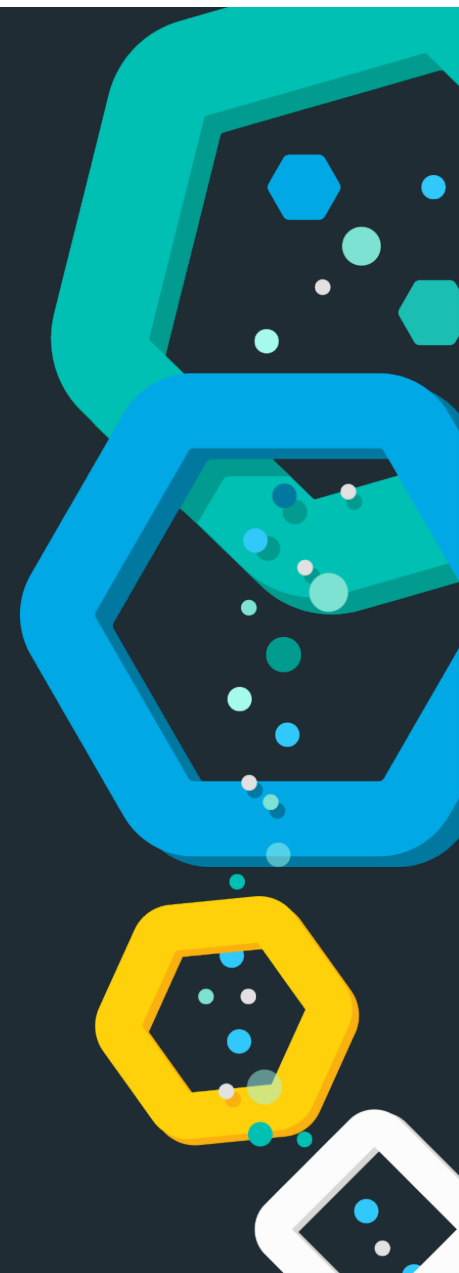




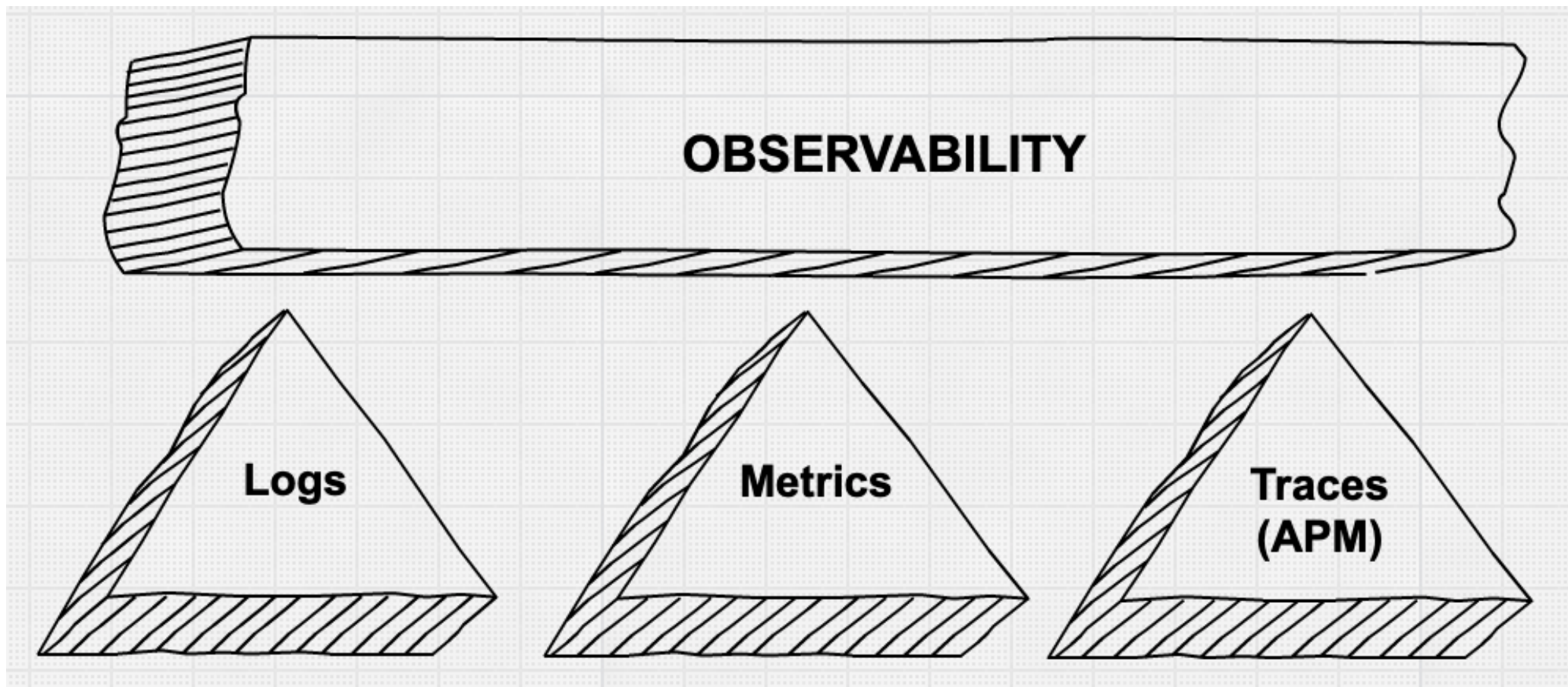
ElasticsearchとKibanaによるオブ ザバービリティハンズオン

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>





マイクロサービス???

 **Honest Status Page**
@honest_update フォローする

We replaced our monolith with micro services so that every outage could be more like a murder mystery.

 ツイートを翻訳

8:10 - 2015年10月8日

3,013件のリツイート 2,612件のいいね



 21  3,013  2,612 

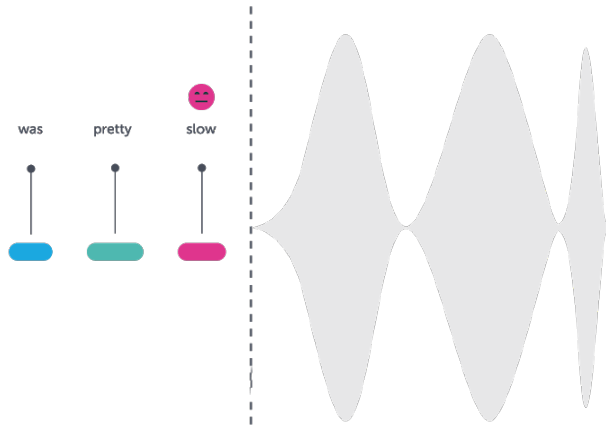
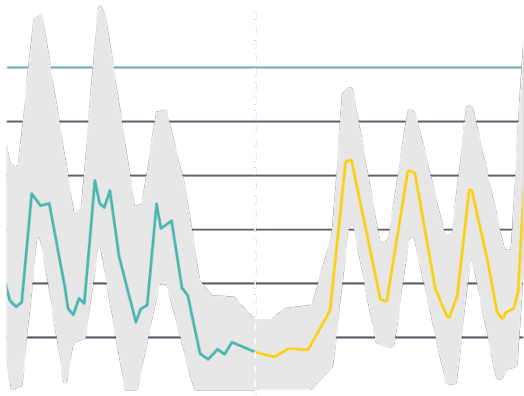
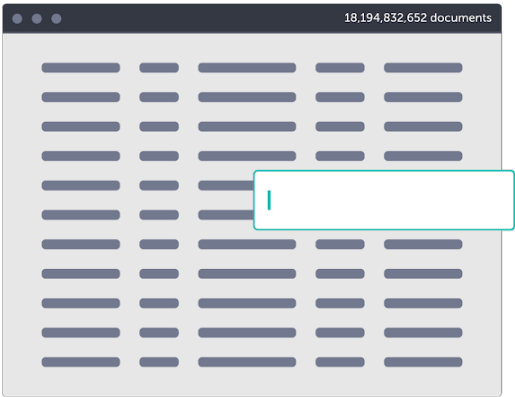
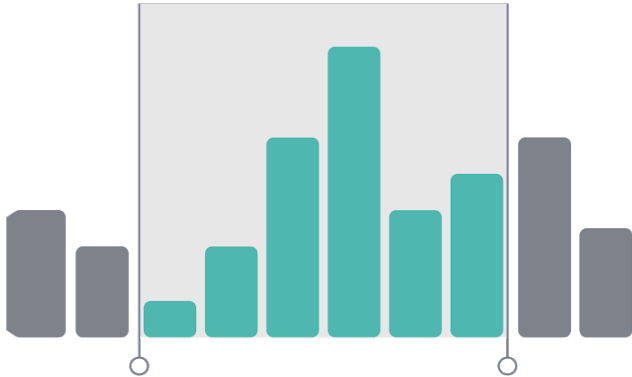
Elastic は **search company**

