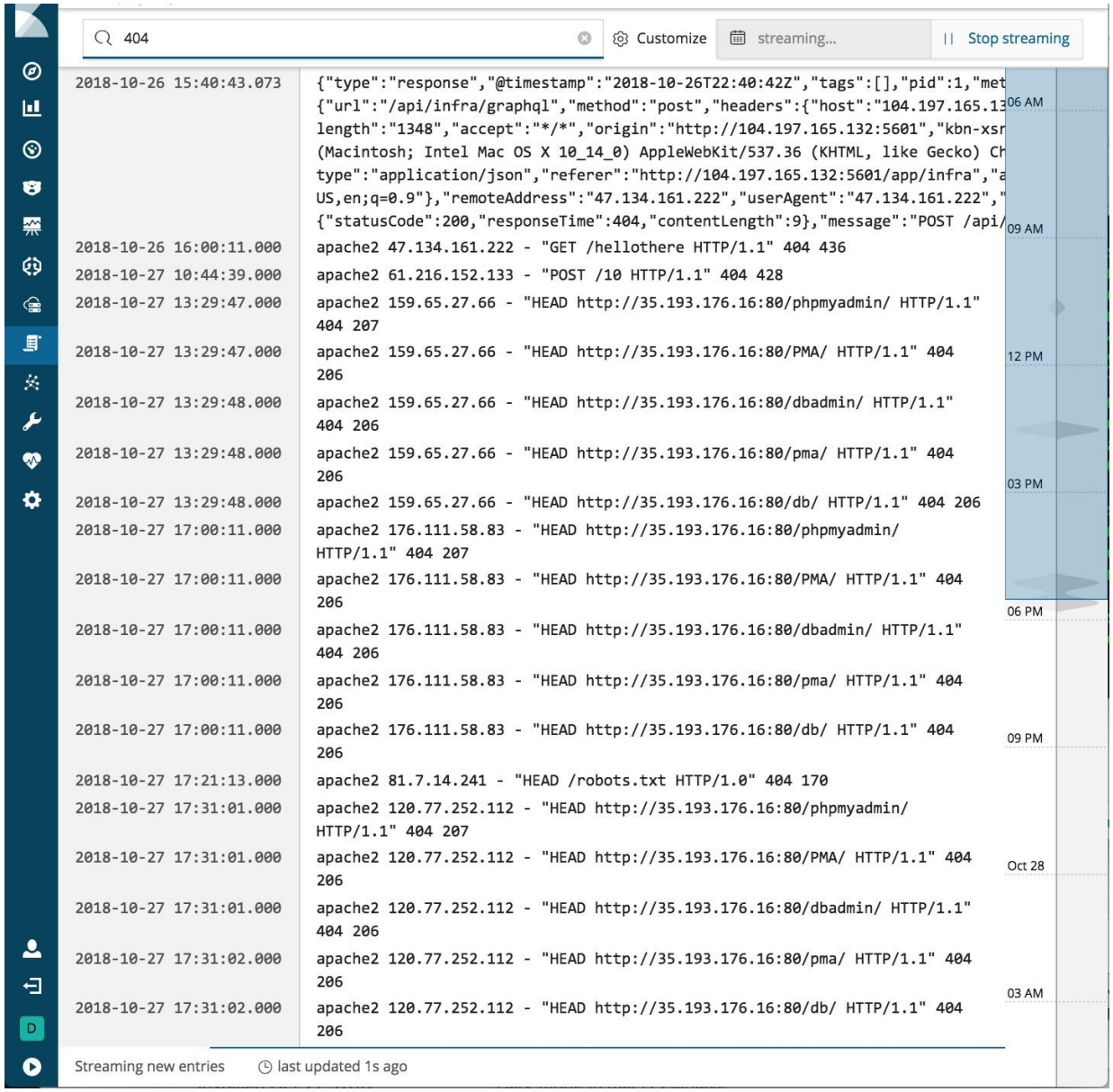
Beta | Basic (free)

ライブログイベントのトラブルシューティングのためのコンパクトなログビューワー

コンソールのような表示

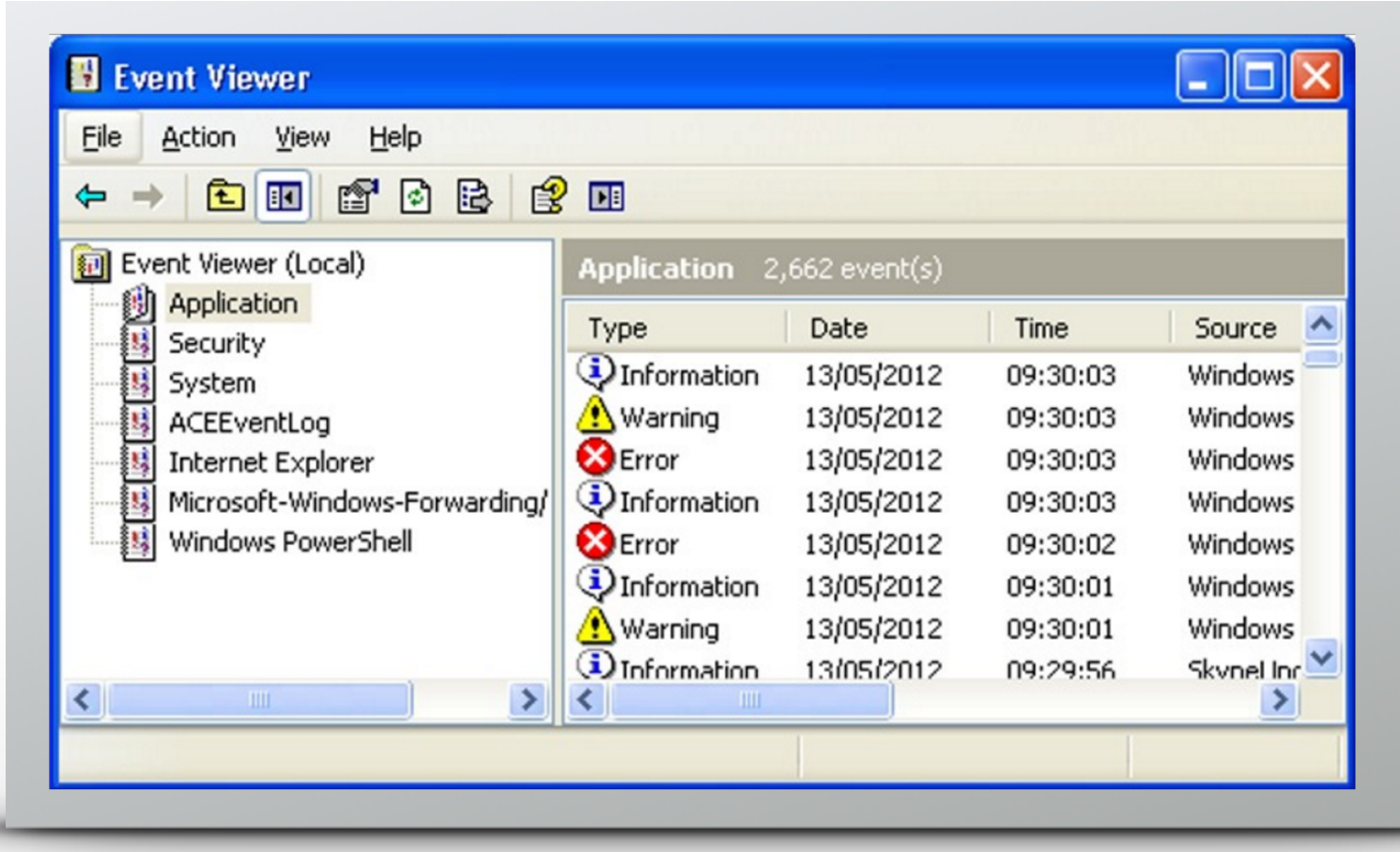
ライブログストリーミング (tail -f風)

アドホックな検索



auditbeat

Welcome to **1998**



カスタムなLog

カスタムなログ

Filebeat + Ingest Node

複数行にわたるログ

- Support Filebeat & Logstash

Filebeat

Java Stack Traces

edit

Java stack traces consist of multiple lines, with each line after the initial line beginning with whitespace, as in this example:

```
Exception in thread "main" java.lang.NullPointerException
        at com.example.myproject.Book.getTitle(Book.java:16)
        at com.example.myproject.Author.getBookTitles(Author.java:25)
        at com.example.myproject.Bootstrap.main(Bootstrap.java:14)
```

To consolidate these lines into a single event in Filebeat, use the following multiline configuration:

```
multiline.pattern: '^[[:space:]]'
multiline.negate: false
multiline.match: after
```

This configuration merges any line that begins with whitespace up to the previous line.

Logstash

Java Stack Traces

edit

Java stack traces consist of multiple lines, with each line after the initial line beginning with whitespace, as in this example:

```
Exception in thread "main" java.lang.NullPointerException
        at com.example.myproject.Book.getTitle(Book.java:16)
        at com.example.myproject.Author.getBookTitles(Author.java:25)
        at com.example.myproject.Bootstrap.main(Bootstrap.java:14)
```

To consolidate these lines into a single event in Logstash, use the following configuration for the multiline codec:

```
input {
  stdin {
    codec => multiline {
      pattern => "^\s"
      what => "previous"
    }
  }
}
```


elastic

Grok filter - Logstash or Ingest Processor

```
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"
  }
}
```

Grok filterでログをパース

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

Grok パターン

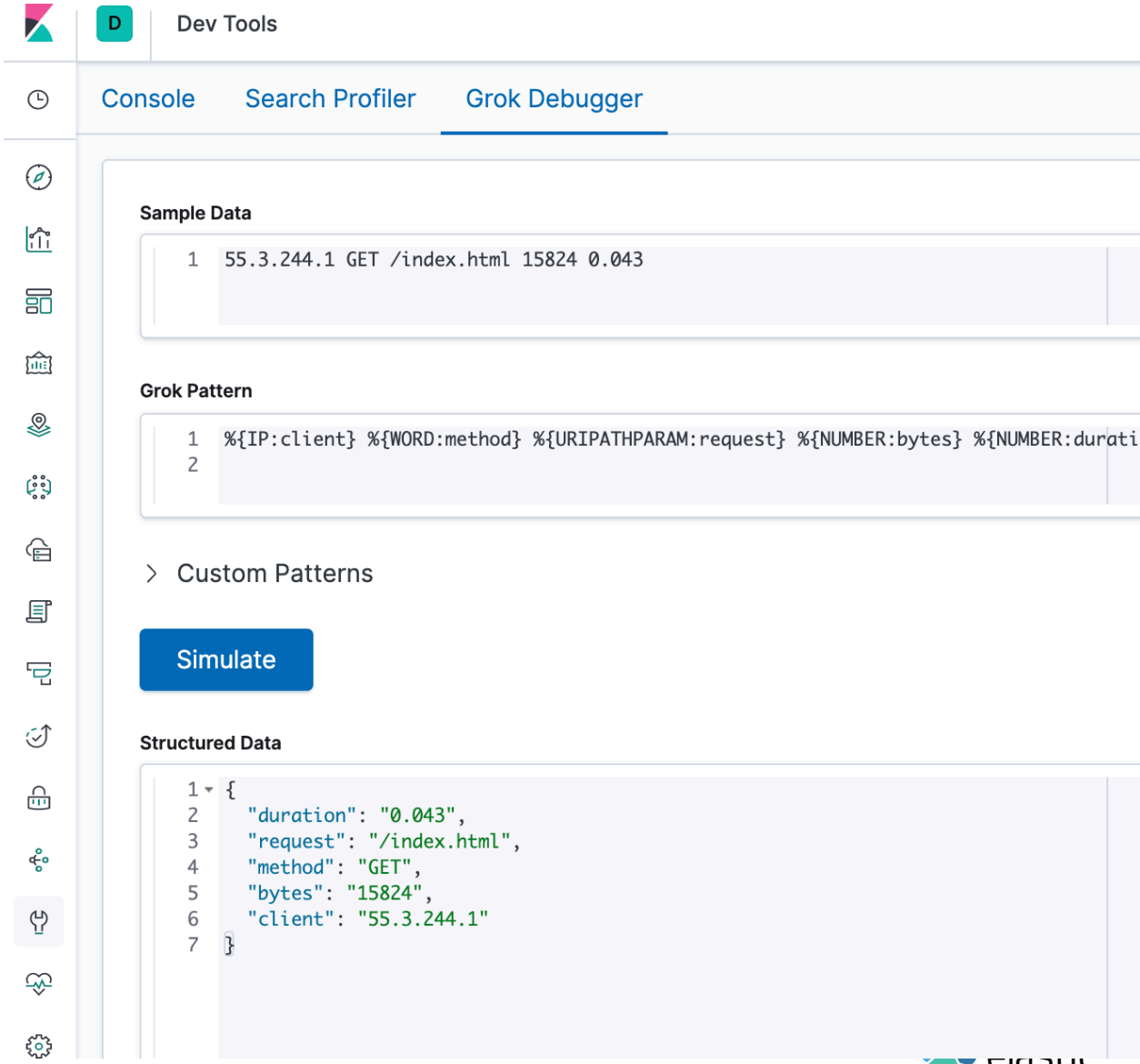
- 正規表現に名前をつけられる仕組み
- 120以上の再利用可能なパターンを用意
- サンプルパターン:

USERNAME	***[a-zA-Z0-9._-]+***
INT	***(?:[+-]?(?:[0-9]+))***
COMMONAPACHELOG	***%{IPORHOST:clientip} %{HTTPDUSER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb} %{NOTSPACE:request} (?: HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})" %{NUMBER:response} (?:%{NUMBER:bytes}|-)***

elastic

Grok デバッガ

- KibanaのDev toolsに
  Elastic Licenseの
  ベーシックとして配布
- オンライン版：
  https://grokdebug.herokuapp.com



APM

Elastic APM

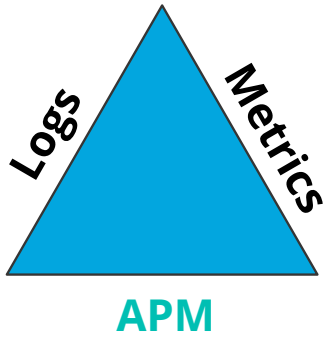
Application Performance Monitoring (APM)

APM データ: アプリケーションの分析

Name	Avg. resp. time	95th percentile	Req. per minute	Impact
GET cyclops.views.product_detail.ESProductDetail…	983 ms	1,331 ms	3.7 rpm	
GET cyclops.views.search.ElasticSearchView	775 ms	1,117 ms	1.3 rpm	
POST cyclops.shuup.front.views.basket.BasketView	1,696 ms	2,636 ms	0.6 rpm	

インストールは簡単で、アプリケーション内部の状況を把握

- アプリケーションで何が起きているかを自動的に把握
  （ライブラリもしくはエージェントをアプリに追加する必要あり）
- トランザクションやトレースを独自に定義カスタマイズ可能



elastic

APM

Unify Logs + Metrics + APM

オープンソース

対応プログラミング言語

Java, Go, RUM, Node, Python,
Ruby, .NETなどなど

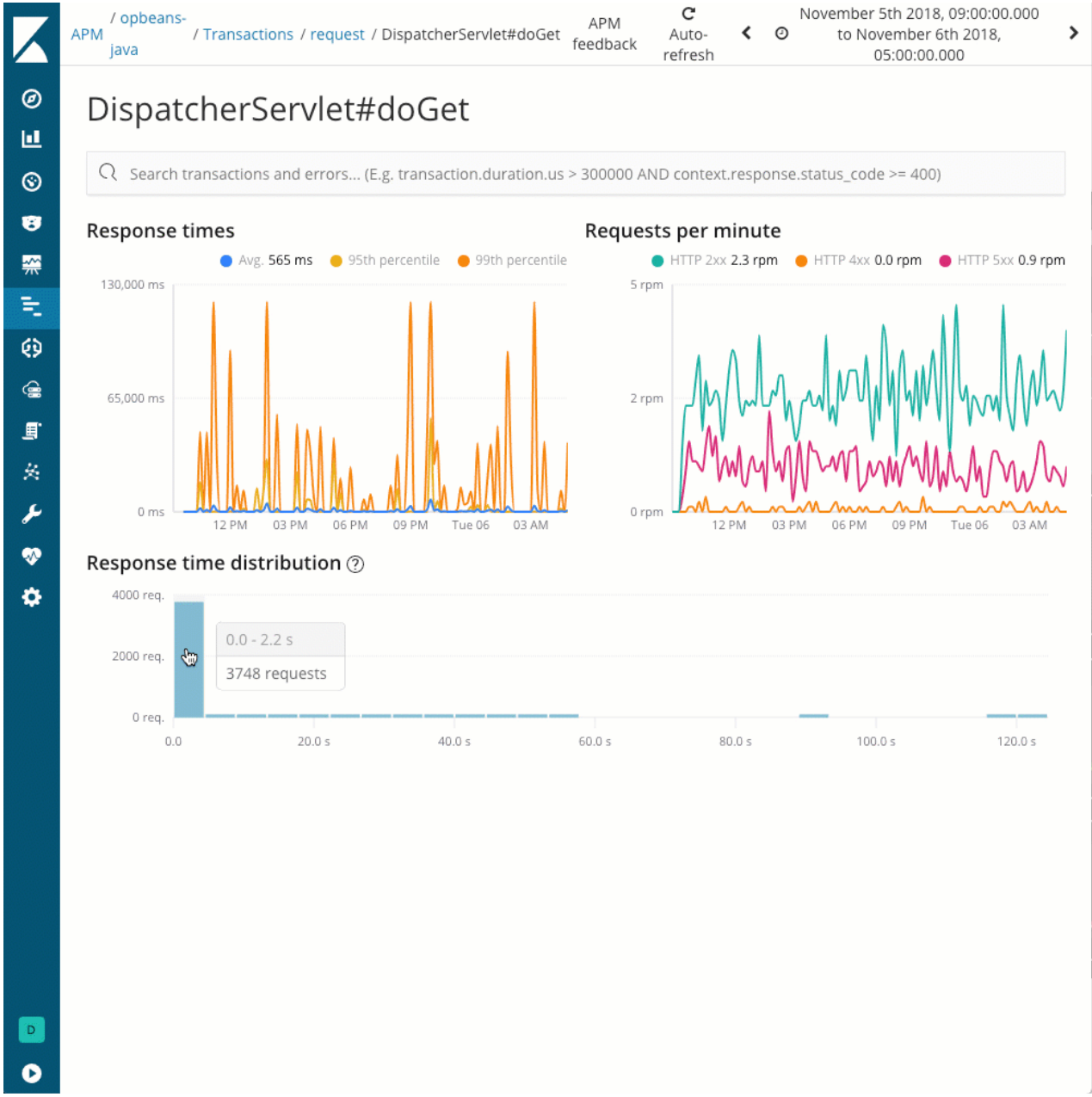
専用 UI

Streamline APM workflows
分散トレーシング

APM以外との連携

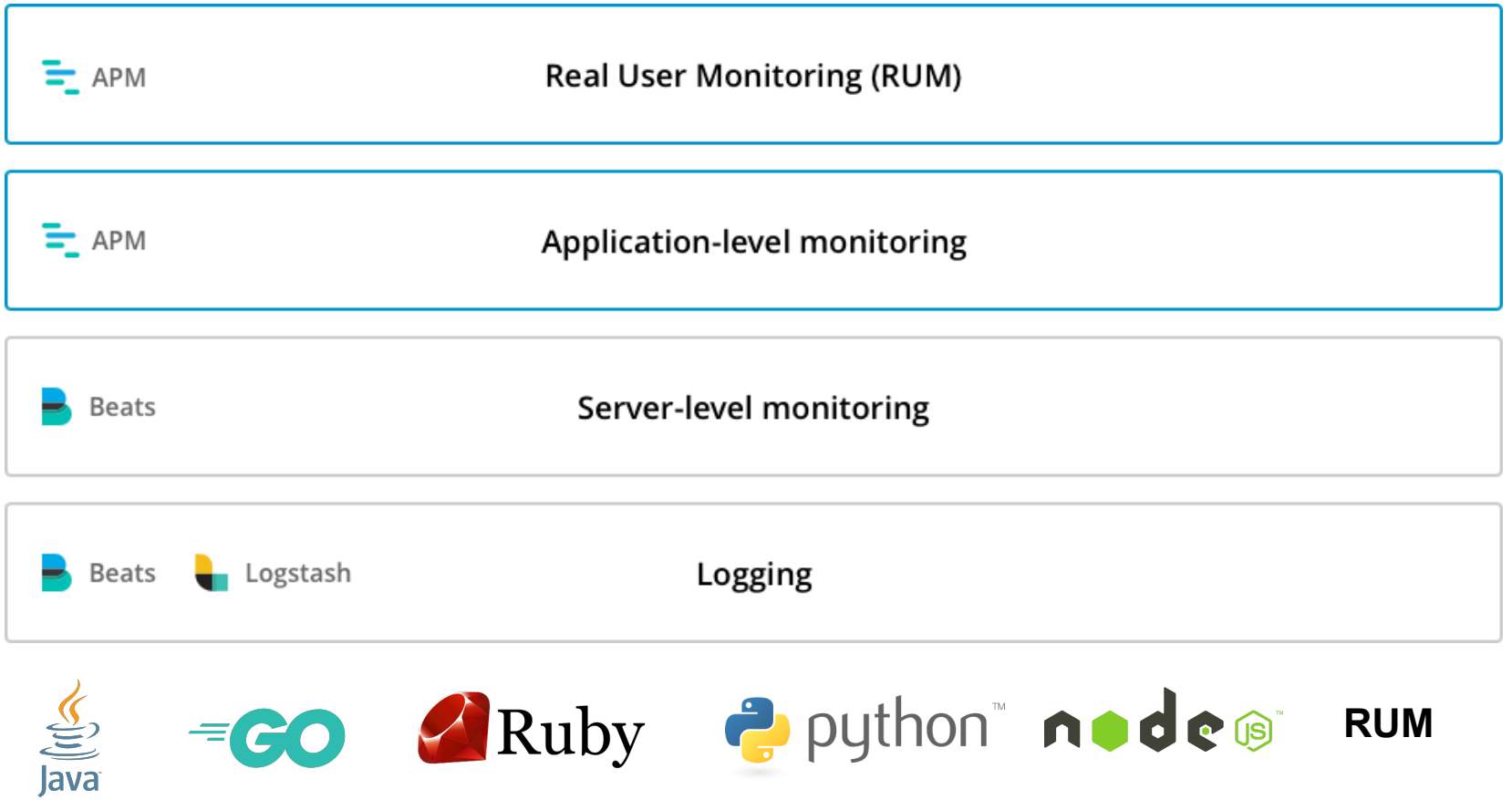
他のデータとの関連

Elastic Stackをフル活用



Kibanaひとつでオブザバビリティをカバー

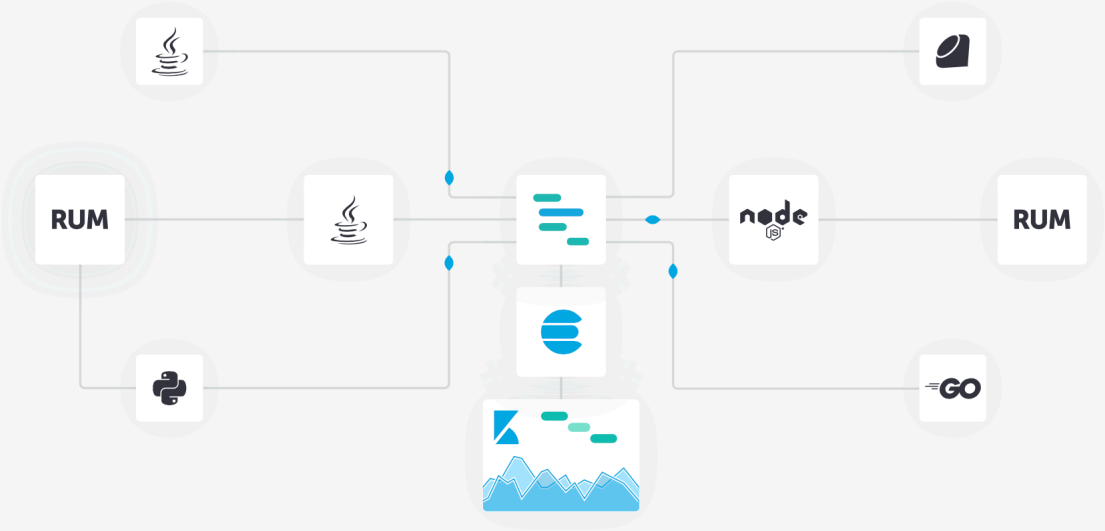
エンドユーザーやアプリケーションのモニタリングをAPMにより追加



elastic

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。

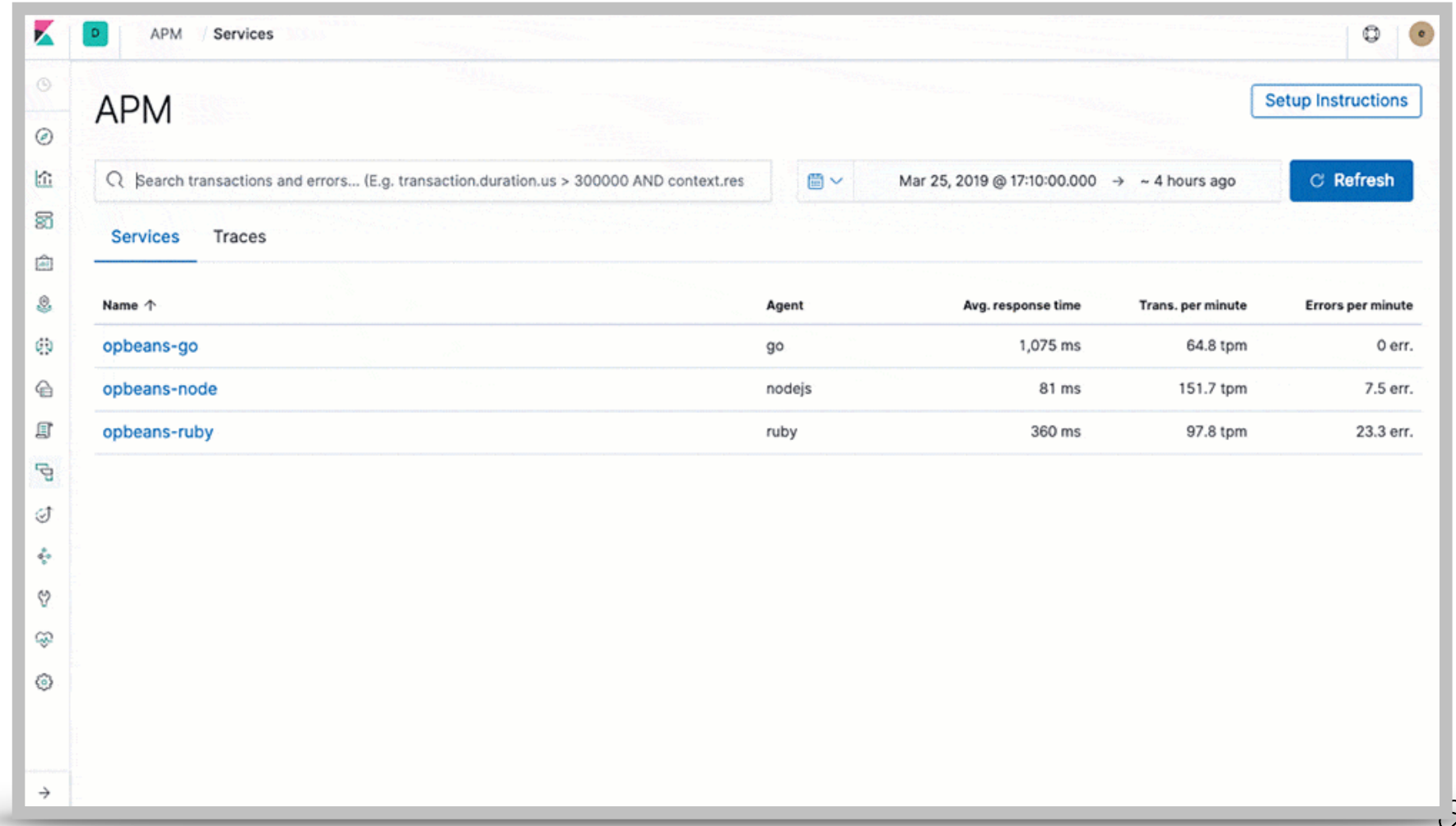


ElasticのAPMで、パフォーマンスメトリックの可視化が簡単に。 | 今すぐトライ

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

Elastic APM



elastic

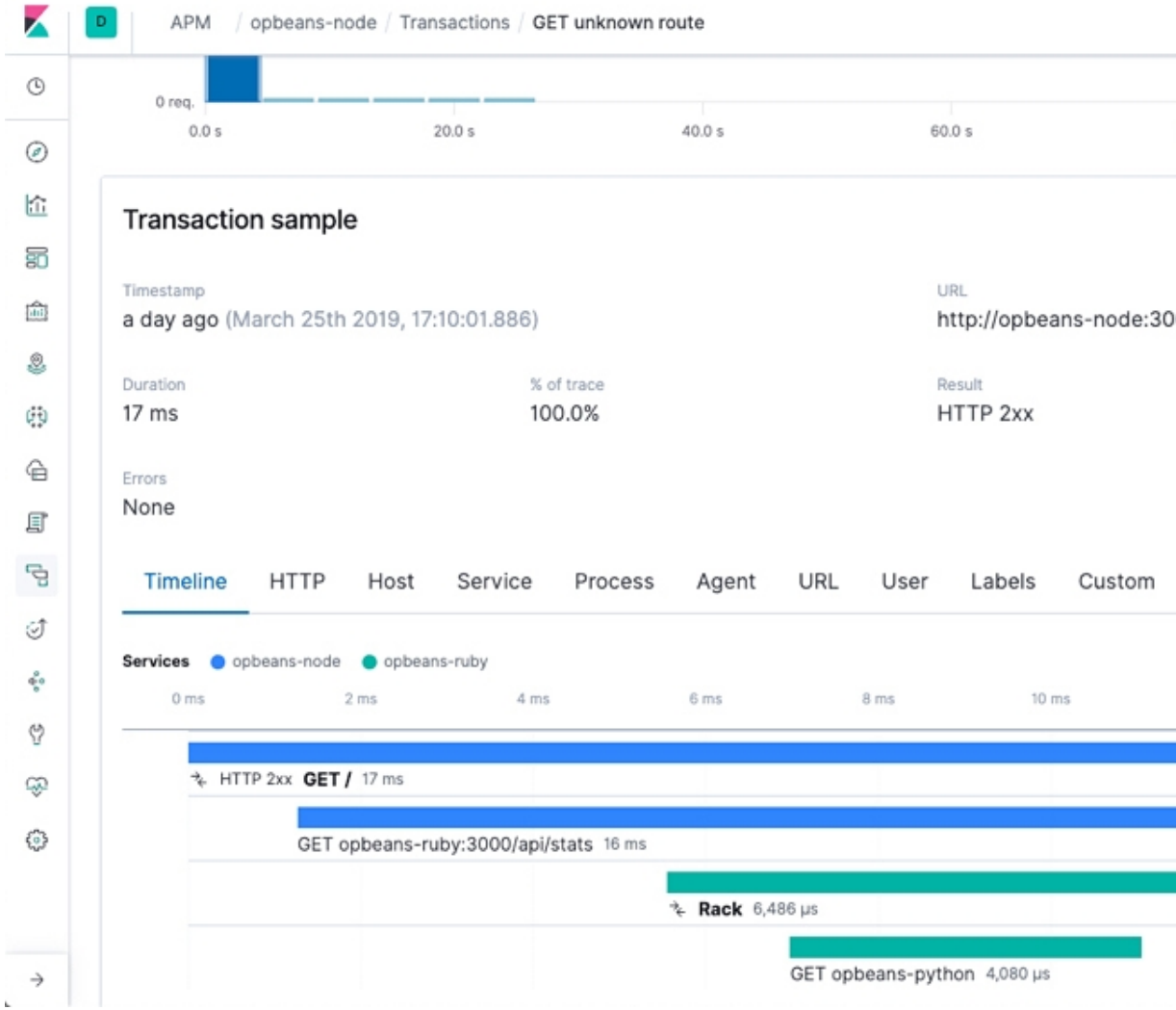
分散トレーシング

GA | Basic (free)