Elasticsearch は検索の技術

検索は**基礎技術**



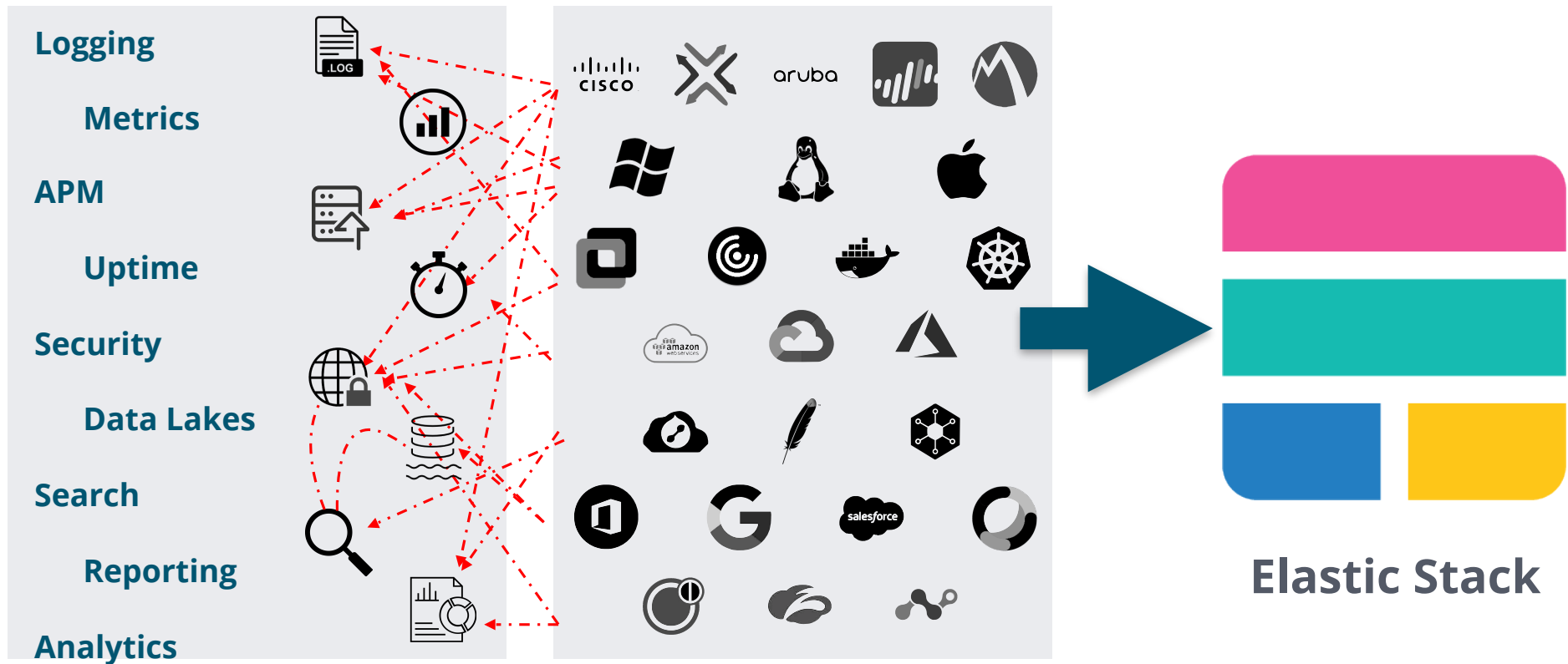
.54 seconds | 1,000,000,000 records



技術による差別化



複雑さを減らしましょう



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



LOGGING



METRICS



APM



ENTERPRISE
SEARCH



APP SEARCH



SITE SEARCH



BUSINESS
ANALYTICS



SECURITY

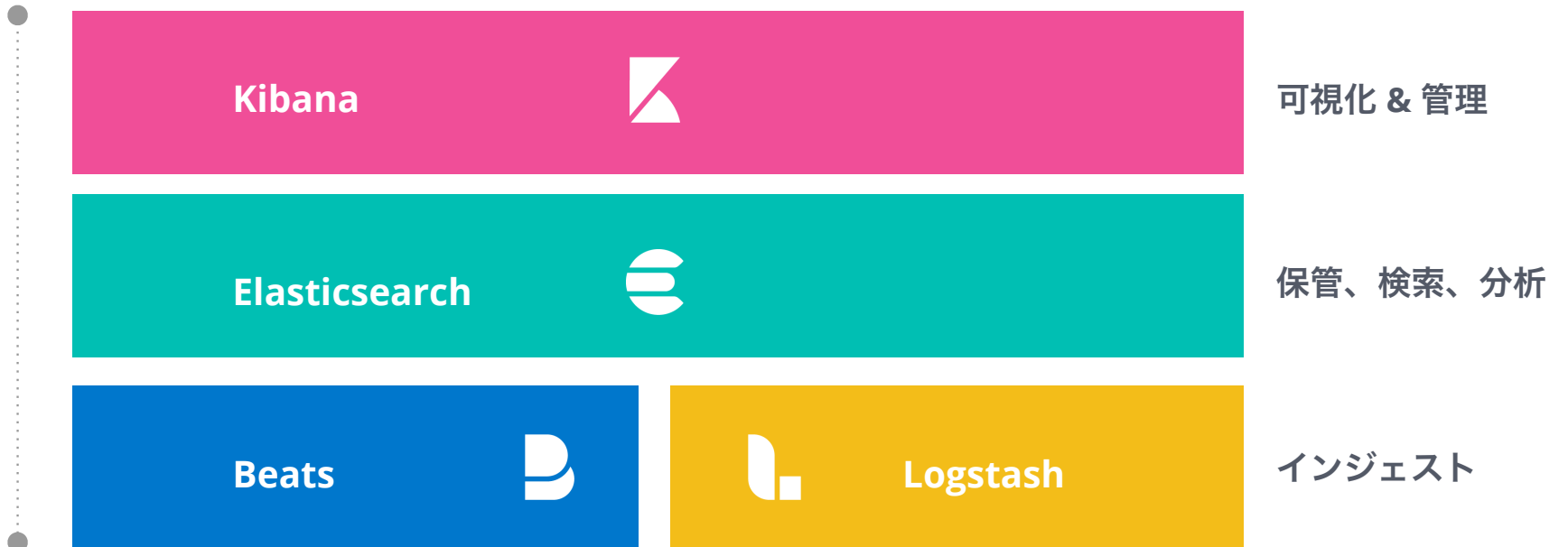


MAPS

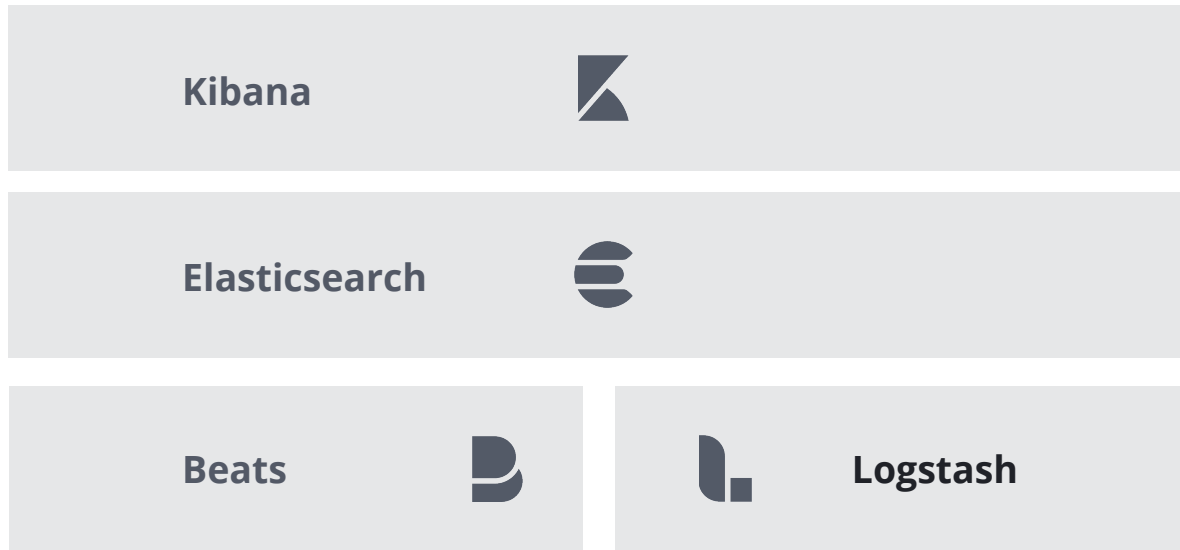
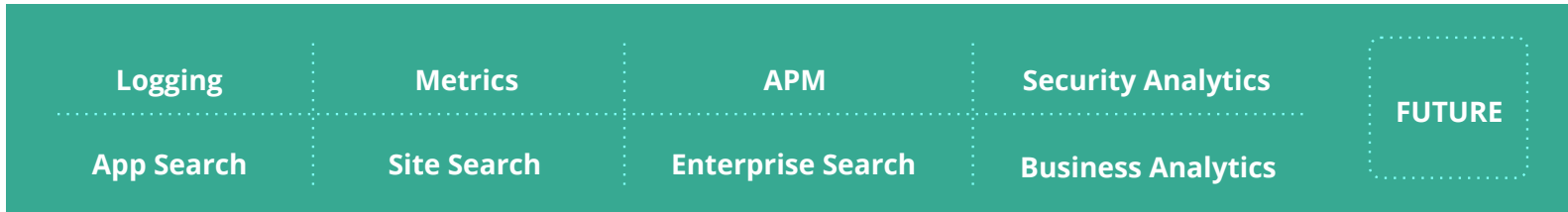