全ての計測されたサービスを見るための
統合されたビュー

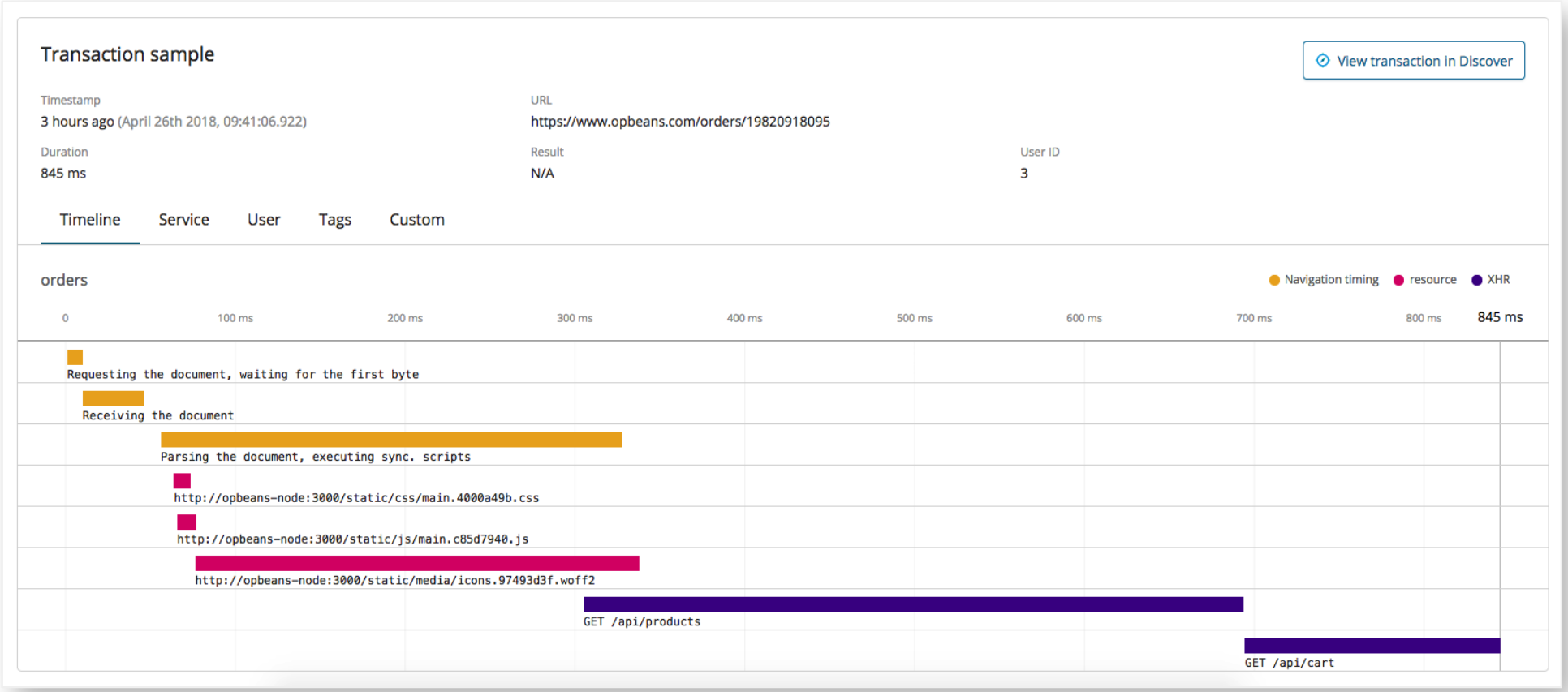
サブコンテキスト内のトレースに遷移

OpenTracing 互換



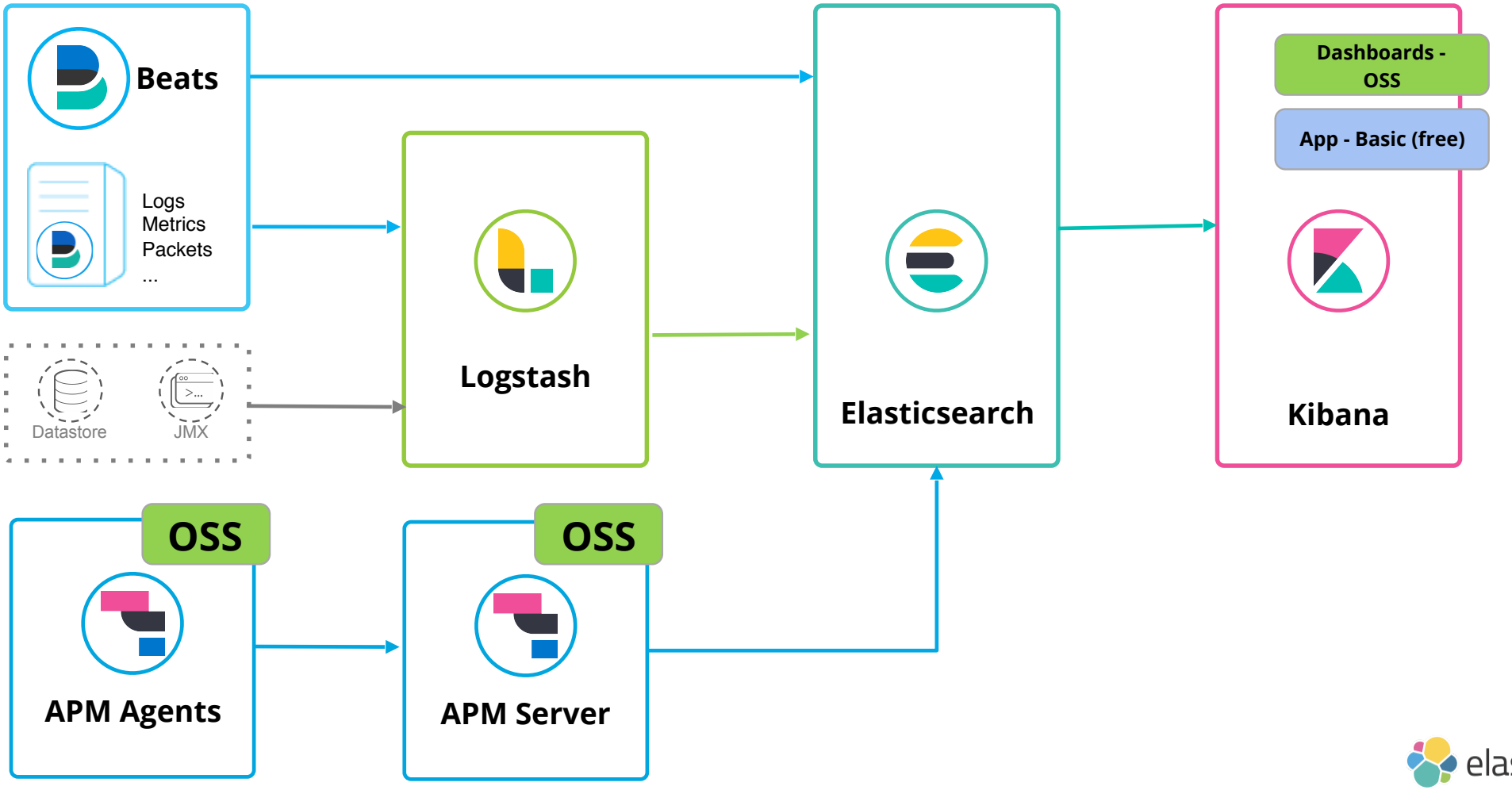
RUM (リアルユーザー監視)

ブラウザでの処理時間を計測



elastic

構成例


Beats
Logs
Metrics
Packets
...
Datastore
JMX
Logstash
Elasticsearch
Dashboards - OSS
App - Basic (free)
Kibana
OSS
APM Agents
OSS
APM Server

elastic

オブザバビリティ

より効率よく3要素を活用するには

Elastic Common Schema - Lets Correlate

https://github.com/elastic/ecs

- Defines a **common** set of fields for ingesting data into Elasticsearch.
- Helps you **correlate** data from different source types
  Logs, Metrics and APM
- Designed to be **extensible** and **reusable**
- Details and **community** feedback @ https://github.com/elastic/ecs

Destination fields

Destination fields describe details about the destination of a packet/event.

Field	Description	Type
`destination.ip`	IP address of the destination. Can be one or multiple IPv4 or IPv6 addresses.	ip
`destination.hostname`	Hostname of the destination.	keyword
`destination.port`	Port of the destination.	long
`destination.mac`	MAC address of the destination.	keyword
`destination.domain`	Destination domain.	keyword
`destination.subdomain`	Destination subdomain.	keyword

elastic

Applications Web apps, servers, APIs log4j, JMX Twitter, Salesforce, Github	**Platform Infrastructure** Windows, Linux/Unix, MacOS Load balancers, proxies, caches S3, HDFS
Containers & Cloud Docker, Kubernetes AWS, Azure, GCP Openshift	**Data Stores & Streams** DBs, Data Warehouses NoSQL Kafka, Spark, Storm, Hive
Networking Netflow, PCAP HTTP, TCP, UDP, DNS, TLS syslog, auditd	**Security Devices** NSM, IDS/IPS, firewalls Web proxies, endpoints ArcSight
Messaging & Alerting Slack, HipChat Pagerduty, Email Nagios, Zabbix	**Raw Documents** PDF, XLS, PPT Technical, legal, healthcare documents
IoT Sensors, robots Connected cars Smart homes	**Build Your Own**

Logs

Metrics

Configs

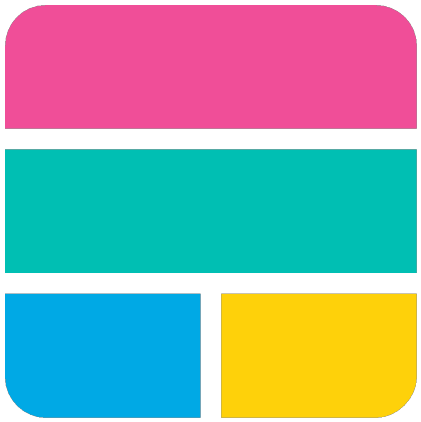
Messages

Scripts

Tickets

Alerts

Ingest Integrations



The Elastic Stack

データの管理

日々増加するデータの管理方法

オペレーション監視

Logs + Metrics + APMの統一

データ登録

コネクターのリッチなエコシステム

拡張可能なパイプライン

開発者に優しいAPI

探索

すぐに利用できるUI

用意されたダッシュボード

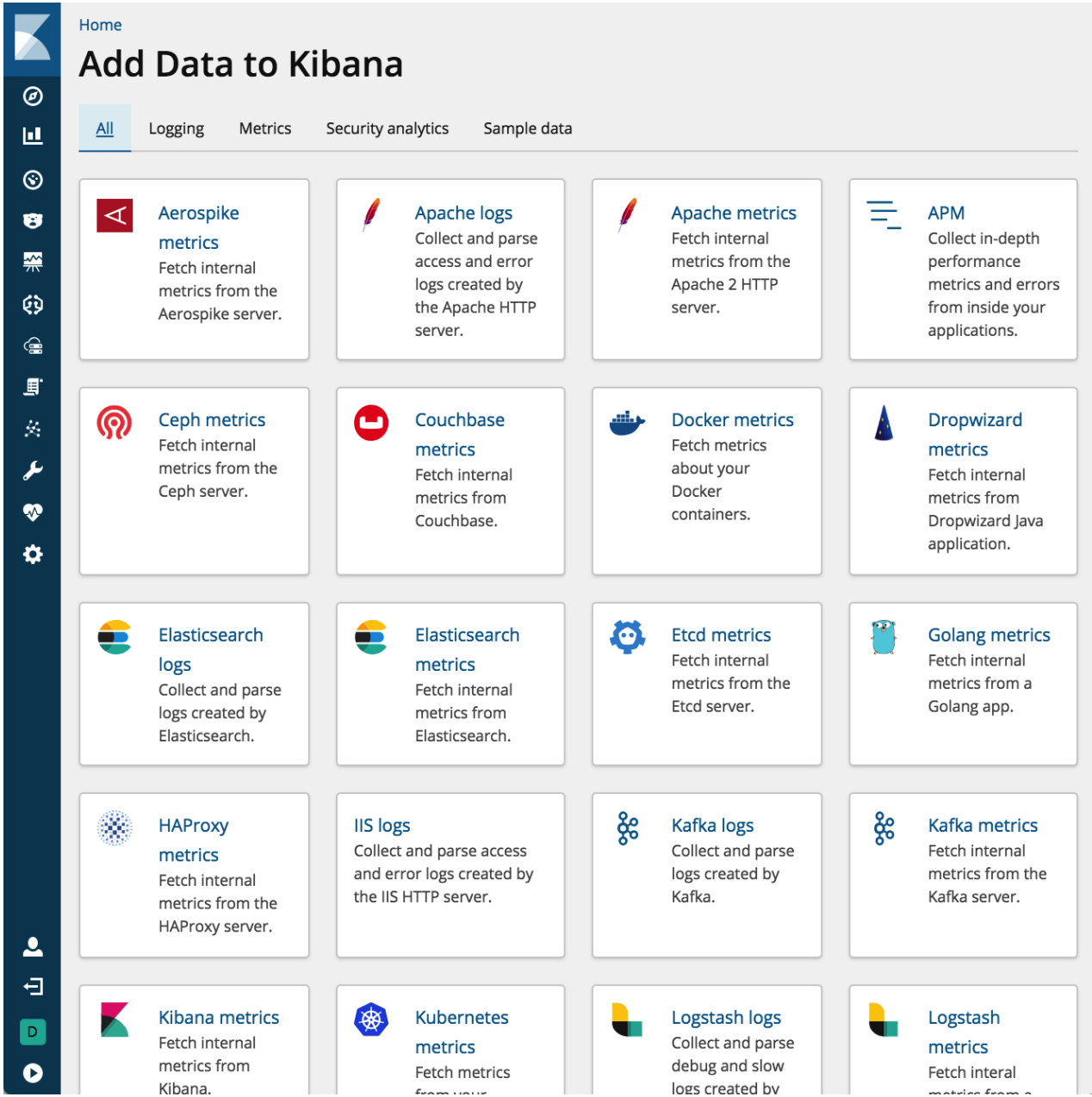
ライブ表示

分析

異常検知

トレンドとフォーキャスト

フレキシブルなアラート

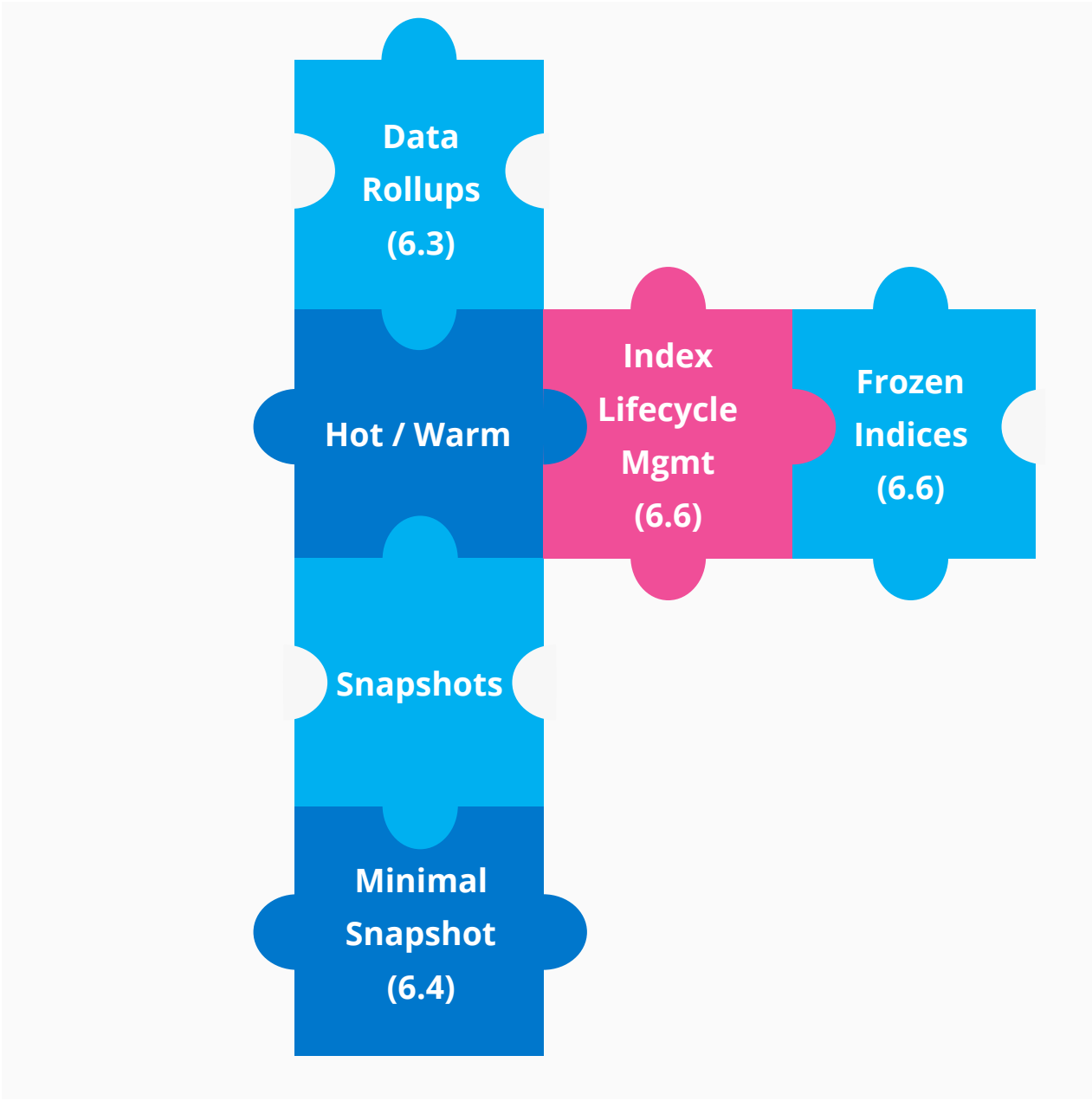


インデックス
ライフサイクル管理

New in 6.7: index freeze action

Basic (free) feature

Part of larger story around data management



Data Rollups

You know, for saving space

Rollup Data into Coarser Buckets

Save on disk space

Automate via a rollup job

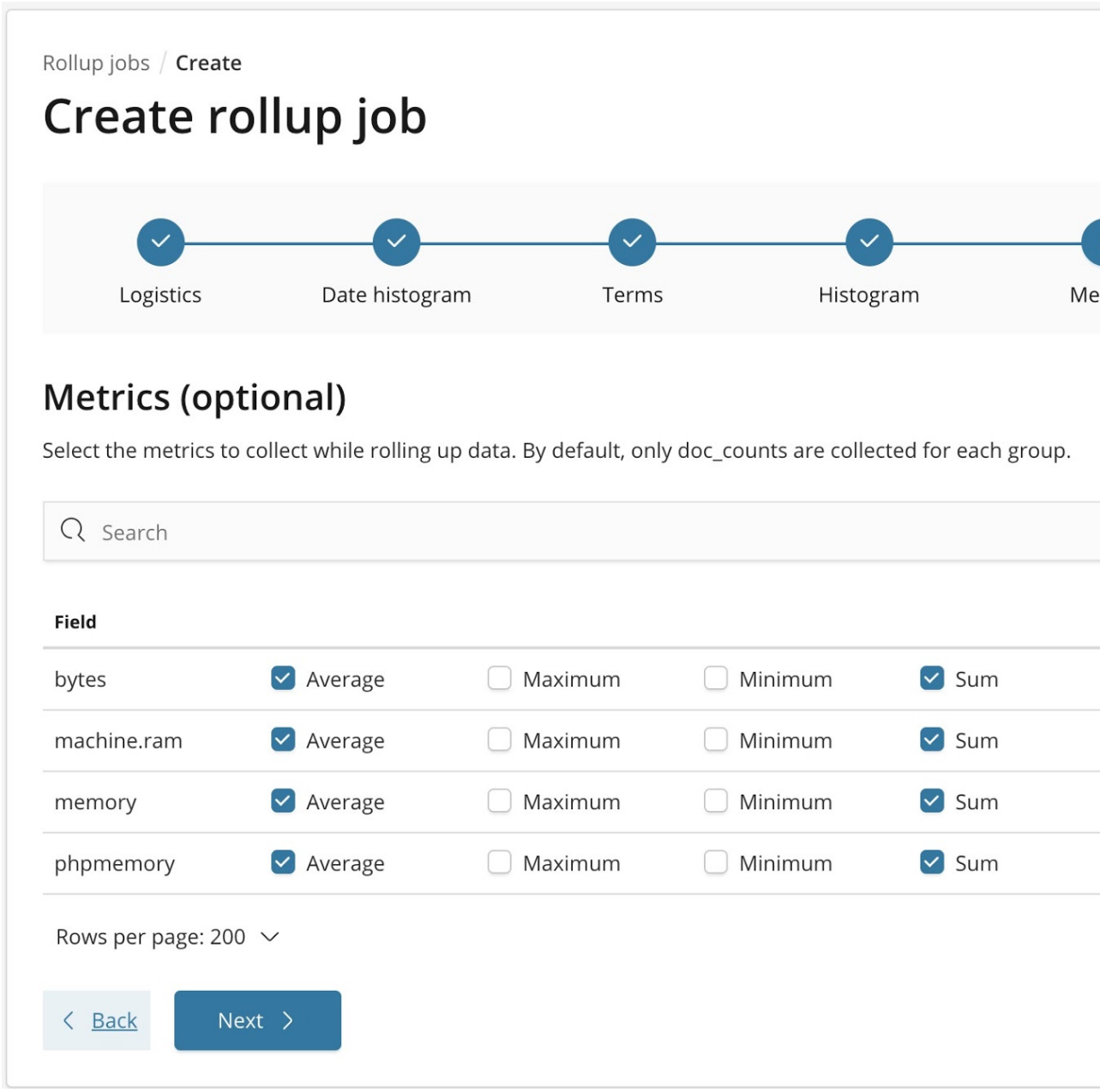
Query just like regular data

Great for metrics use cases

Kibana Support

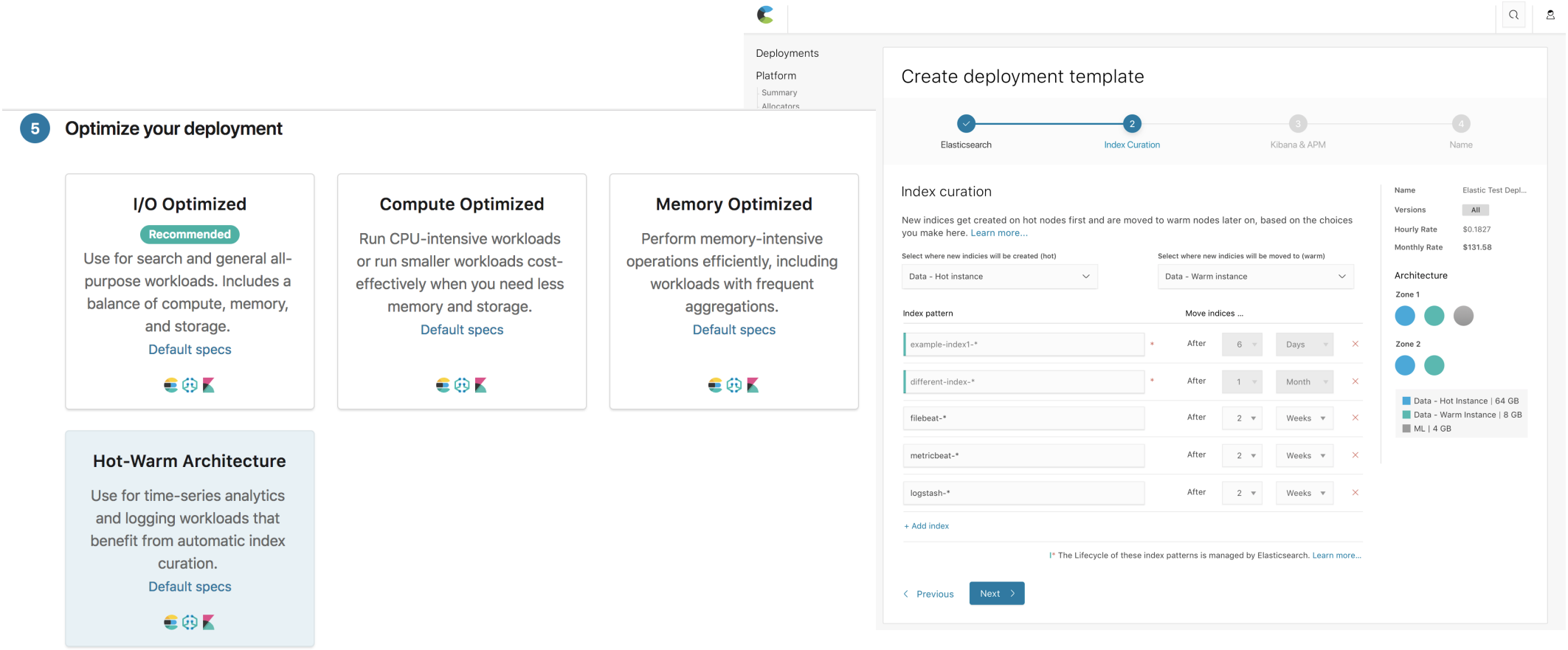
Rollups Management UI

Visualize rolled up data



Hot/Warm Architecture in EC / ECE

Optimize the use of compute resources and save $$$



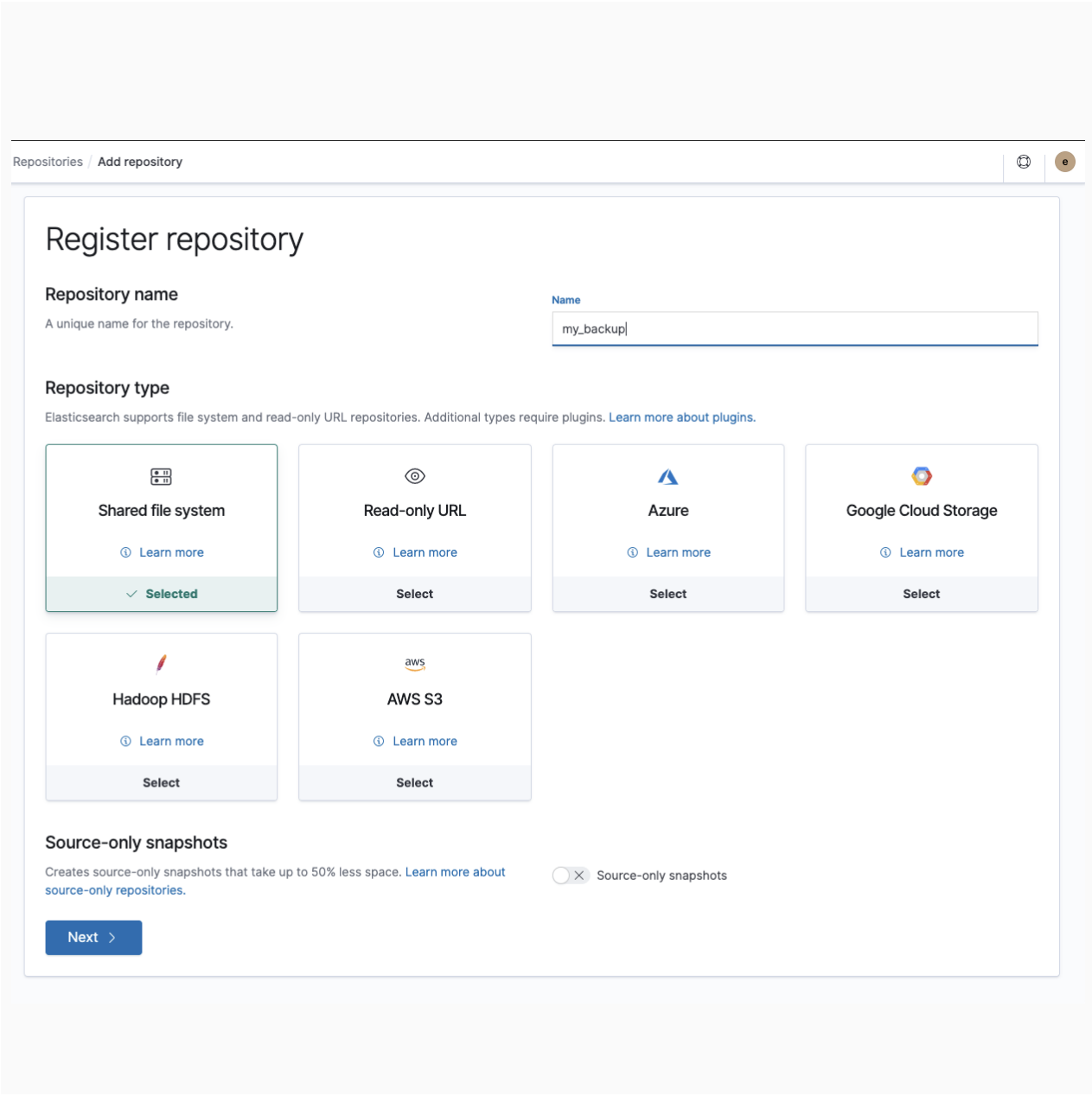
Snapshot UIs

Basic (free)

New UI features for snapshot features:

- Register snapshots repo (with support for various plugins)
- Browse repositories and snapshots

More UI improvements coming soon



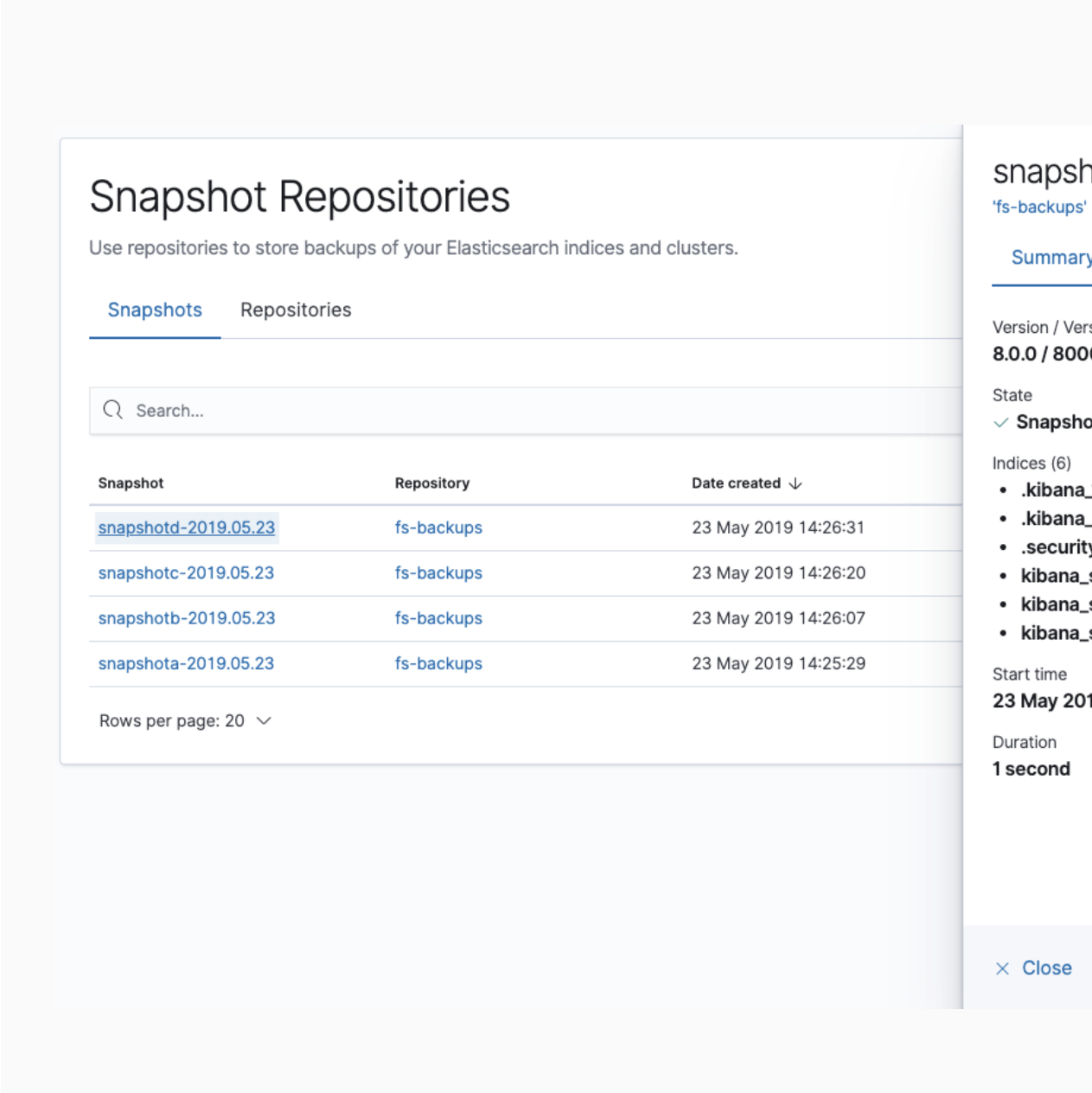
Snapshot UIs

Basic (free)

New UI features for snapshot features:

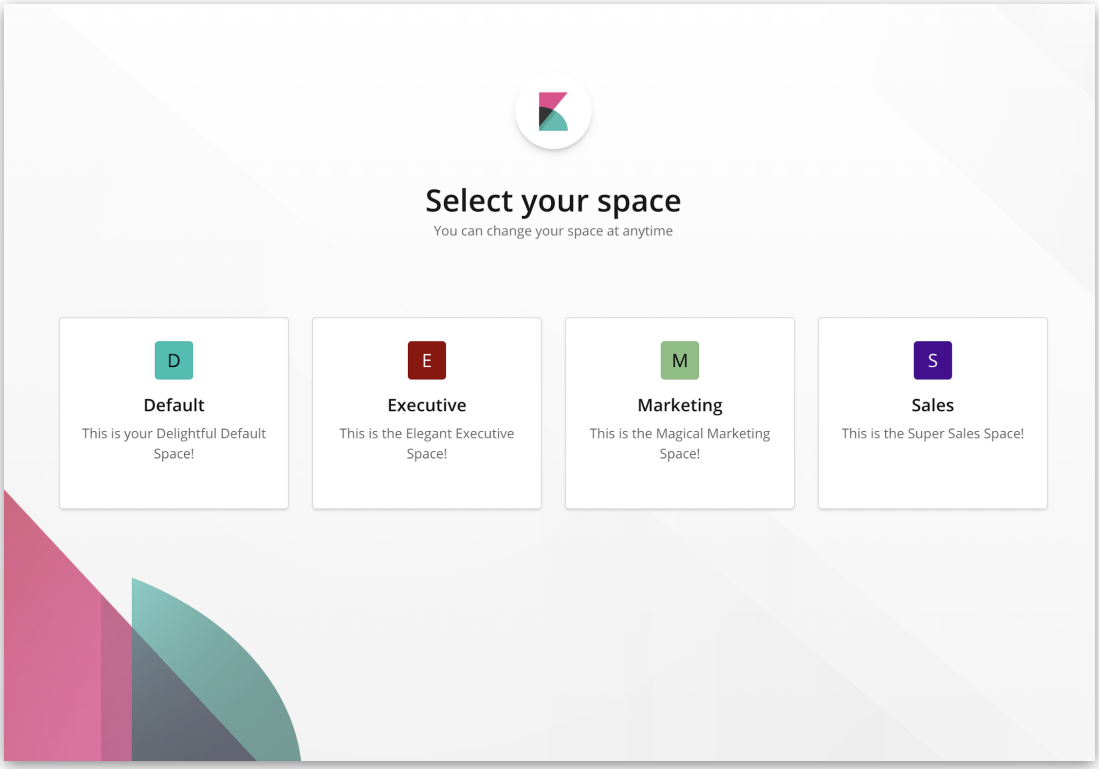
- Register snapshots repo (with support for various plugins)
- Browse repositories and snapshots

More UI improvements coming soon



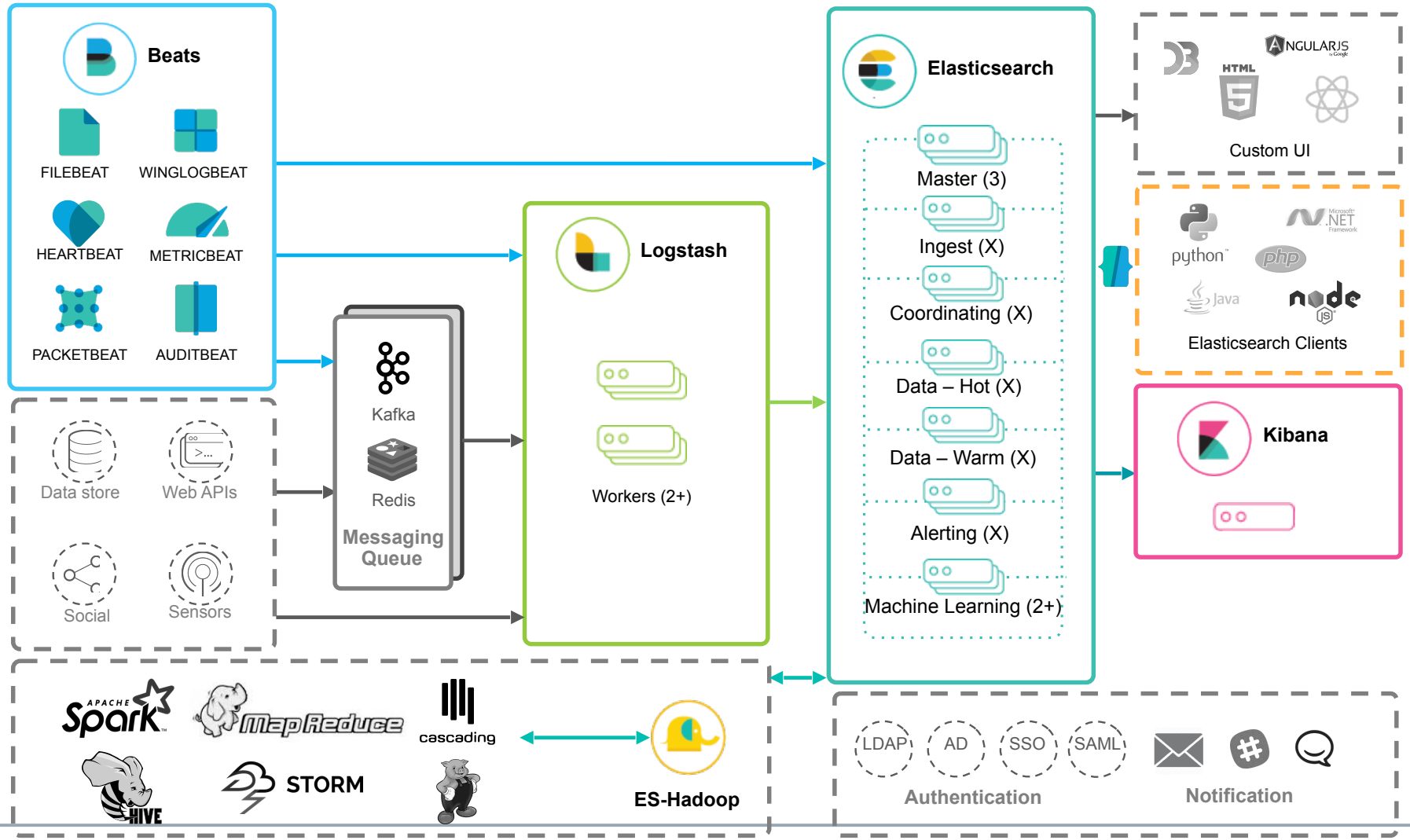
Kibana Spaces - Let's Organize

- One Kibana instance can hold many spaces
- Each space can have different sets of index patterns, visualizations, saved searches and dashboards.
- You can move objects between spaces
- Space specific settings allow to customize the space to the team using it