UPTIME

Elastic Stack



ソリューション



SaaS

SELF-MANAGED

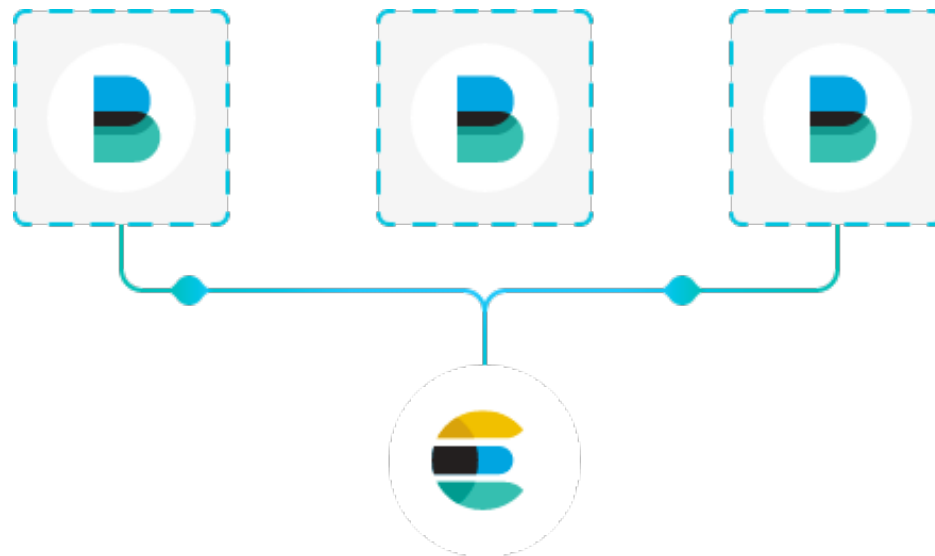


beats



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

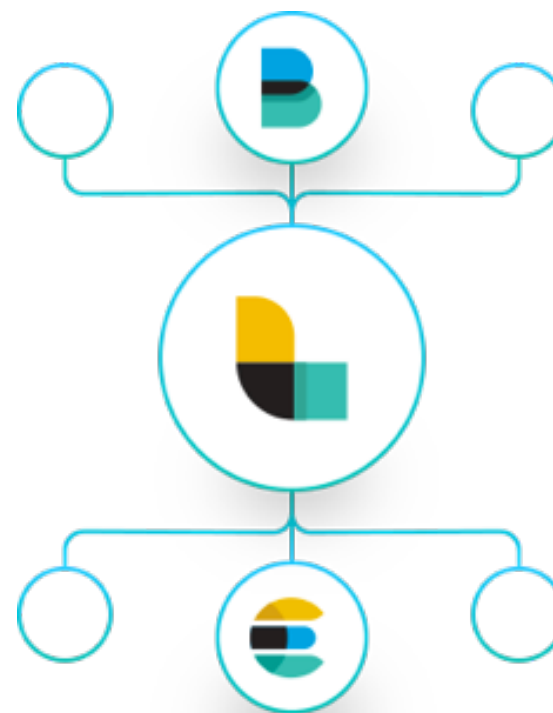


logstash



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

安全で暗号化された
データ入力

パースと動的な
データ変換

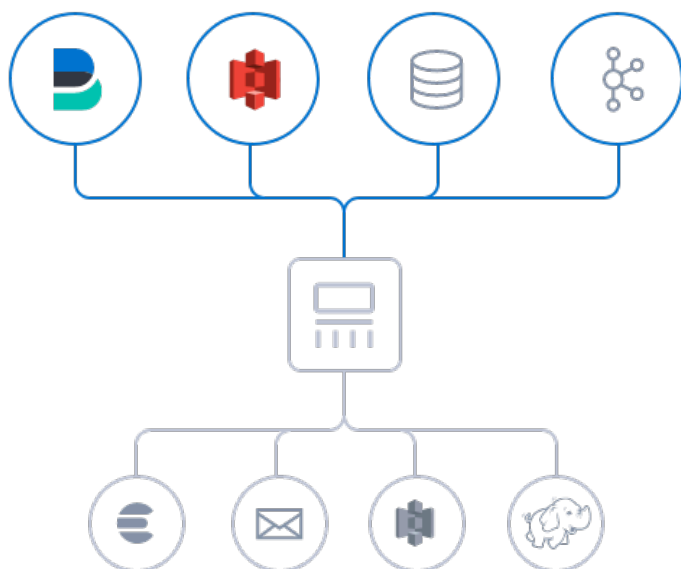
独自のパイプライン処理
の作成

あらゆる出力に
データ転送

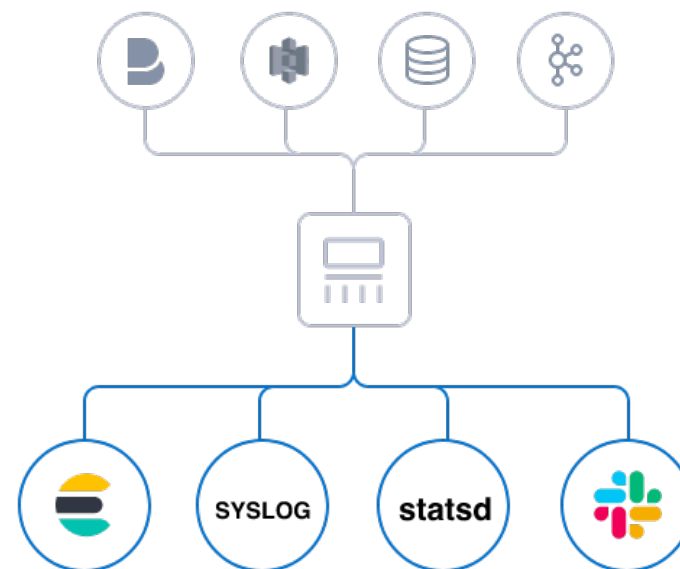
200以上のプラグイン

多種多様な入出力

さまざまな入力プラグイン

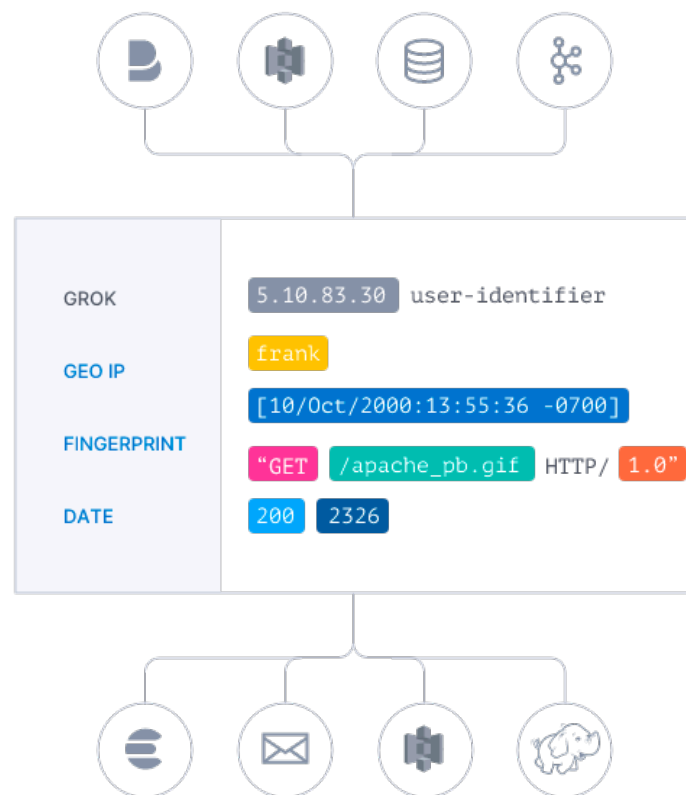


さまざまな出力プラグイン



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

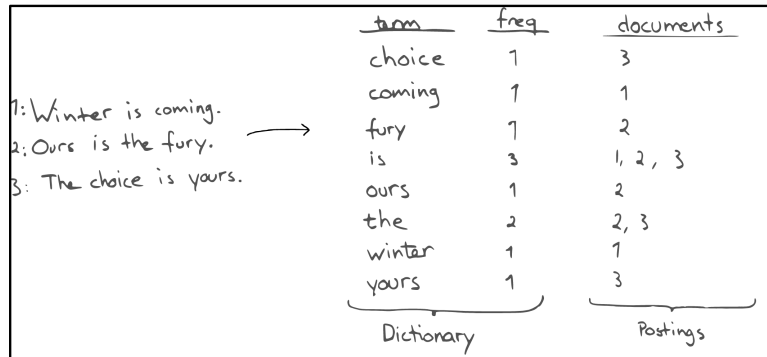
開発者フレンドリー

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

userid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrjce	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

Management

- Elasticsearch
 - License management
 - Users
 - Roles
 - Watches
 - Index management
 - Index rules
- Kibana
 - Index patterns
 - Reporting
 - Advanced settings
 - Saved objects
- Logstash
 - Pipelines

Create a new rollup job

Optional: Collect metrics on important fields
You can collect metrics on as many fields as you want.