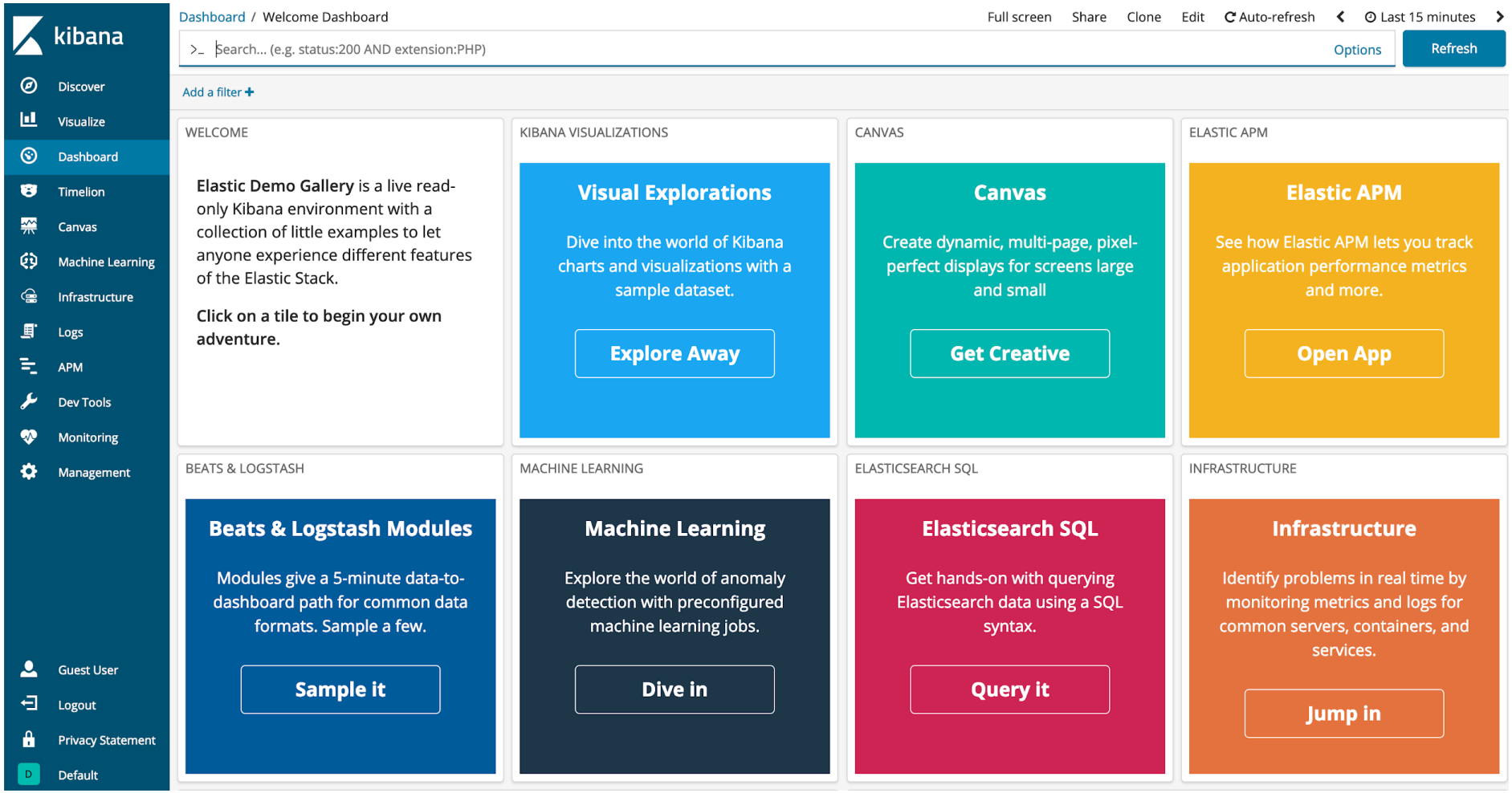
elastic

Typical Logging **Deployment in the Enterprise**



elastic

View Live Beats Dashboards on https://demo.elastic.co



What’s others?

セキュリティ、アラート、機械学習など

Spaces

Basic (free) / Gold

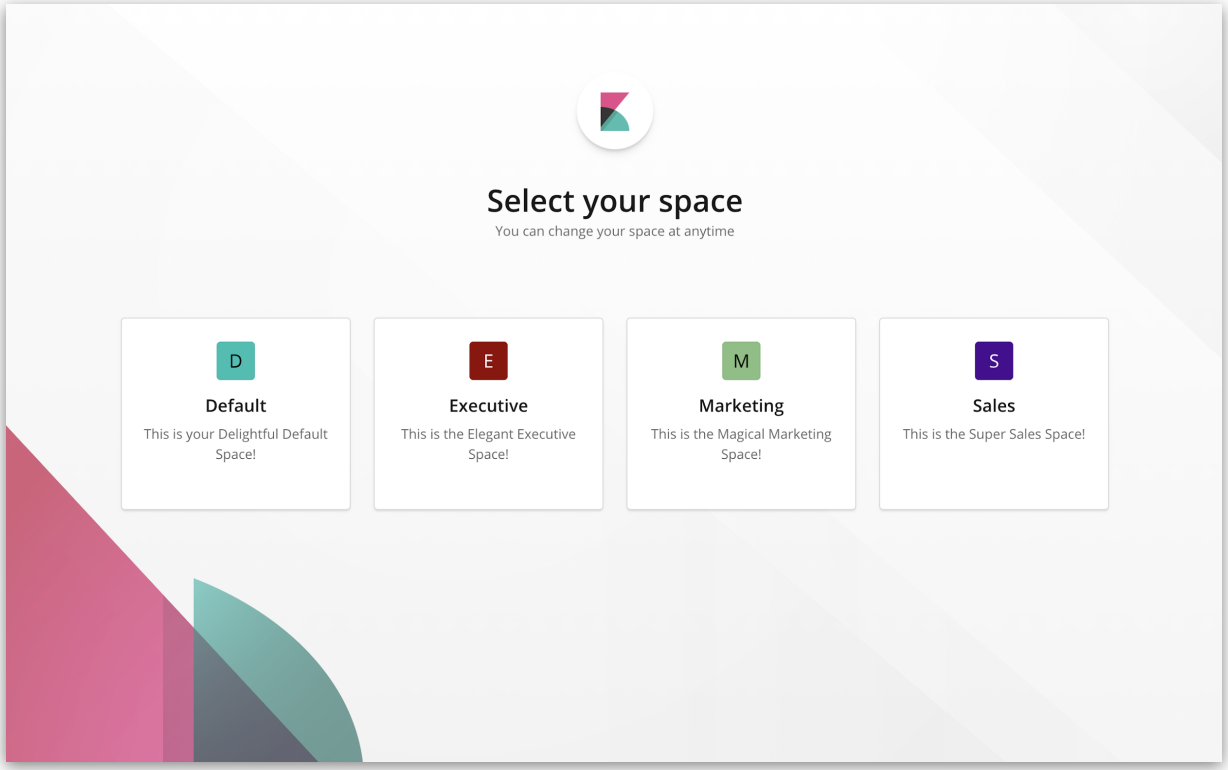
個別の**スペース**でグラフやダッシュボードを管理

RBACと一緒に使うことでスペースごとのアクセス制御も可能

Kibanaをマルチテナントで利用

ユースケース:

- 組織ごと
- フェーズ（dev, stage, prod, etc）
- セキュリティ(アクセス制限)



Feature Controls

Basic (free)

Kibana UIで、個別の機能に制限（非表示、アクセス制限）をかけることが可能

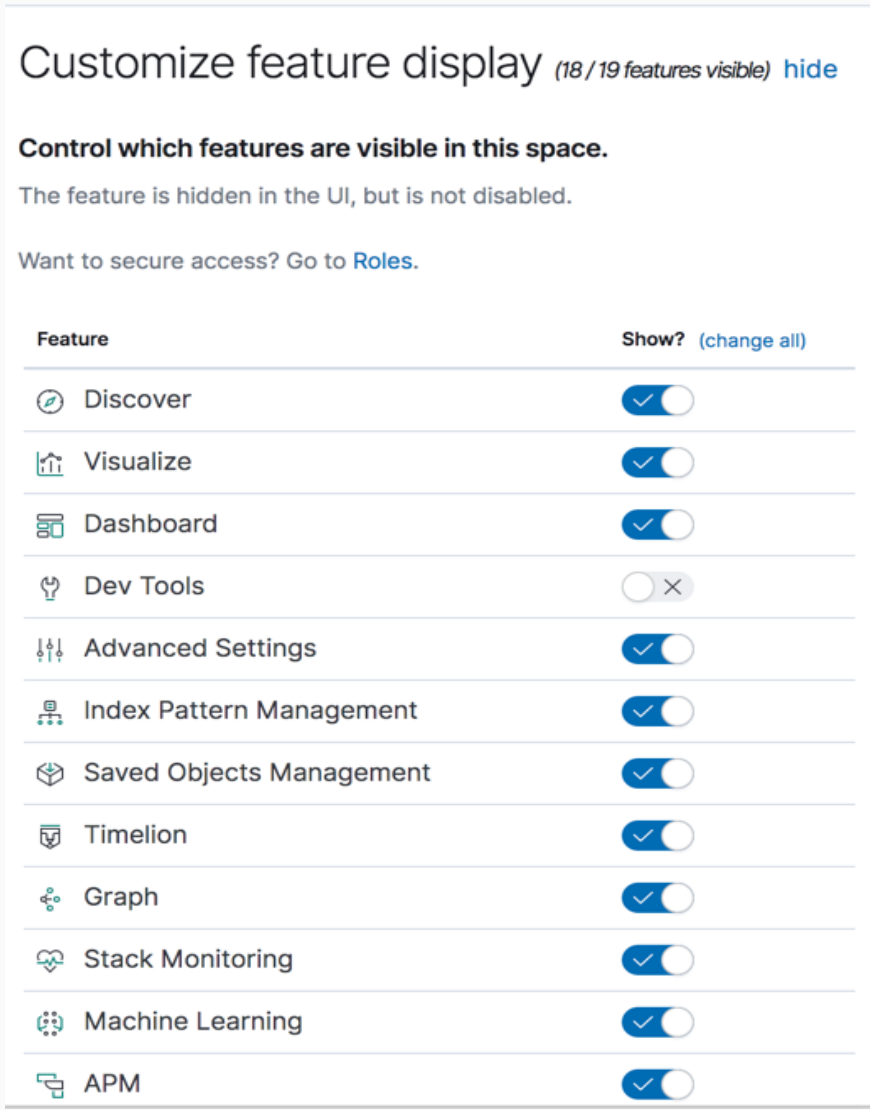
ロールごとのアクセス制限

特定のスペースのロールに対して機能を割り当て

スペースの設定で制御可能

権限レベル:

- アクセス不可
- 読み込みのみ
- すべて



Maps

Beta | Basic (free)

1つの地図に複数のデータソースおよびレイヤーを表示

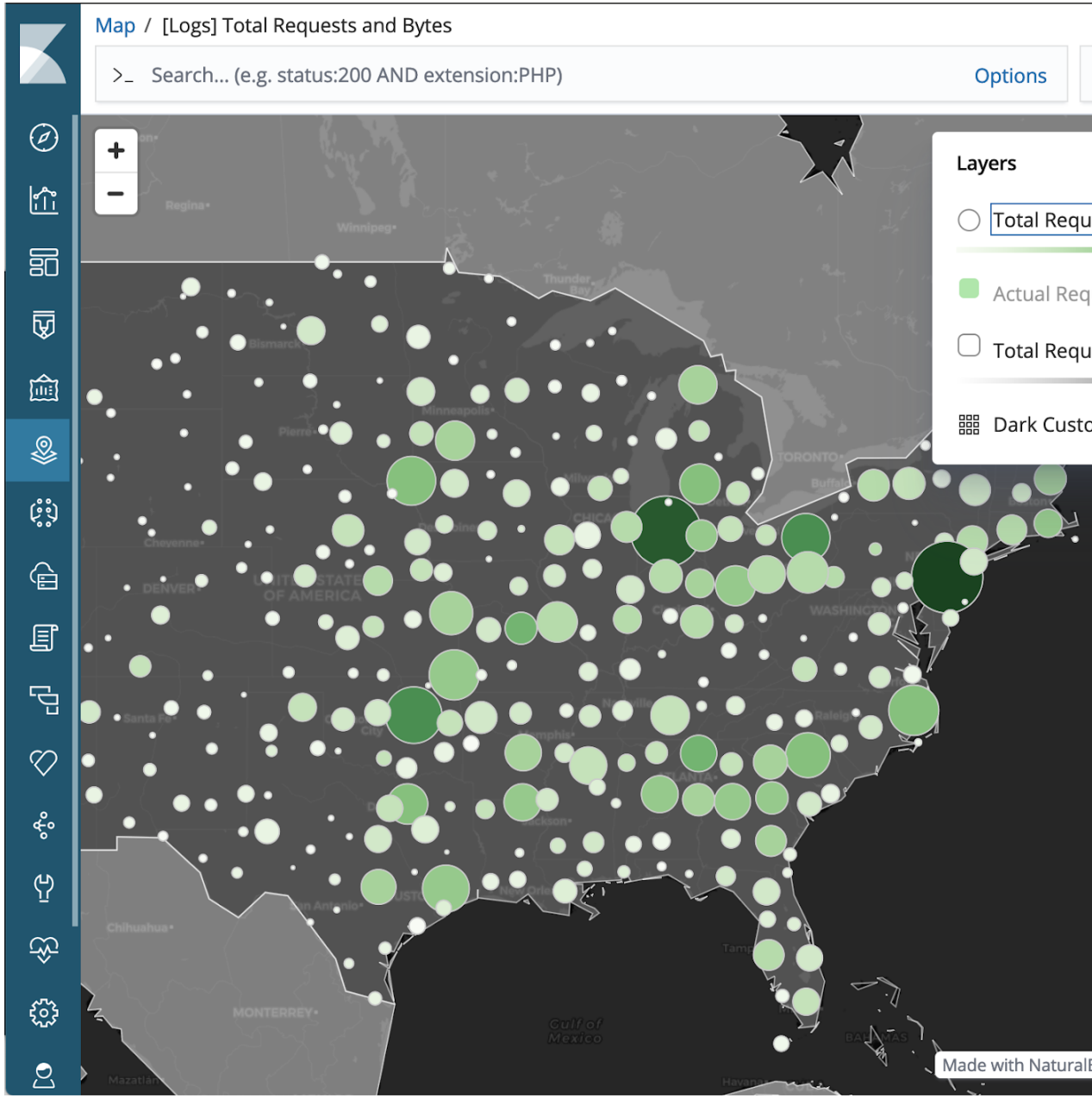
`geo_points` と **`geo_shapes`** 両方をMap上にそのまま表示可能

分析のためのグローバル検索

フルスクリーンモード

Elastic Maps Serviceによる地図

カスタマイズ



セキュリティ

データをセキュアに

セキュリティ

統合された細やかな制御

認証

Native (built-in)
3rd Party (LDAP と AD)

SSO (SAML & Kerberos)
カスタム (ユーザーによる追加)

細かな制御

ドキュメント & フィールドレベル権限

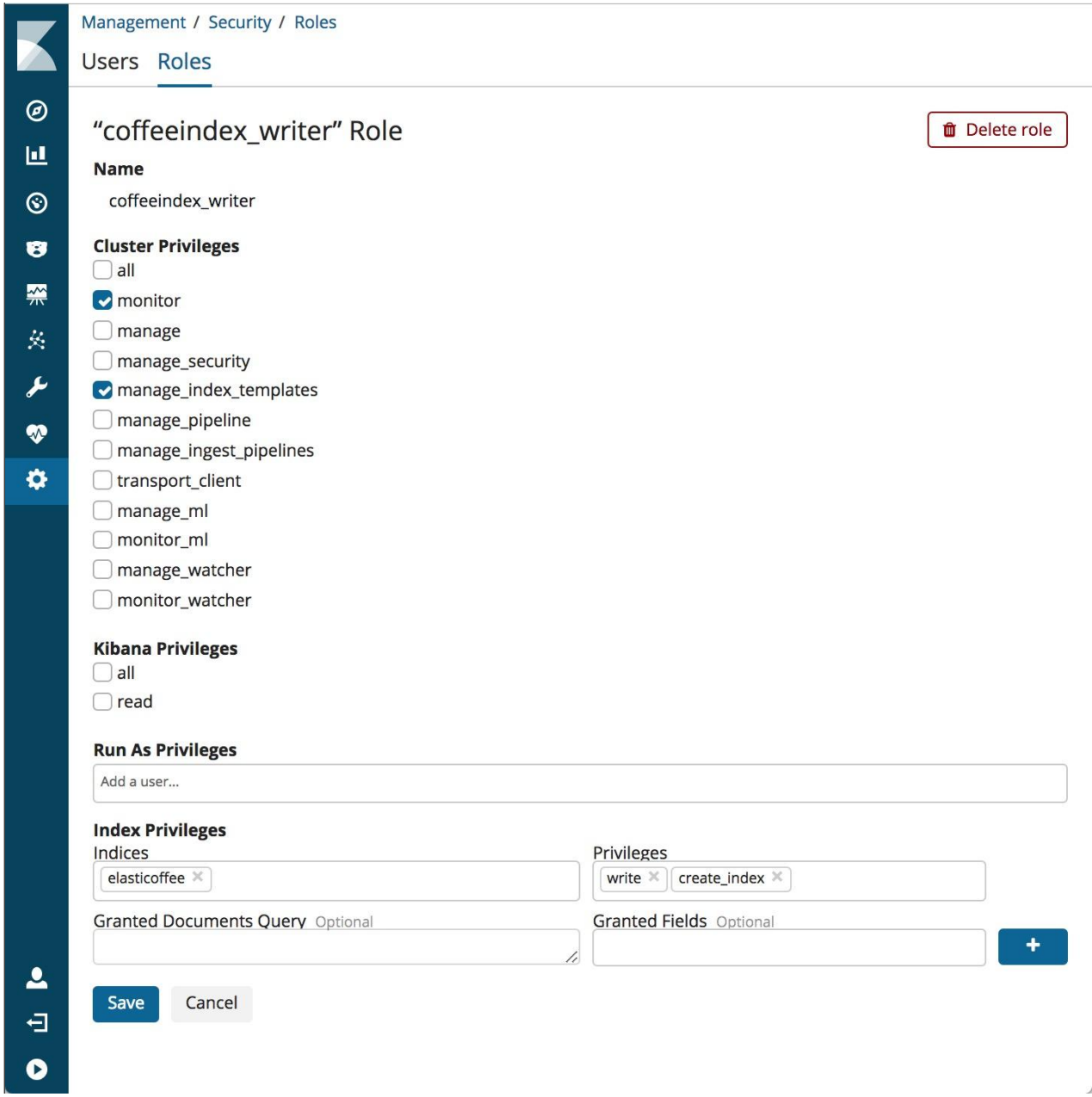
Kibanaのスペースとの統合

暗号化

通信 (TLS & SSL)

データ (dmcryptの利用)

その他にも (監査ログ、IP フィルタ...)



セキュリティ

統合された細やかな制御

認証

Native (built-in)
3rd Party (LDAP と AD)

SSO (SAML & Kerberos)
カスタム (ユーザーによる追加)

細かな制御

ドキュメント & フィールドレベル権限

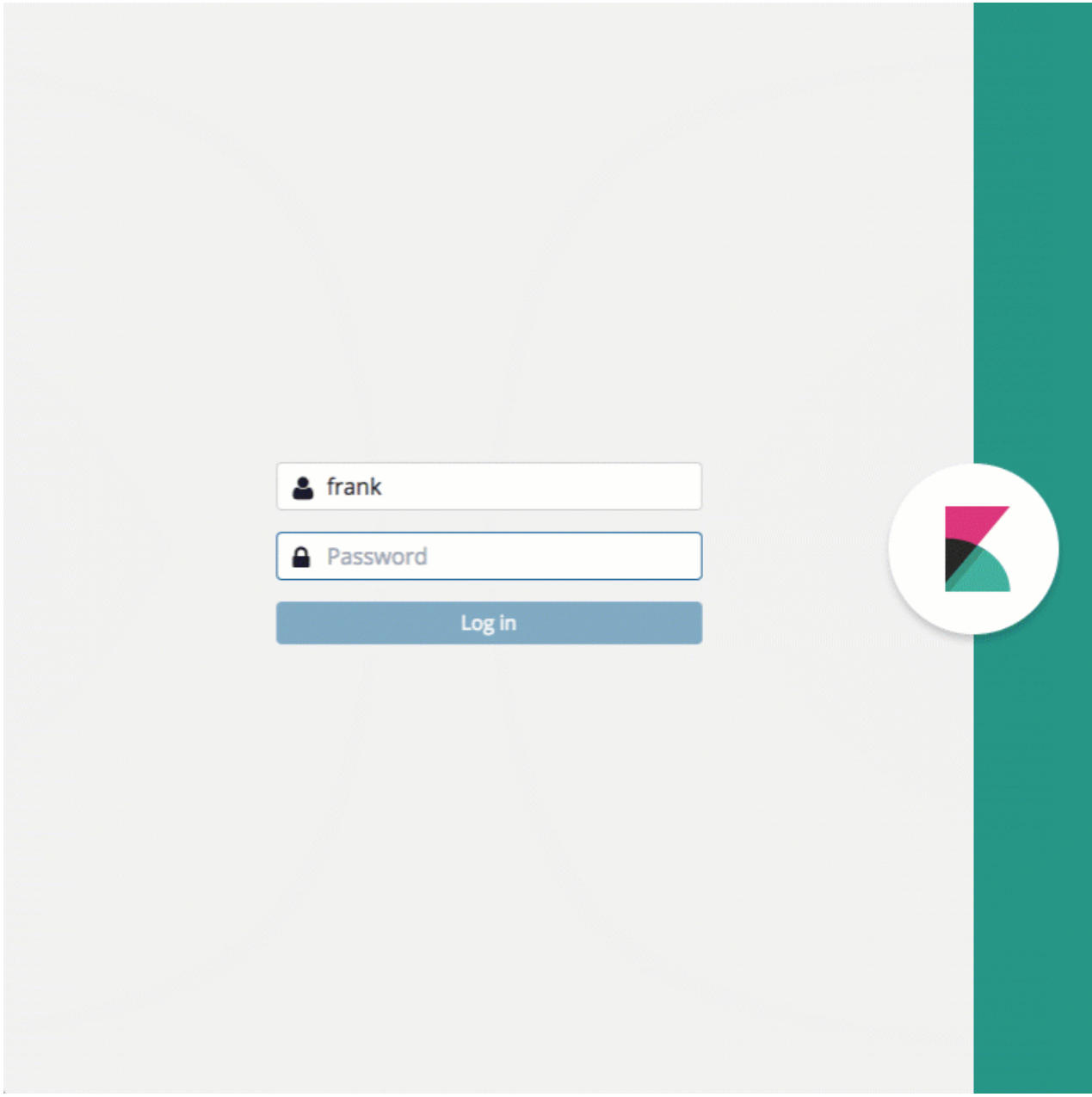
Kibanaのスペースとの統合

暗号化

通信 (TLS & SSL)

データ (dmcryptの利用)

その他にも (監査ログ、IP フィルタ...)



機械学習

自動的に問題点をあぶり出す

機械学習

データの異常を検知

自動的な異常検知

教師なし学習

継続的 (オンライン) モデル

複数の時系列データに対応

集団からの外れ値

予測

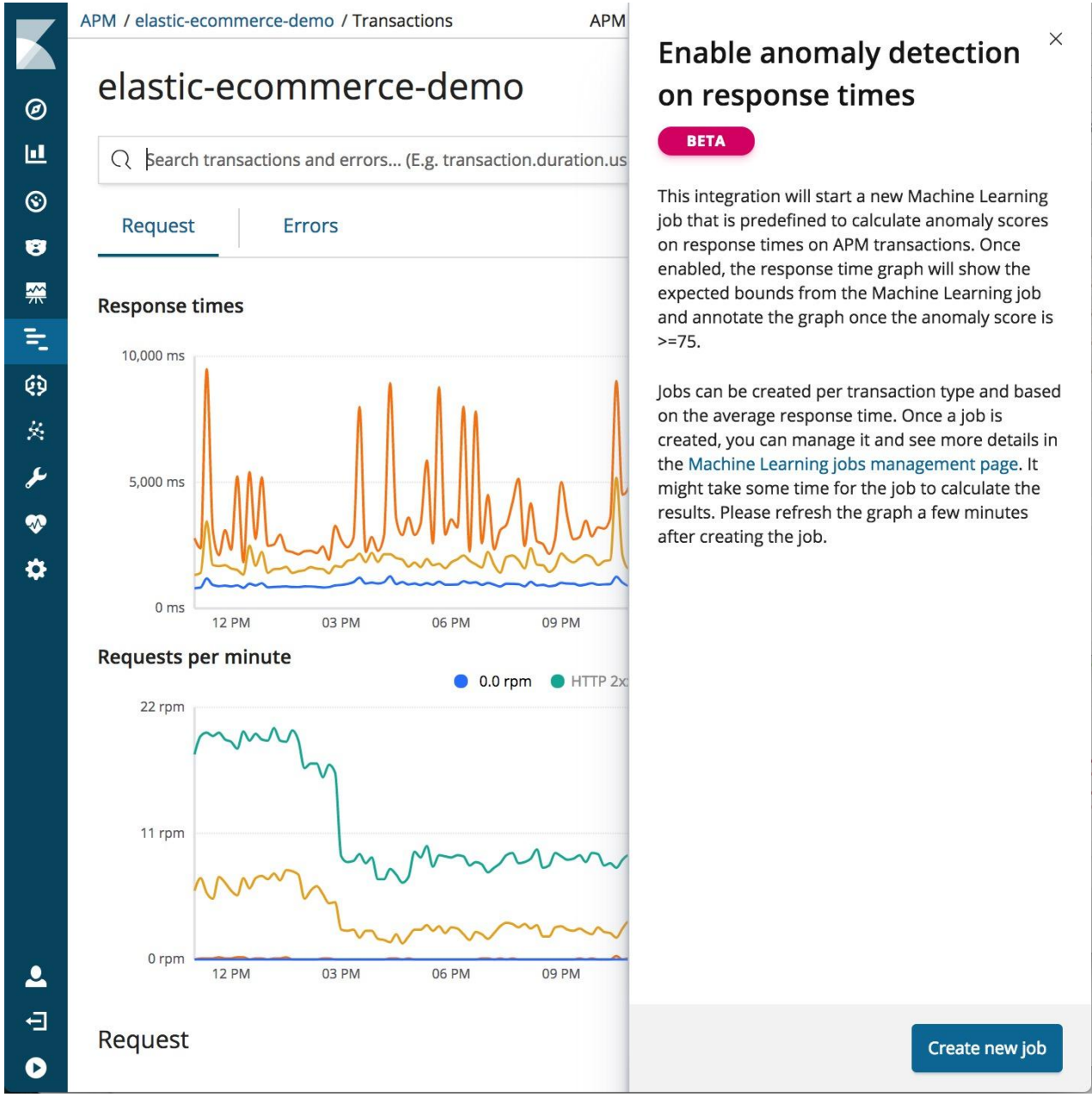
多くのユースケース

ITオペレーション

セキュリティ分析

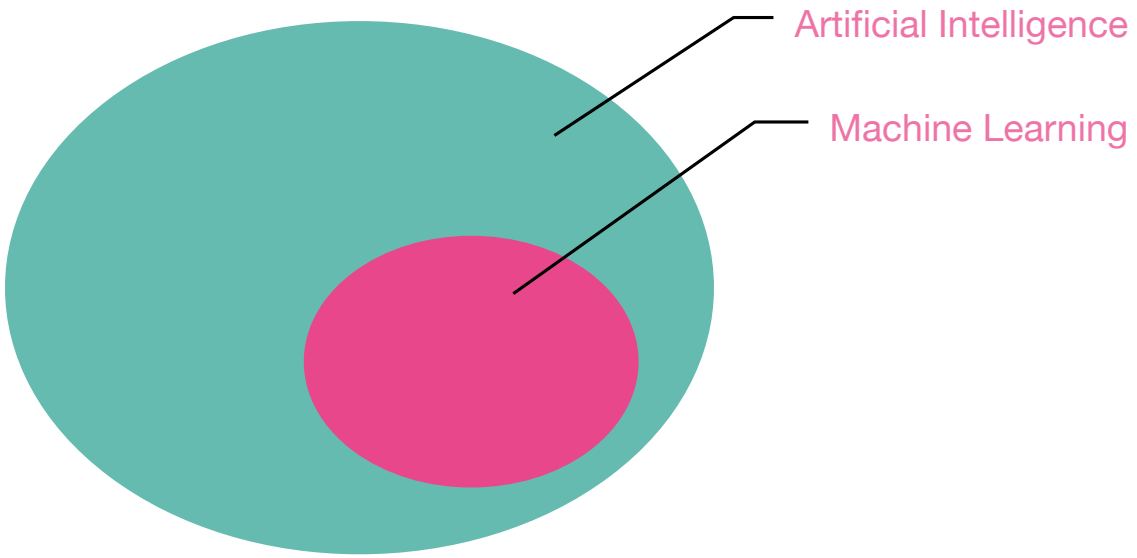
ビジネスKPI

APM



What's Machine Learning?

- **Algorithms that**
  - Learn from Data
  - Using Statistical Techniques
  - Without Explicit Programming



Elastic Machine Learning Scope

Image Classification **Recommendations**

Autonomous cars Voice Recognition Predictive Medicine

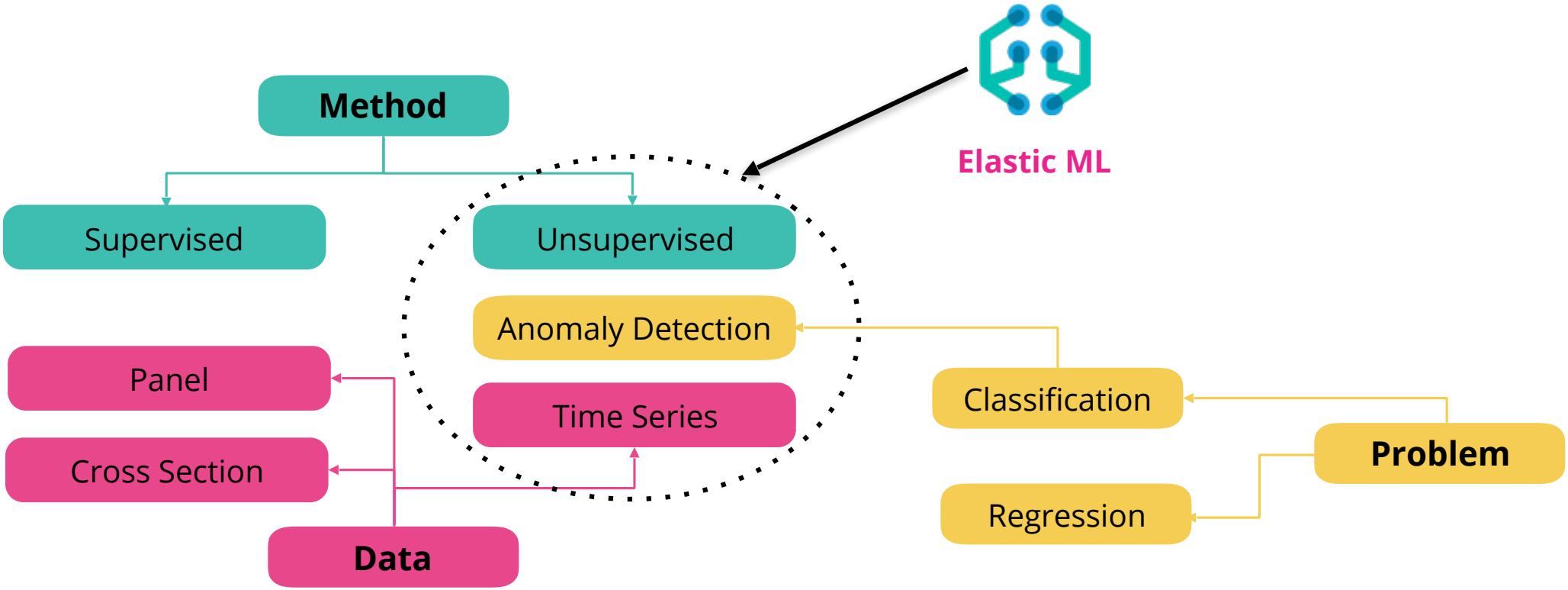
Fraud detection **Anomaly Detection**

Learn to Rank Speech Recognition

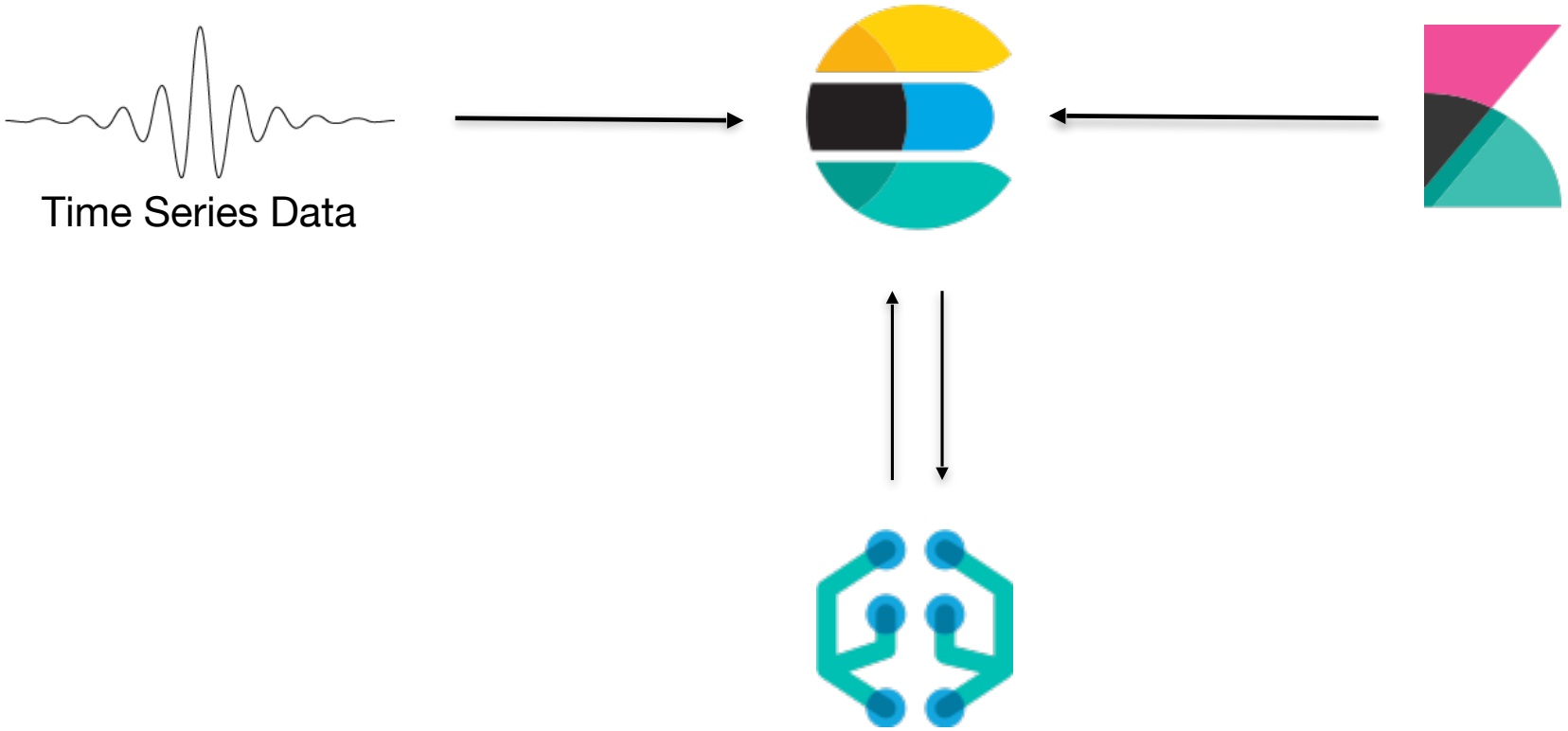
Language Translation **Entity Resolution**

elastic

Elastic Machine Learning Scope



Elastic Machine Learning Flow

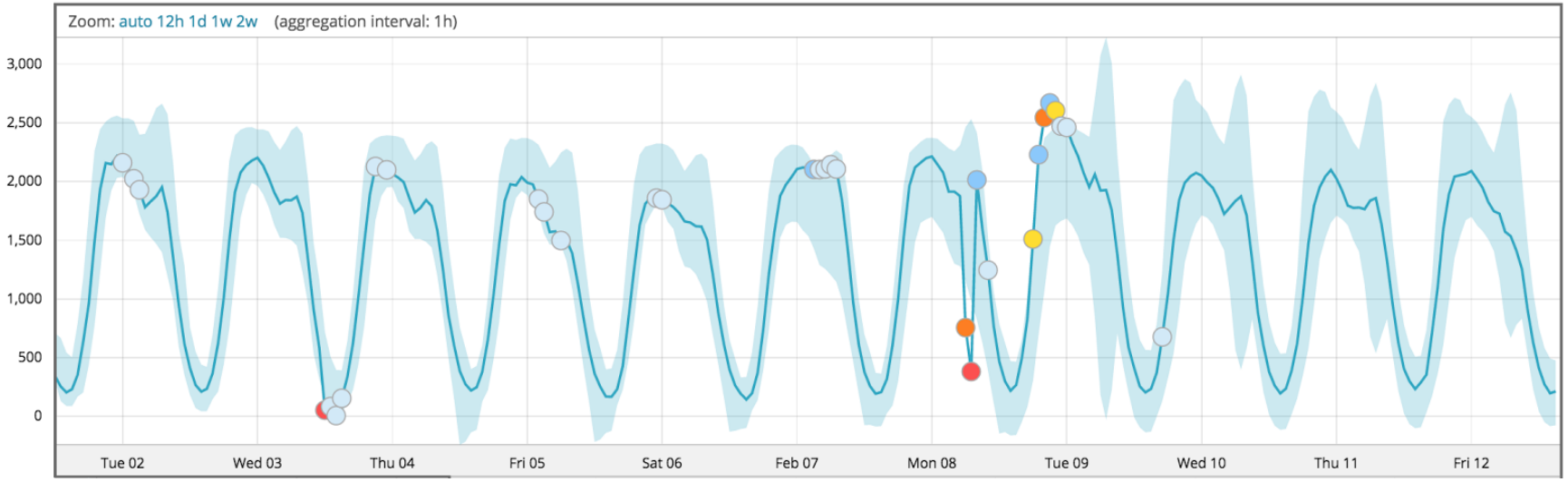


Challenges that Anomaly Detection Solves

- **IT Operations**
  - How do I know my systems are behaving normally?
  - Where to set thresholds for good alerting?
  - How to find the root cause of problems when I don’t know what to look for?
- **IT Security**
  - Do I have systems that are compromised with malware?
  - Which users could be an insider threat?
- **IoT / SCADA / Other**
  - Is my factory working normally?
  - What do I do with thousands of time-series data points?
  - Which traffic incidents are causing the most delay?