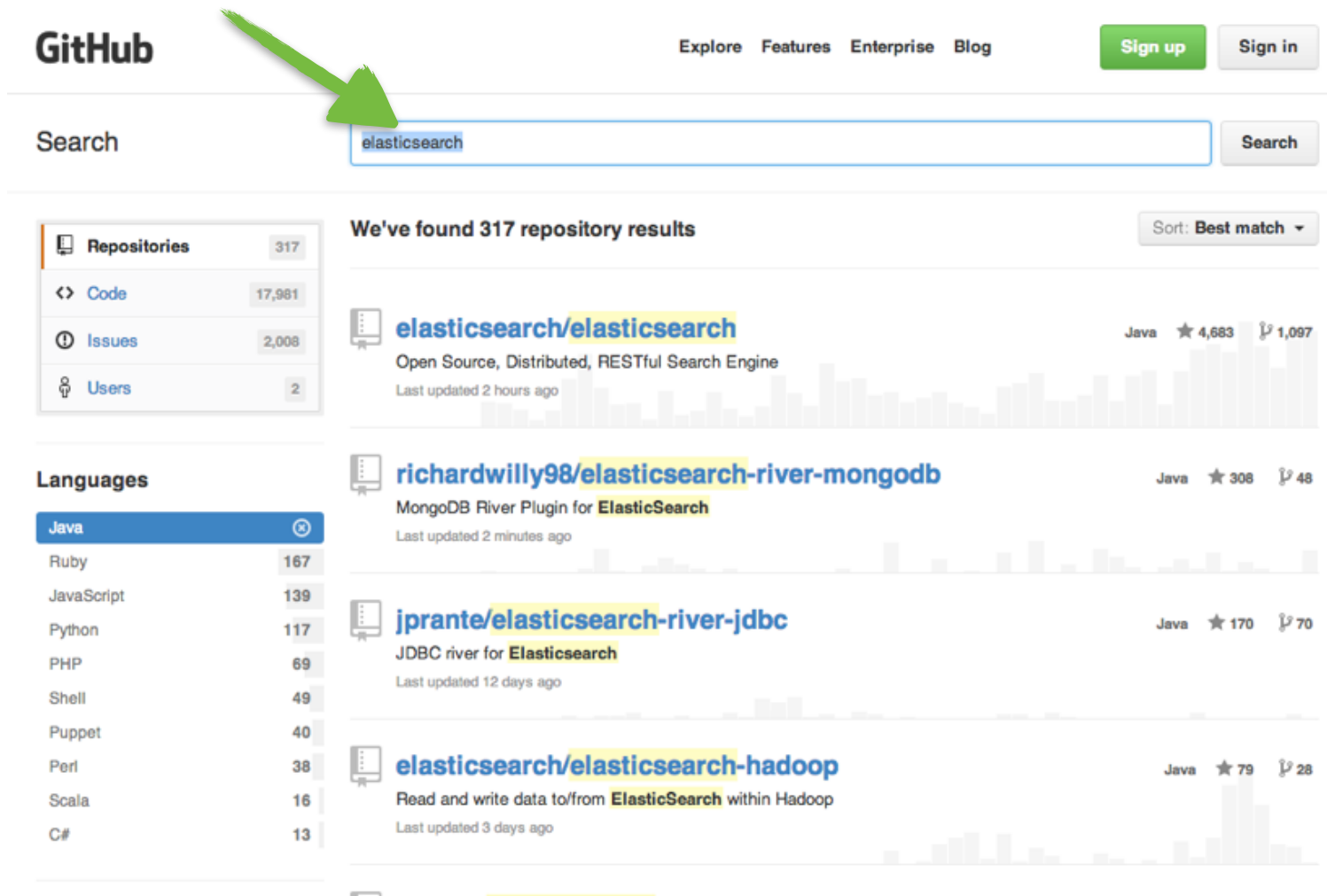
Field	Min	Max	Avg	Sum	Value count	Cardinality
system.network.out.bytes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
system.network.out.errors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
system.network.usage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Metric to aggregate: system.network.high_fives

Metrics to capture: Min, Max, Sum, Value count

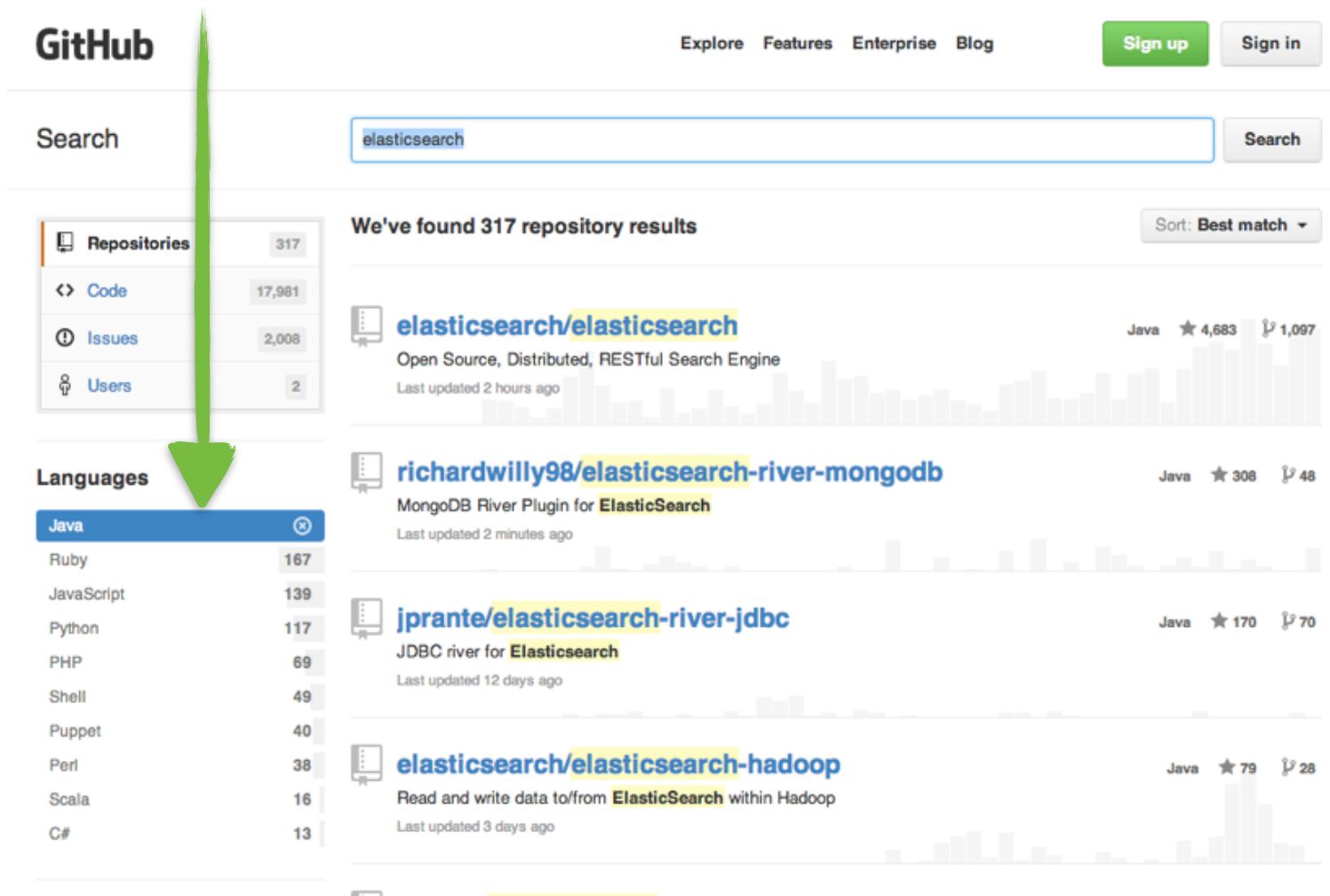
Elasticsearchとは？

フリーワード検索



The screenshot shows the GitHub search interface. At the top left is the GitHub logo. To its right are links for 'Explore', 'Features', 'Enterprise', and 'Blog'. Further right are 'Sign up' and 'Sign in' buttons. Below the GitHub logo is the word 'Search'. A search bar contains the text 'elasticsearch' and a green arrow points to it from the left. To the right of the search bar is a 'Search' button. Below the search bar, the results are displayed. On the left side, there is a sidebar with 'Repositories' (317), 'Code' (17,981), 'Issues' (2,008), and 'Users' (2). Below this is a 'Languages' section with a list: Java (167), Ruby (139), JavaScript (117), PHP (69), Shell (49), Puppet (40), Perl (38), Scala (16), and C# (13). The main content area shows 'We've found 317 repository results' with a 'Sort: Best match' dropdown. The first result is 'elasticsearch/elasticsearch' (Java, 4,683 stars, 1,097 forks), described as 'Open Source, Distributed, RESTful Search Engine'. The second is 'richardwilly98/elasticsearch-river-mongodb' (Java, 308 stars, 48 forks), described as 'MongoDB River Plugin for ElasticSearch'. The third is 'jprante/elasticsearch-river-jdbc' (Java, 170 stars, 70 forks), described as 'JDBC river for Elasticsearch'. The fourth is 'elasticsearch/elasticsearch-hadoop' (Java, 79 stars, 28 forks), described as 'Read and write data to/from ElasticSearch within Hadoop'. Each result includes a commit history bar.

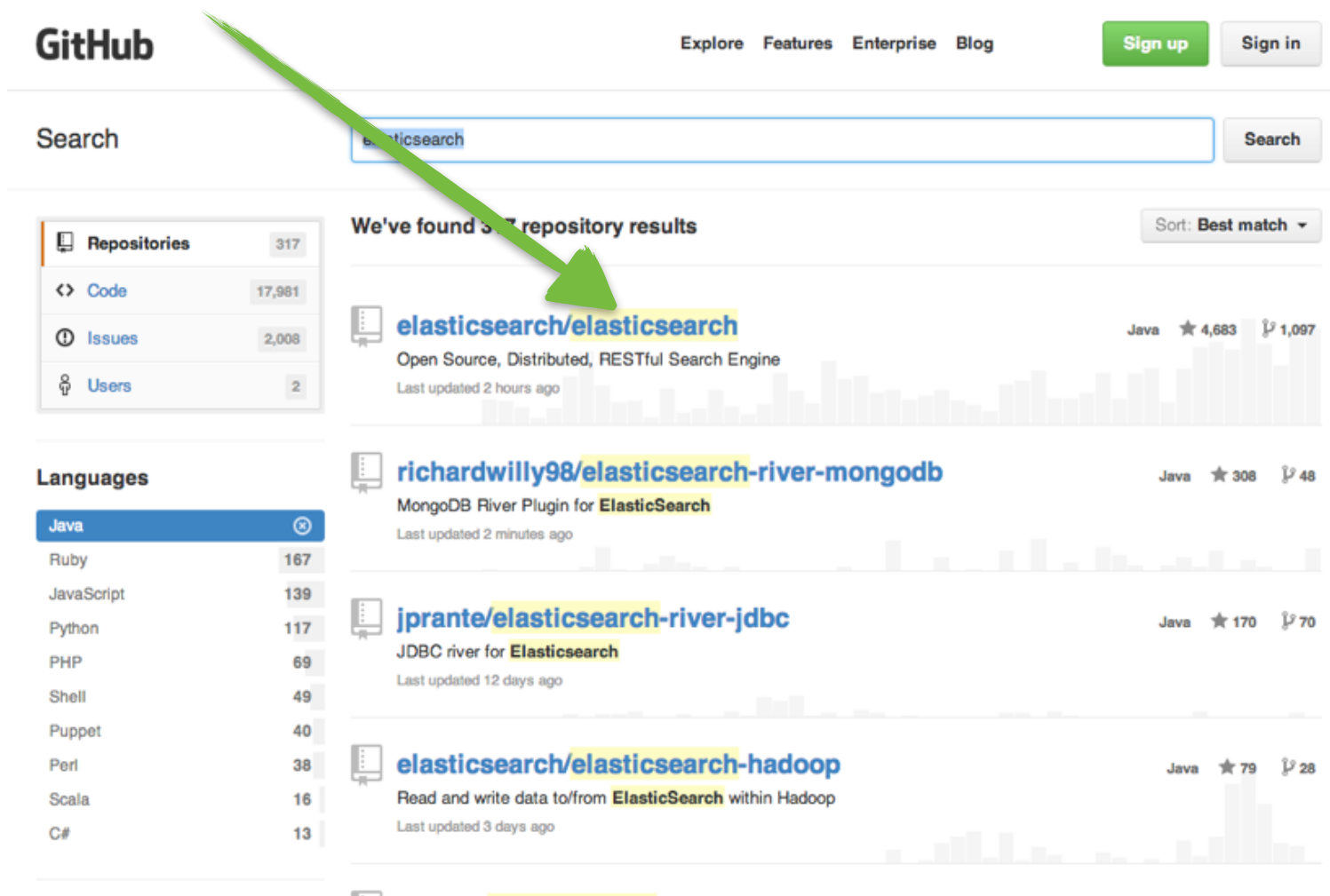
絞り込み



The screenshot shows the GitHub search interface. At the top left is the GitHub logo. To its right are links for 'Explore', 'Features', 'Enterprise', and 'Blog', along with 'Sign up' and 'Sign in' buttons. Below the logo is a search bar containing 'elasticsearch' and a 'Search' button. A green arrow points from the search bar down to the 'Languages' filter section on the left. The search results are titled 'We've found 317 repository results' and are sorted by 'Best match'. The results list several repositories related to Elasticsearch, including the main 'elasticsearch/elasticsearch' repository and various plugins like 'river-mongodb' and 'river-jdbc'. Each result shows the repository name, description, language (Java), star count, and fork count.

Repository	Description	Language	Stars	Forks
elasticsearch/elasticsearch	Open Source, Distributed, RESTful Search Engine	Java	4,683	1,097
richardwilly98/elasticsearch-river-mongodb	MongoDB River Plugin for ElasticSearch	Java	308	48
jprante/elasticsearch-river-jdbc	JDBC river for Elasticsearch	Java	170	70
elasticsearch/elasticsearch-hadoop	Read and write data to/from ElasticSearch within Hadoop	Java	79	28

ハイライト



The screenshot shows the GitHub search interface. At the top left is the GitHub logo. To its right are links for 'Explore', 'Features', 'Enterprise', and 'Blog'. Further right are 'Sign up' and 'Sign in' buttons. Below the logo is a search bar containing the text 'elasticsearch' and a 'Search' button. A green arrow points from the search bar down to the first search result.

Search **Search**

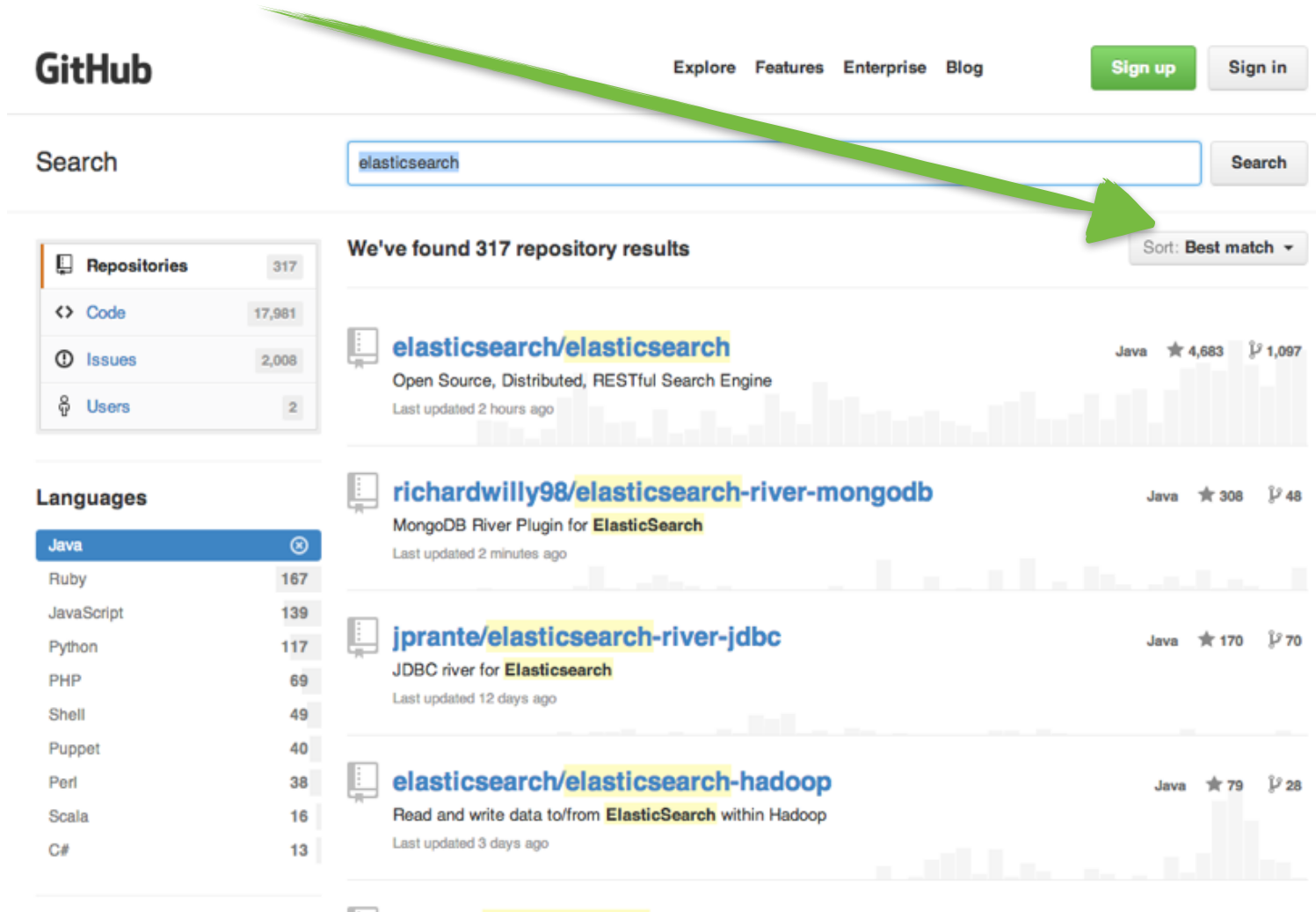
Repositories 317
Code 17,981
Issues 2,008
Users 2

Languages
Java 167
Ruby 139
JavaScript 139
Python 117
PHP 69
Shell 49
Puppet 40
Perl 38
Scala 16
C# 13

We've found 37 repository results Sort: **Best match**

- elasticsearch/elasticsearch** Java ★ 4,683 📄 1,097
Open Source, Distributed, RESTful Search Engine
Last updated 2 hours ago
- richardwilly98/elasticsearch-river-mongodb** Java ★ 308 📄 48
MongoDB River Plugin for **ElasticSearch**
Last updated 2 minutes ago
- jprante/elasticsearch-river-jdbc** Java ★ 170 📄 70
JDBC river for **Elasticsearch**
Last updated 12 days ago
- elasticsearch/elasticsearch-hadoop** Java ★ 79 📄 28
Read and write data to/from **ElasticSearch** within Hadoop
Last updated 3 days ago

ソート



The screenshot shows the GitHub search interface. At the top left is the GitHub logo. To its right are navigation links: "Explore", "Features", "Enterprise", and "Blog". Further right are "Sign up" and "Sign in" buttons. Below the navigation is a search bar containing the text "elasticsearch" and a "Search" button. A large green arrow points from the search bar area down to a dropdown menu that says "Sort: Best match".