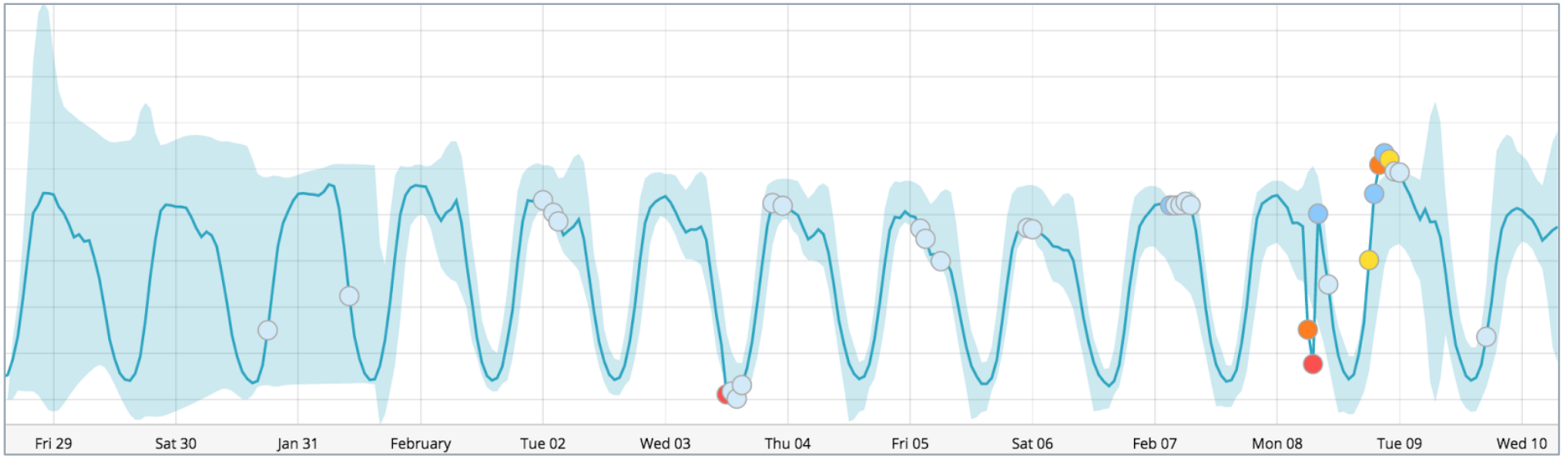
Elastic Machine Learning

- Uses unsupervised machine learning techniques to
  - Learn what's "normal" by modeling historic behavior
  - Detect anomalies when data falls outside expected bounds
  - Use models to predict future behavior (prediction)
  - Use predictions to make decisions



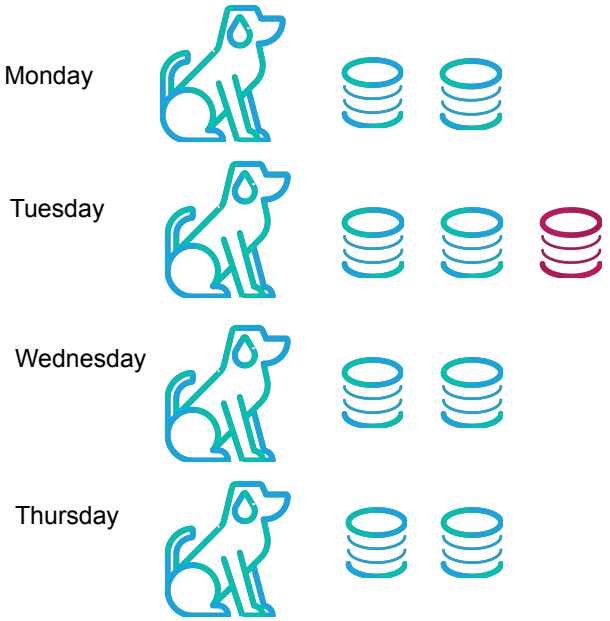
Elastic Machine Learning

- Unsupervised techniques - no manual training / input needed
- Evolves with the data - “online” model learns continuously
- Influencer detection - accelerates root cause identification

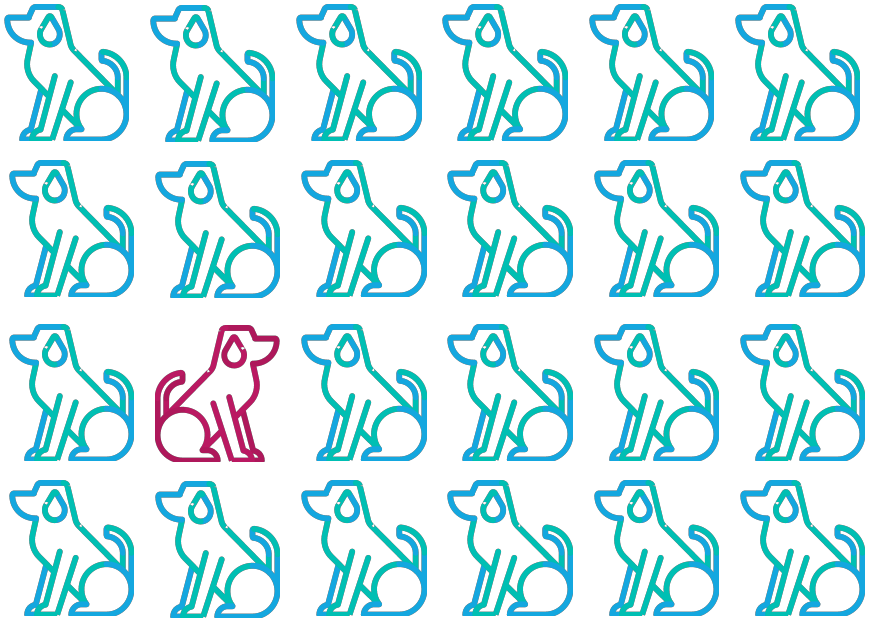


Population Analysis / Entity Behavior Analytics with ML

When something behaves like itself



When something behaves like its peers

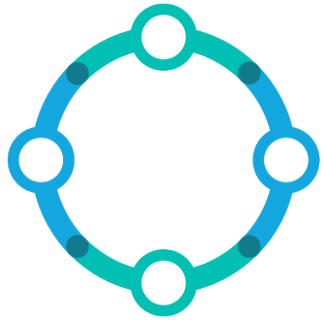


The advantages of anomaly-driven alerting

Understand Seasonality

Reduce False Positives

Identify Areas of Focus



Avoid Manual Review and Revision

アラート

データに基づき通知し、アクションを起こす

Alerting

Alert on anything you can query

Powered by Elasticsearch

Alert on any Elasticsearch query

Distributed execution

Highly available

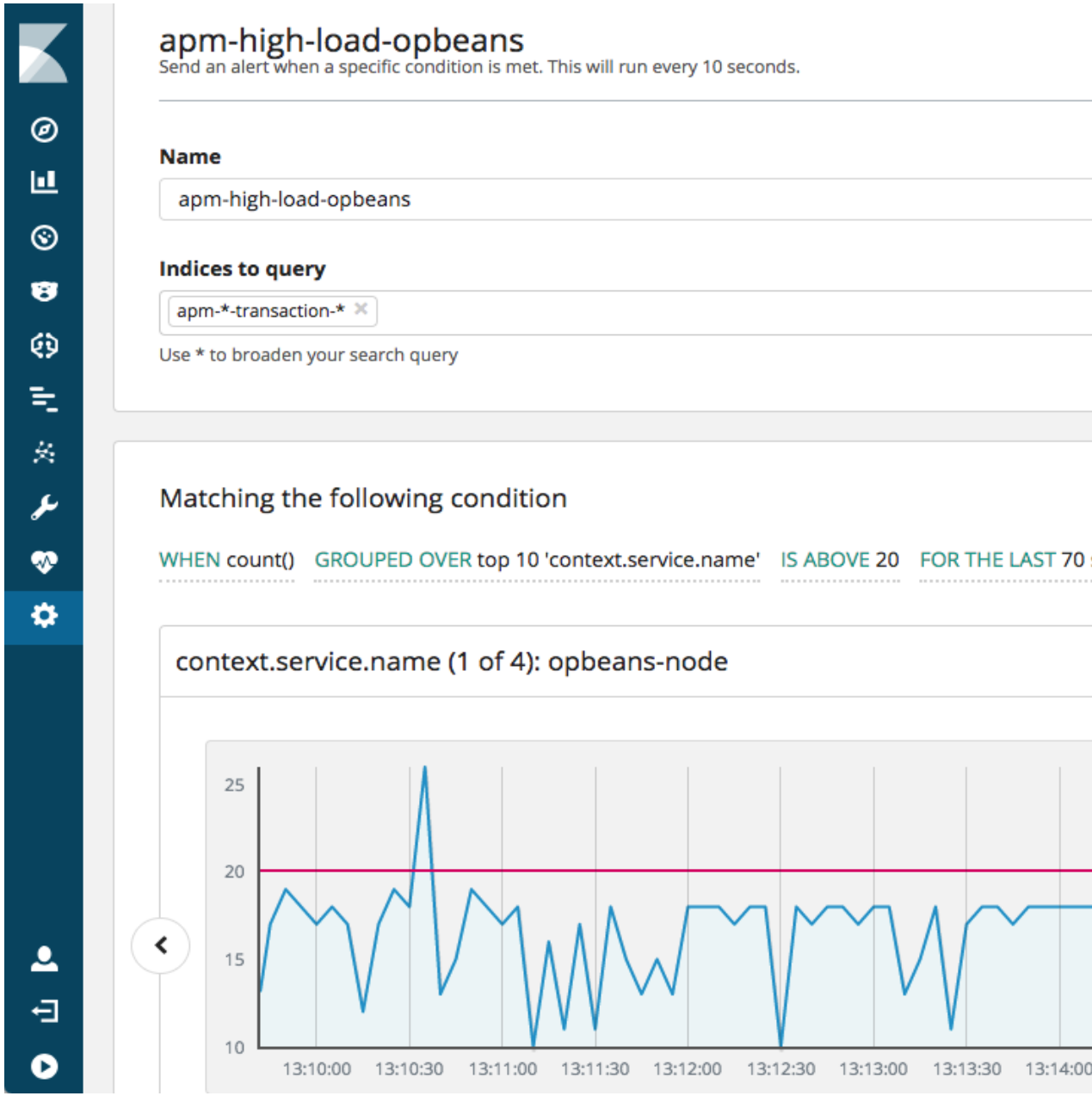
Notifications

Email, Slack, PagerDuty.

Custom (webhook)

Stack Integrations

Machine learning, Monitoring, and Reporting



Alerting

Alert on anything you can query

Powered by Elasticsearch

Alert on any Elasticsearch query

Distributed execution

Highly available

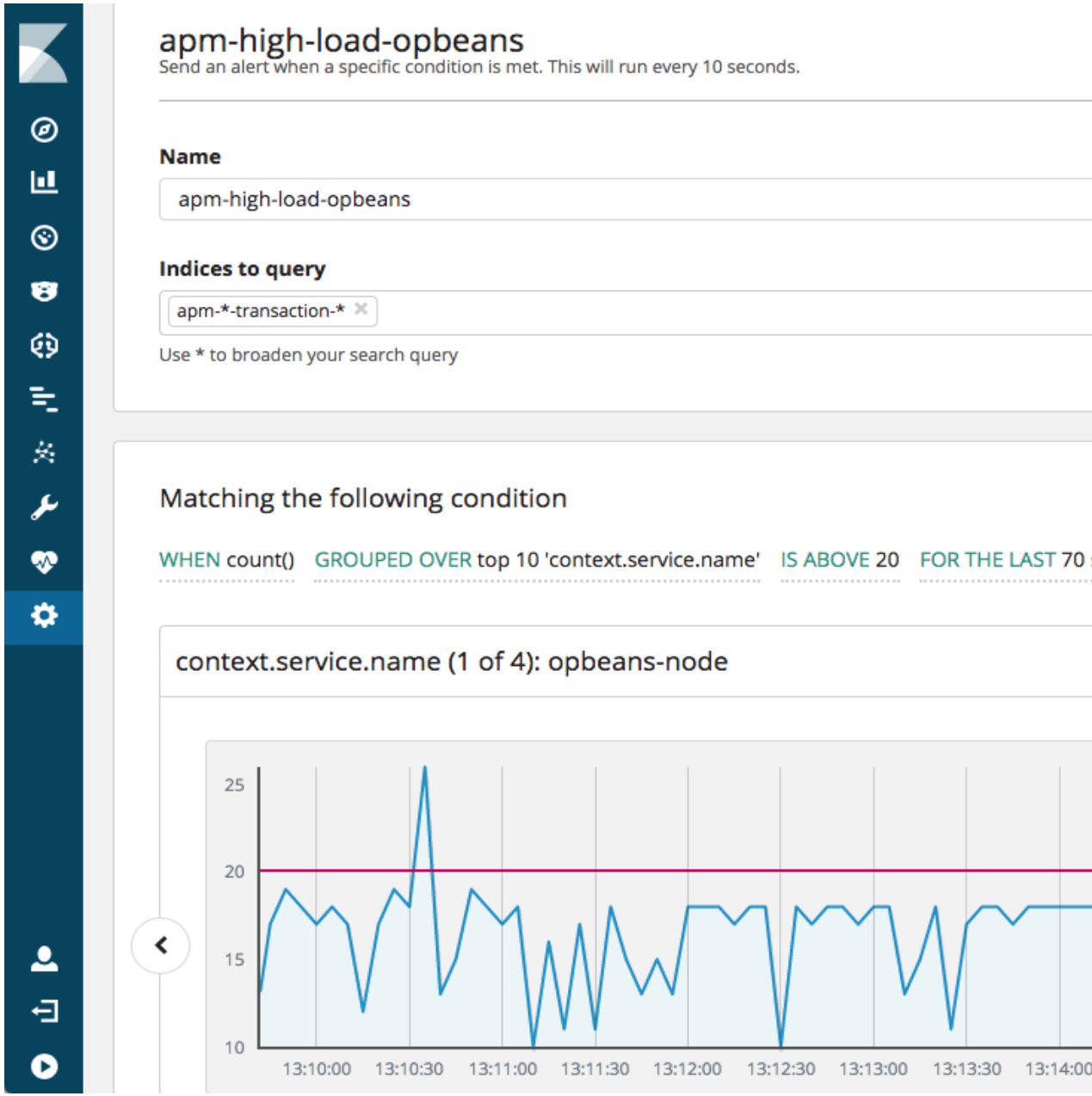
Notifications

Email, Slack, PagerDuty.