Below the search bar, the page displays "We've found 317 repository results". On the left side, there is a sidebar with navigation options: "Repositories" (317), "Code" (17,981), "Issues" (2,008), and "Users" (2). Below this is a "Languages" section with a list of programming languages and their repository counts: Java (167), Ruby (139), JavaScript (117), Python (69), PHP (49), Shell (40), Puppet (38), Perl (16), Scala (13), and C# (13).

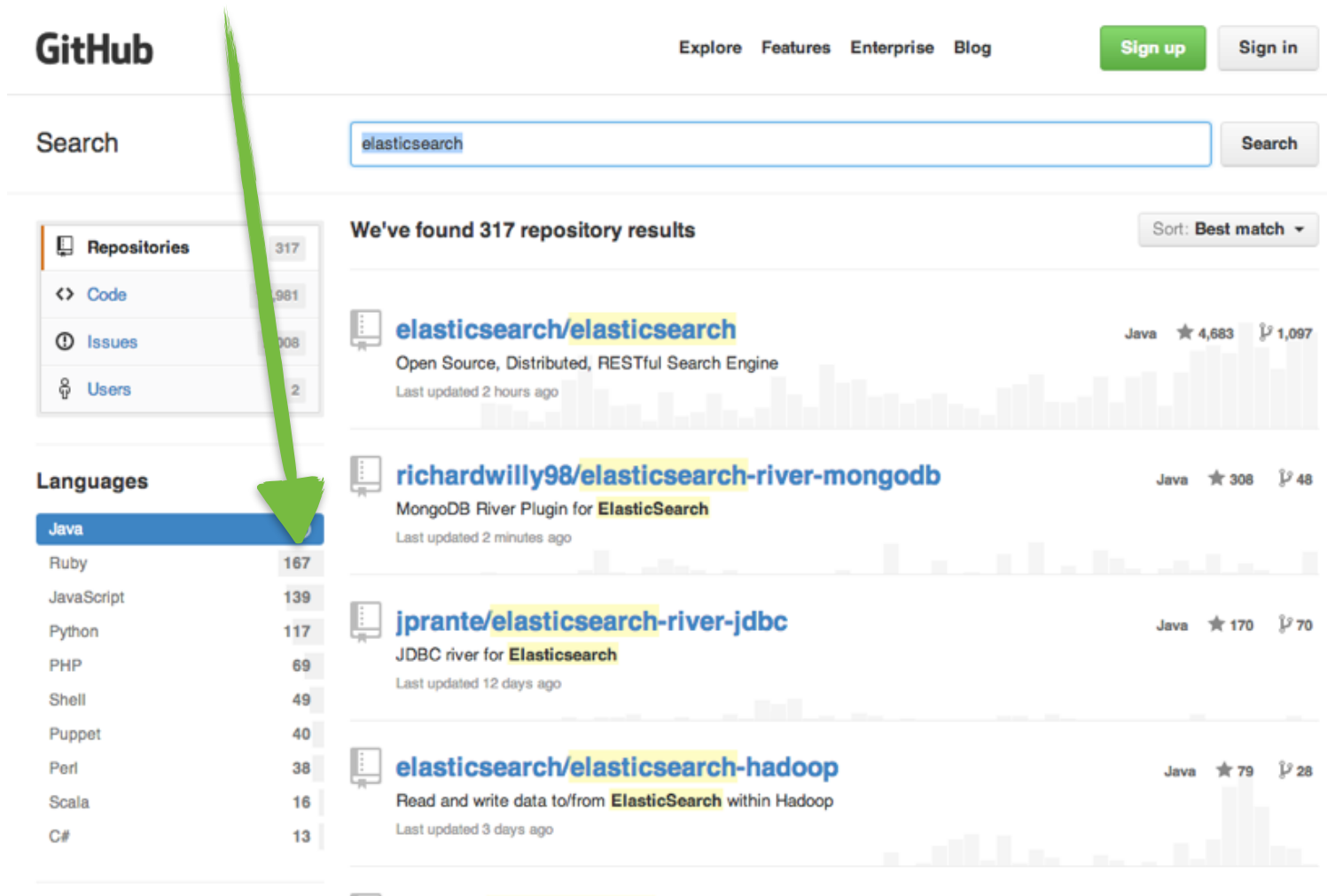
The main content area shows a list of repository results, each with a repository icon, the repository name, a description, the last update time, and a bar chart showing activity over time. The results are:

- elasticsearch/elasticsearch**: Open Source, Distributed, RESTful Search Engine. Last updated 2 hours ago. Java, 4,683 stars, 1,097 forks.
- richardwilly98/elasticsearch-river-mongodb**: MongoDB River Plugin for ElasticSearch. Last updated 2 minutes ago. Java, 308 stars, 48 forks.
- jprante/elasticsearch-river-jdbc**: JDBC river for Elasticsearch. Last updated 12 days ago. Java, 170 stars, 70 forks.
- elasticsearch/elasticsearch-hadoop**: Read and write data to/from ElasticSearch within Hadoop. Last updated 3 days ago. Java, 79 stars, 28 forks.

ペーシング

The screenshot shows the GitHub search interface. At the top, the GitHub logo is on the left, and navigation links for 'Explore', 'Features', 'Enterprise', and 'Blog' are on the right. There are 'Sign up' and 'Sign in' buttons. Below the navigation is a search bar containing the text 'elasticsearch' and a 'Search' button. The search results are displayed under the heading 'We've found 317 repository results'. On the left side, there is a sidebar with filters for 'Repositories' (317), 'Code' (17,981), 'Issues' (2,008), and 'Users' (2). Below this is a 'Languages' section with a list of programming languages and their respective repository counts: Java (317), Ruby (167), JavaScript (139), Python (117), PHP (69), Shell (49), Puppet (40), Perl (38), Scala (16), and C# (13). The main content area shows a list of repository results. The first result is 'elasticsearch/elasticsearch', described as 'Open Source, Distributed, RESTful Search Engine', with 4,683 stars and 1,097 forks. The second result is 'richardwilly98/elasticsearch-river-mongodb', described as 'MongoDB River Plugin for ElasticSearch', with 308 stars and 48 forks. The third result is 'jprante/elasticsearch-river-jdbc', described as 'JDBC River for Elasticsearch', with 170 stars and 70 forks. The fourth result is 'elasticsearch/elasticsearch-hadoop', described as 'Read and write to/from ElasticSearch within Hadoop', with 79 stars and 28 forks. A green arrow points from the top left towards the 'elasticsearch/elasticsearch-hadoop' repository entry.

集計



The screenshot shows the GitHub search interface. At the top left is the GitHub logo. To its right are links for 'Explore', 'Features', 'Enterprise', and 'Blog'. Further right are 'Sign up' and 'Sign in' buttons. Below the logo is a search bar containing 'elasticsearch' and a 'Search' button. On the left side, there is a sidebar with navigation options: 'Repositories' (317), 'Code' (981), 'Issues' (1008), and 'Users' (2). Below this is a 'Languages' section with a list of programming languages and their repository counts: Java (167), Ruby (167), JavaScript (139), Python (117), PHP (69), Shell (49), Puppet (40), Perl (38), Scala (16), and C# (13). A green arrow points from the top of the sidebar down to the 'Java' language filter, which is highlighted in blue. The main content area shows search results for 'elasticsearch'. It starts with 'We've found 317 repository results' and a 'Sort: Best match' dropdown. The first result is 'elasticsearch/elasticsearch', described as 'Open Source, Distributed, RESTful Search Engine', with 4,683 stars and 1,097 forks. The second result is 'richardwilly98/elasticsearch-river-mongodb', described as 'MongoDB River Plugin for ElasticSearch', with 308 stars and 48 forks. The third result is 'jprante/elasticsearch-river-jdbc', described as 'JDBC river for Elasticsearch', with 170 stars and 70 forks. The fourth result is 'elasticsearch/elasticsearch-hadoop', described as 'Read and write data to/from ElasticSearch within Hadoop', with 79 stars and 28 forks. Each result includes a small bar chart showing activity over time.

サジェスト

The screenshot shows the GitHub interface for the repository `elasticsearch/elasticsearch`. The search bar contains the text `repository debian`. A dropdown menu displays the following search results:

- `elasticsearch/elasticsearch#1726` **debian** package violates naming convention
- `elasticsearch/elasticsearch#3571` **debian** package init-script: start-stop-daemon ne
- `elasticsearch/elasticsearch#1681` **Debian** pkg
- `elasticsearch/elasticsearch#3286` There is no official **debian**/ubuntu repository
- `elasticsearch/elasticsearch#3500` Elasticsearch should include **debian**'s standard j
- `elasticsearch/elasticsearch#1526` Moving **debian** package to maven

Below the search results, there are search suggestions:

- Search elasticsearch/elasticsearch for 'debian'
- Search GitHub for 'debian'

The main content area shows a list of issues:

- NoShardAvailableActionException in ES 0.90.3 on startup** #3700
- Feature Request: Don't reindex the document when updating non-indexed fields** #3696

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,
```

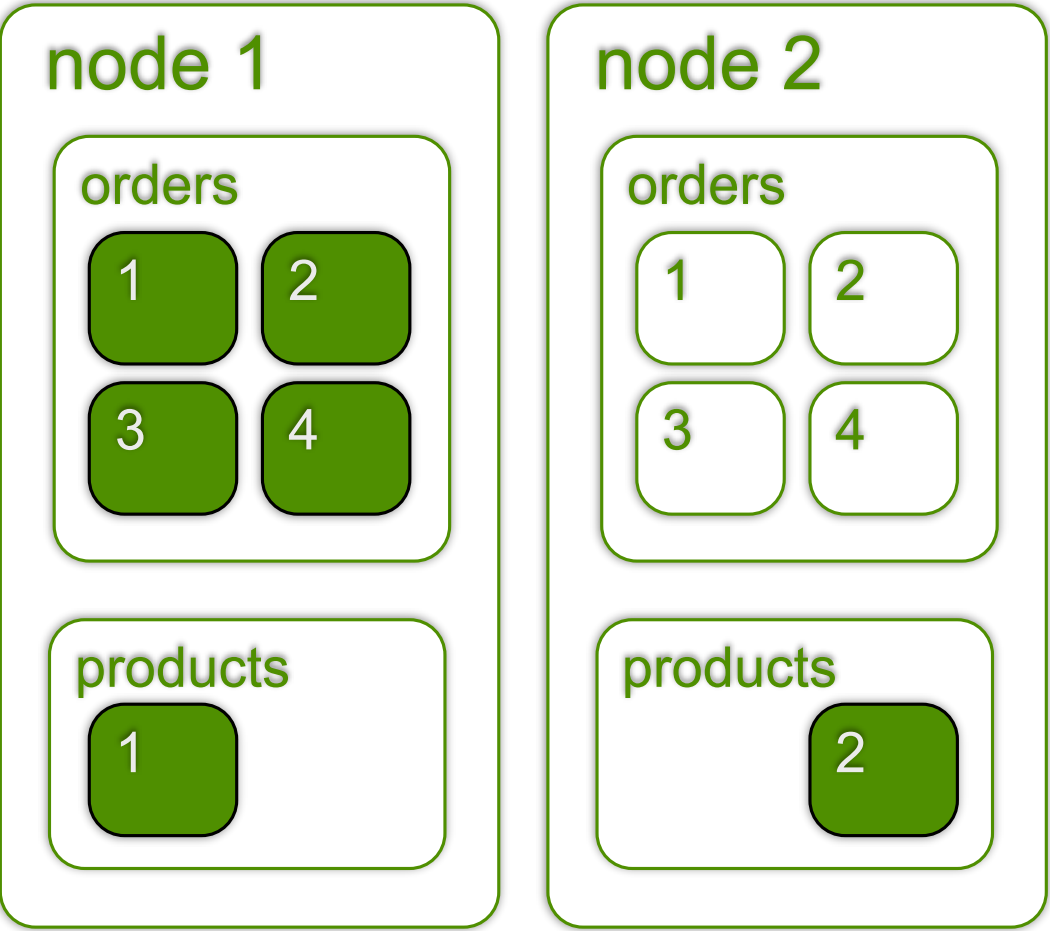
```
          "balance" : 28770,
          "firstname" : "Michael",
          "lastname" : "Bray",
          "age" : 31,
          "gender" : "M",
          "address" : "935 Lake Place",
          "employer" : "Telepark",
          "email" : "michaelbray@telepark.com",
          "city" : "Lemoyne",
          "state" : "CT"
        }
      ],
    }
  },
```

分散構成、 スケール

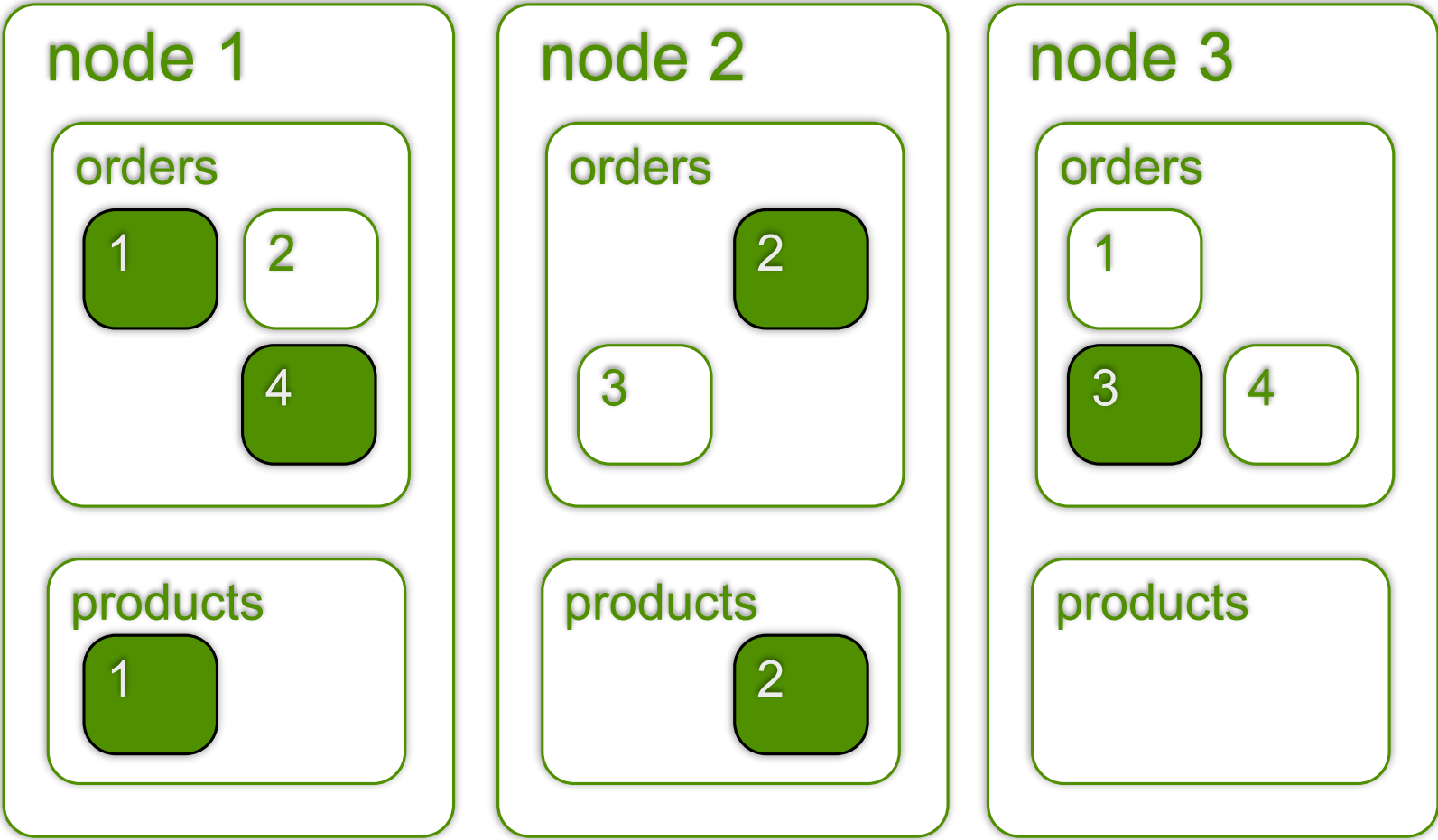
自動的な分散



自動的な分散



自動的な分散



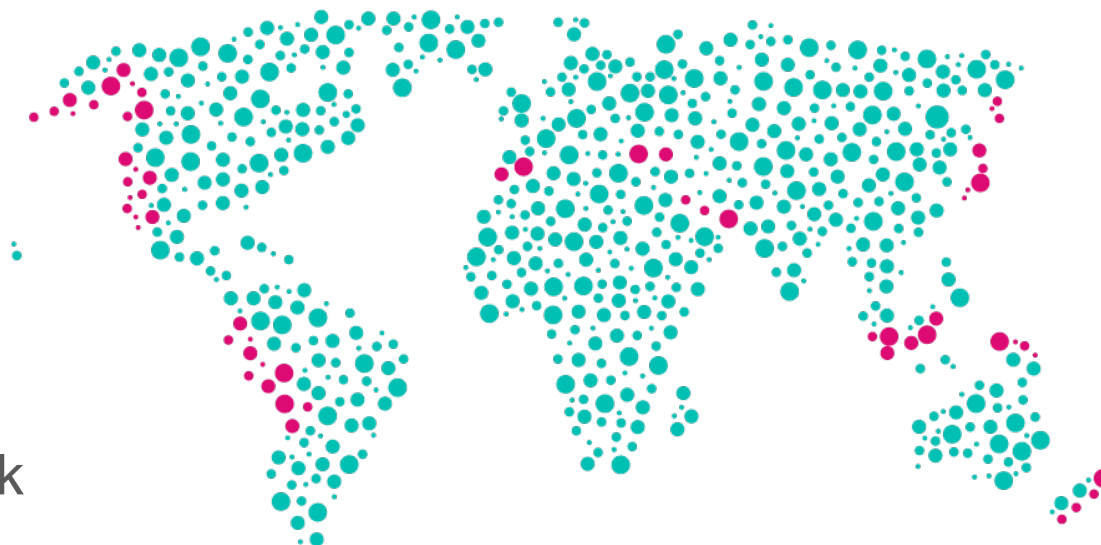


kibana



Kibana

Window into the Elastic Stack



可視化と分析

グラフ探索

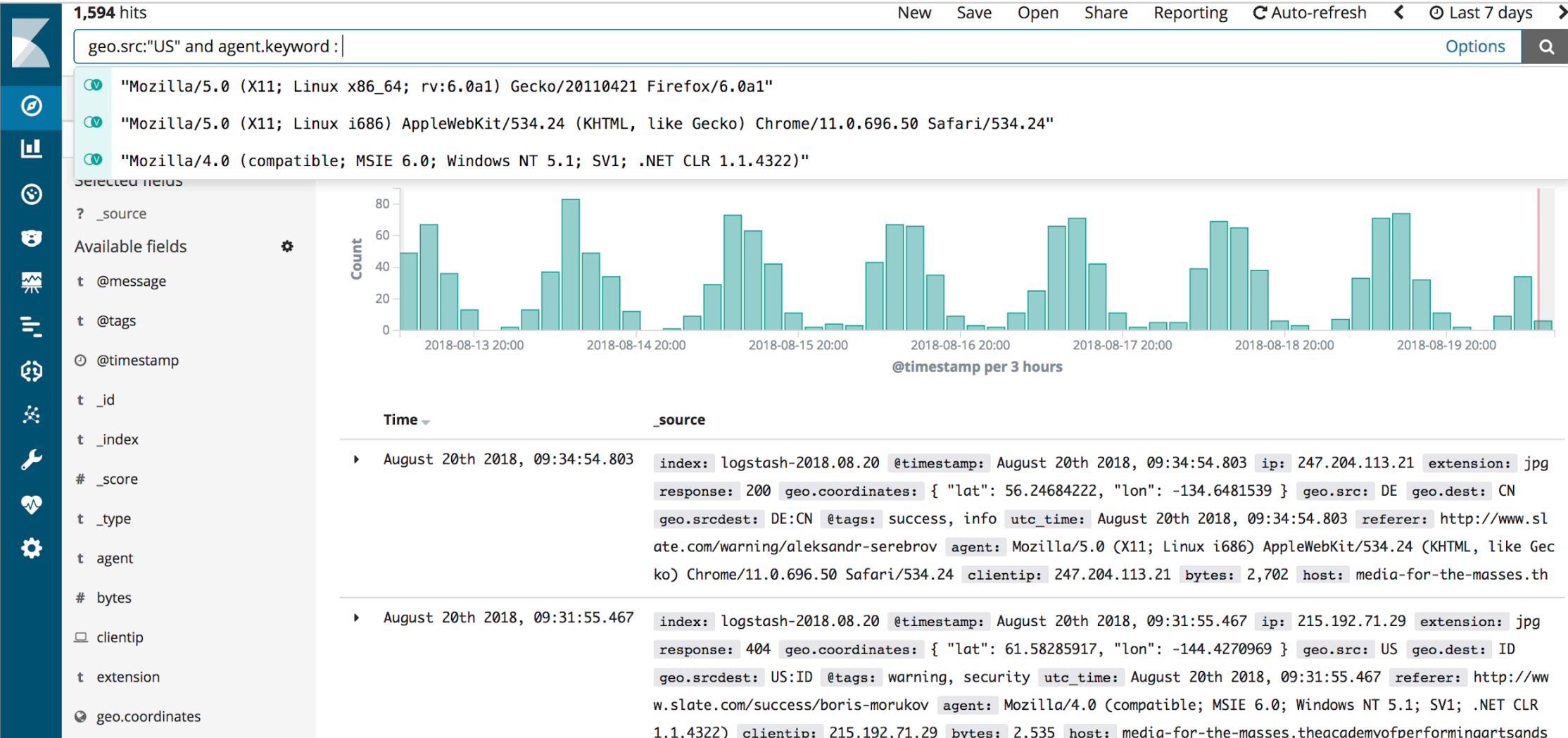
地理空間

Elastic Stackへの
セキュアなアクセスと管理

カスタマイズと
レポートの共有

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

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

Management / Index patterns / Create index pattern

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Step 1 of 2: Define index pattern

Index pattern

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

Your index pattern can match any of your **18 indices**, below.

accounts
apm-7.4.0-error-000001
apm-7.4.0-error-000002
apm-7.4.0-error-000003
apm-7.4.0-metric-000001
apm-7.4.0-onboarding-2019.10.03
apm-7.4.0-span-000001
apm-7.4.0-span-000002
apm-7.4.0-span-000003
apm-7.4.0-span-000004

Rows per page: 10 ▾

Index Pattern

- 日時のフィールドを指定

The screenshot shows the Kibana interface for creating an index pattern. The breadcrumb navigation at the top reads 'Management / Index patterns / Create index pattern'. The left sidebar contains a navigation menu with categories: Elasticsearch (Index Management, Index Lifecycle Policies, Rollup Jobs, Watcher, Snapshot and Restore, 8.0 Upgrade Assistant), Kibana (Index Patterns, Saved Objects, Spaces, Reporting, Advanced Settings), Logstash (Pipelines), Beats (Central Management), Machine Learning (Jobs