Custom (webhook)

Stack Integrations

Machine learning, Monitoring, and Reporting



Alert Users to Conditions

Host Behavior

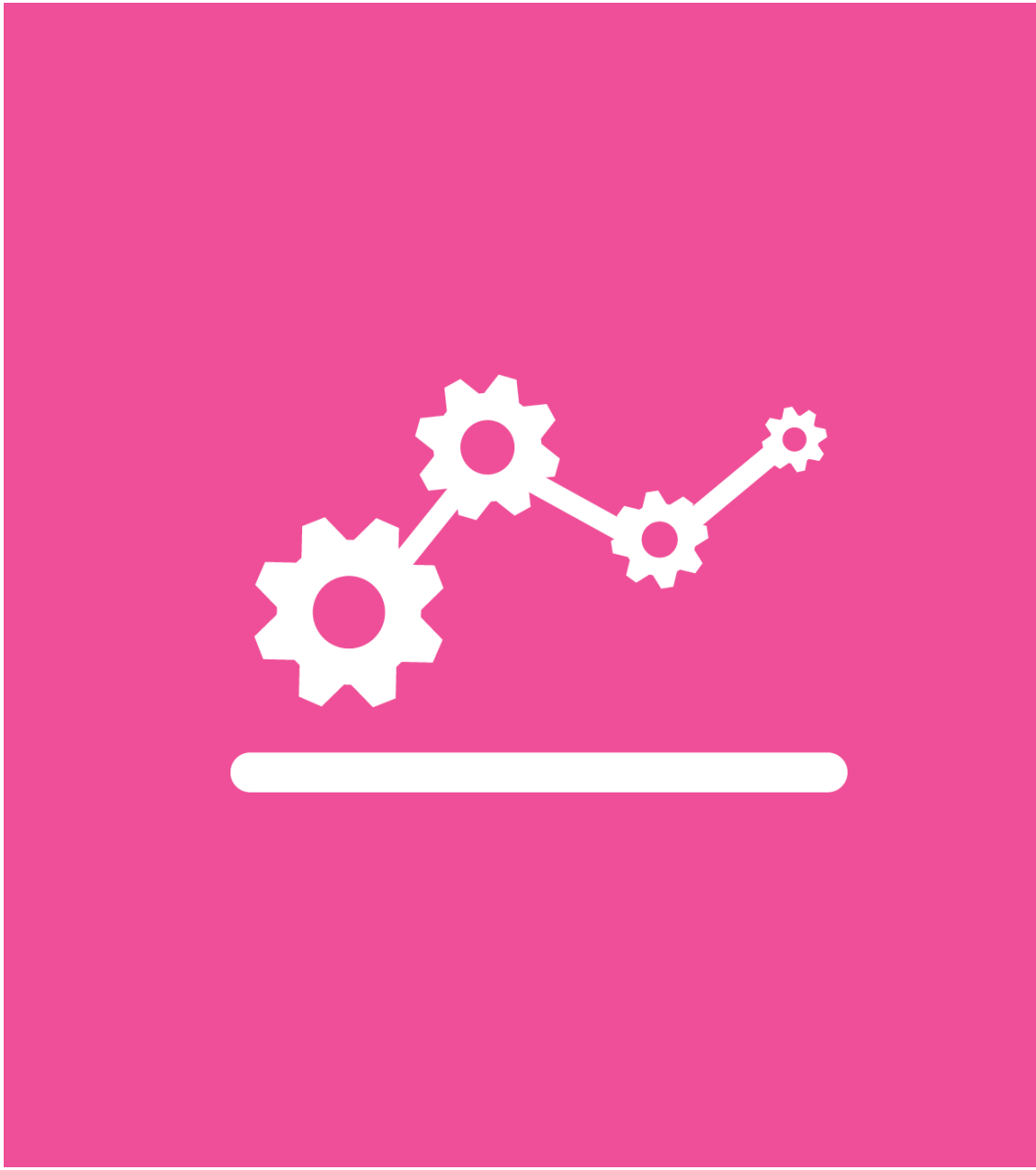
- Free disk space goes below 5%
- Process X starts on any server

Network or User Behavior

- > 5 failed logins on a machine in 5 min
- Excessive data transfer

Application Monitoring

- App response time exceeds SLA
- Active connections exceed threshold



Alert using all of the power of Elasticsearch

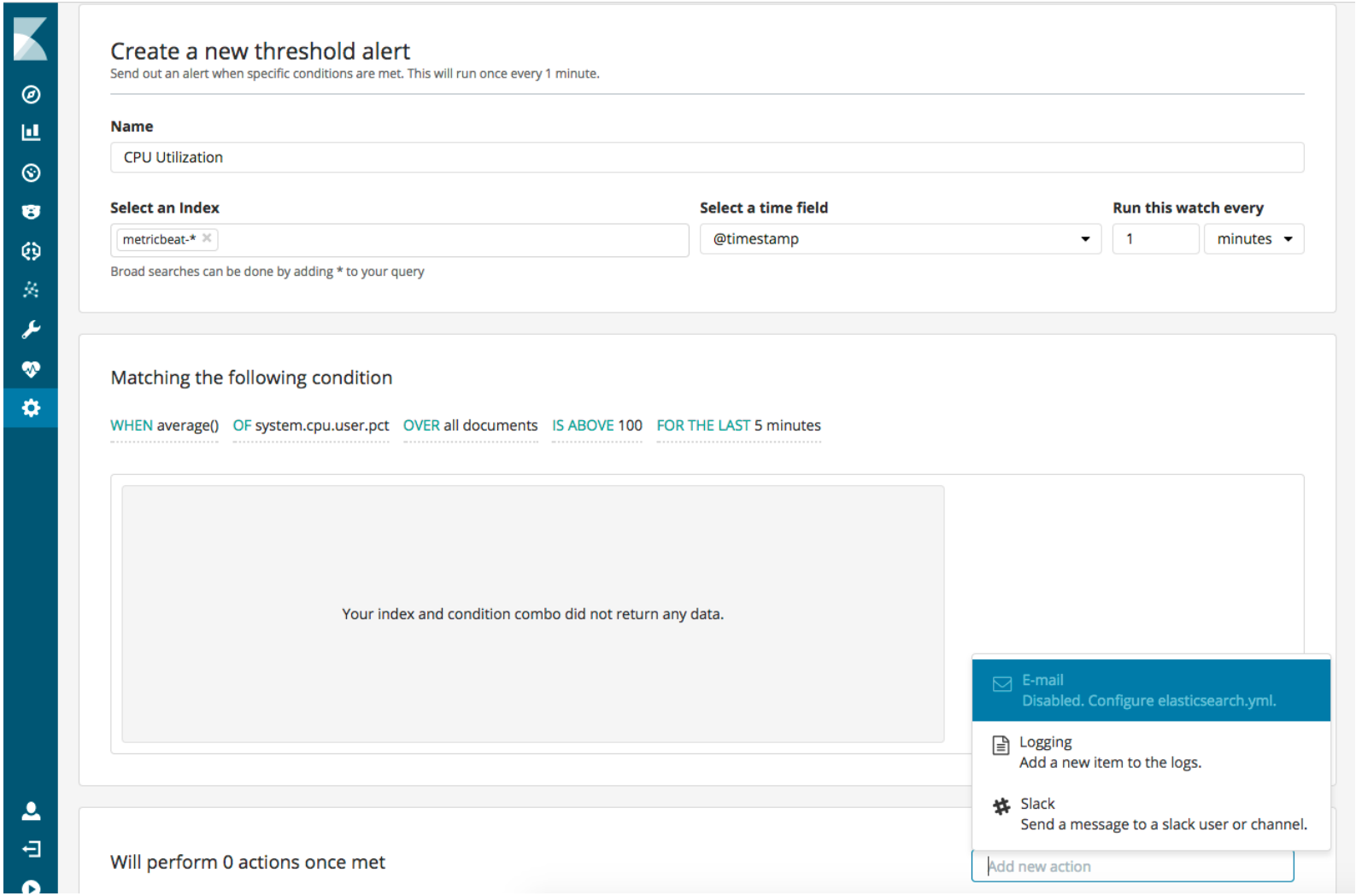
If you can query it, you can alert on it

- any Elasticsearch queries (full-text, geo, date math, pipeline aggs)
- anomalies detected by **machine learning**

Combine data from multiple sources

- Combine multiple Elasticsearch indices
- Include external http feeds (weather, threats feeds, etc.)

Creating Threshold Based Alerts is Easy



Leverage Your Alert History

Full alert history is available:

- How often are SLAs violated?
- What security incidents are trending?
- Which servers fail the most?
- What events are correlated with other events in the infrastructure?

Elastic SIEM (beta)

Same data. Different questions.

Ingest & prepare

Ecosystem of network and host data connectors

Elastic Common Schema (ECS)

Analytics

Machine learning and alerting

Ad hoc queries at scale

Graph analytics

Detect, hunt, investigate

Automated attack detection

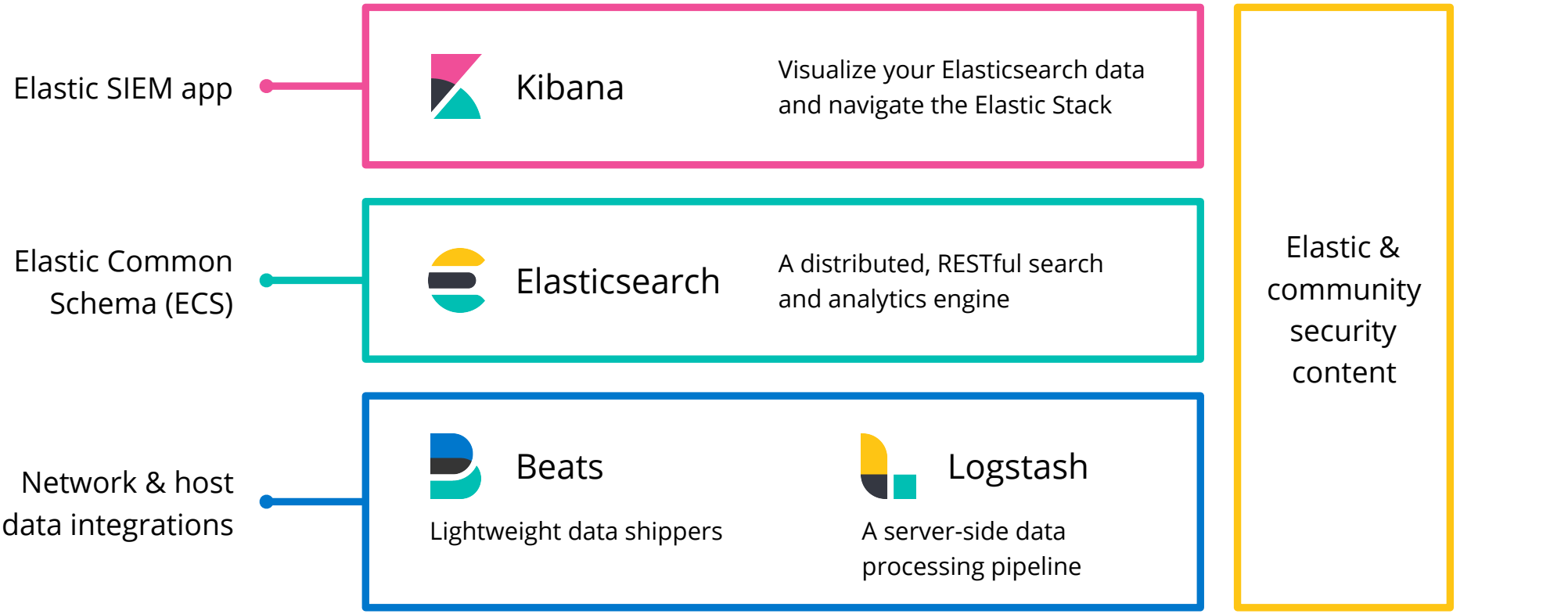
Interactive threat hunting

Rapid event triage and investigation

elastic

Elastic SIEM

A SIEM for Elastic Stack users everywhere



elastic

Elastic SIEM app (beta)

Triage and qualify security alerts at the speed of thought

Analyst-friendly experience for investigating security alerts

Time-ordered events

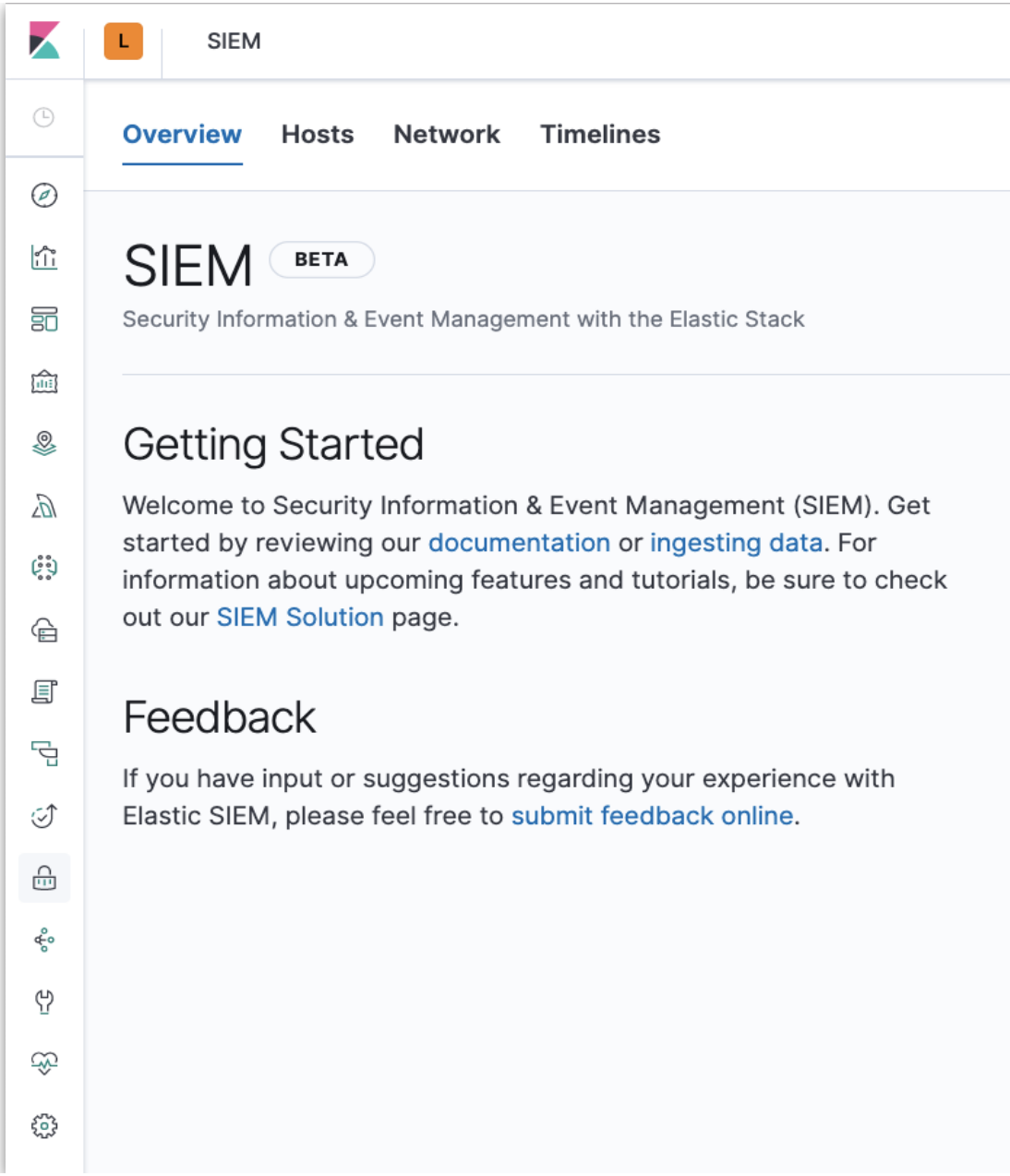
Drag-and-drop filtering

Multi-index search

Annotations, comments

Formatted event views

Persistent forensic data storage



Data Frame

Basic (free)

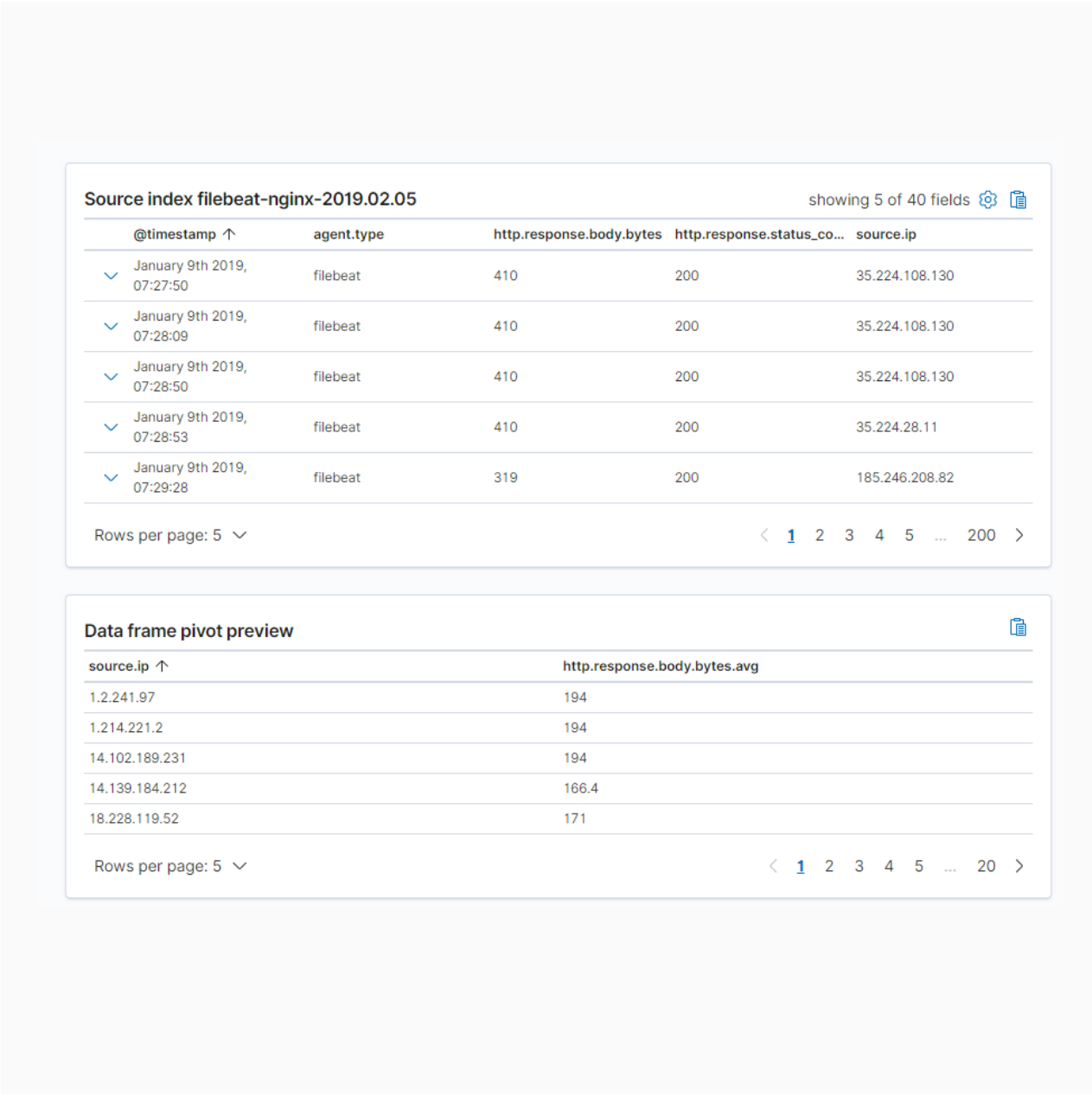
Pivot and aggregate existing indices to secondary index for specific use-cases

For example:

- summarize user behavior
- create entity-centric indices

New wizard in Machine Learning app

Currently implemented as batch job on existing indices



Thank you!

Elastic Training

Empowering Your People

Immersive Learning

Lab-based exercises and knowledge checks to help master new skills

Solution-based Curriculum

Real-world examples and common use cases

Experienced Instructors

Expertly trained and deeply rooted in everything Elastic

Performance-based Certification

Apply practical knowledge to real-world use cases, in real-time