list), and Security (Users, Roles). The main content area is titled 'Create index pattern' and includes the text: 'Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.' Below this, it indicates 'Step 2 of 2: Configure settings' and states: 'You've defined **apm-7*** as your index pattern. Now you can specify some settings before'. A dropdown menu for 'Time Filter field name Refresh' is set to '@timestamp'. A note explains: 'The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.' A link '> Show advanced options' is provided at the bottom.

Discover

- データの概観をつかむ

The screenshot shows the Elastic Discover interface. At the top, there's a search bar with the query 'metricbeat-*' and a 'Discover' button. Below the search bar, there are options for 'New', 'Save', 'Open', 'Share', and 'Inspect'. A 'Search' field is present with a 'KQL' button and a date range of 'Last 15 minutes'. A 'Refresh' button is on the right. On the left sidebar, there are various icons for navigation and a list of fields. The main area displays a bar chart titled '288 hits' for the time range 'Nov 7, 2019 @ 05:20:23.030 - Nov 7, 2019 @ 05:35:23.031'. The chart shows a peak in hits around 05:34:00. Below the chart, there's a table of search results with columns for 'Time' and '_source'. The results show details for three different events, including timestamps, process information, and system metrics.

Time	_source
> Nov 7, 2019 @ 05:35:21.164	@timestamp: Nov 7, 2019 @ 05:35:21.164 process.executable: /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/78.0.3904.70/Helpers/Google Chrome Helper (Renderer).app/Contents/MacOS/Google Chrome Helper (Renderer) process.args: /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome
> Nov 7, 2019 @ 05:35:21.164	@timestamp: Nov 7, 2019 @ 05:35:21.164 system.process.memory.size: 9GB system.process.memory.rss.bytes: 1.5GB system.process.memory.rss.pct: 4.53% system.process.memory.share: 0B system.process.cpu.total.value: 48,492 system.process.cpu.total.pct: 4.23% system.process.cpu.total.norm.pct: 0.26% system.process.cpu.start_time: Nov 7, 2019 @ 05:32:09.246
> Nov 7, 2019 @ 05:35:21.164	@timestamp: Nov 7, 2019 @ 05:35:21.164 system.process.state: running system.process.cpu.start_time: Nov 6, 2019 @ 02:36:42.289 system.process.cpu.total.norm.pct: 0.14% system.process.cpu.total.value: 558,534 system.process.cpu.total.pct: 2.23% system.process.memory.size: 7.7GB system.process.memory.rss.bytes: 558.2MB system.process.memory.rss.pct: 1.7%
> Nov 7, 2019 @ 05:35:21.164	@timestamp: Nov 7, 2019 @ 05:35:21.164 service.type: system system.process.state: running system.process.cpu.total.norm.pct: 0.11% system.process.cpu.total.value: 1,670 system.process.cpu.total.pct: 1.69% system.process.cpu.start_time: Nov 7, 2019 @ 05:34:01.013 system.process.memory.size: 4.3GB system.process.memory.rss.bytes: 95MB

Visualize

- グラフをつくる

Visualizations

[+ Create new visualization](#)

Search...

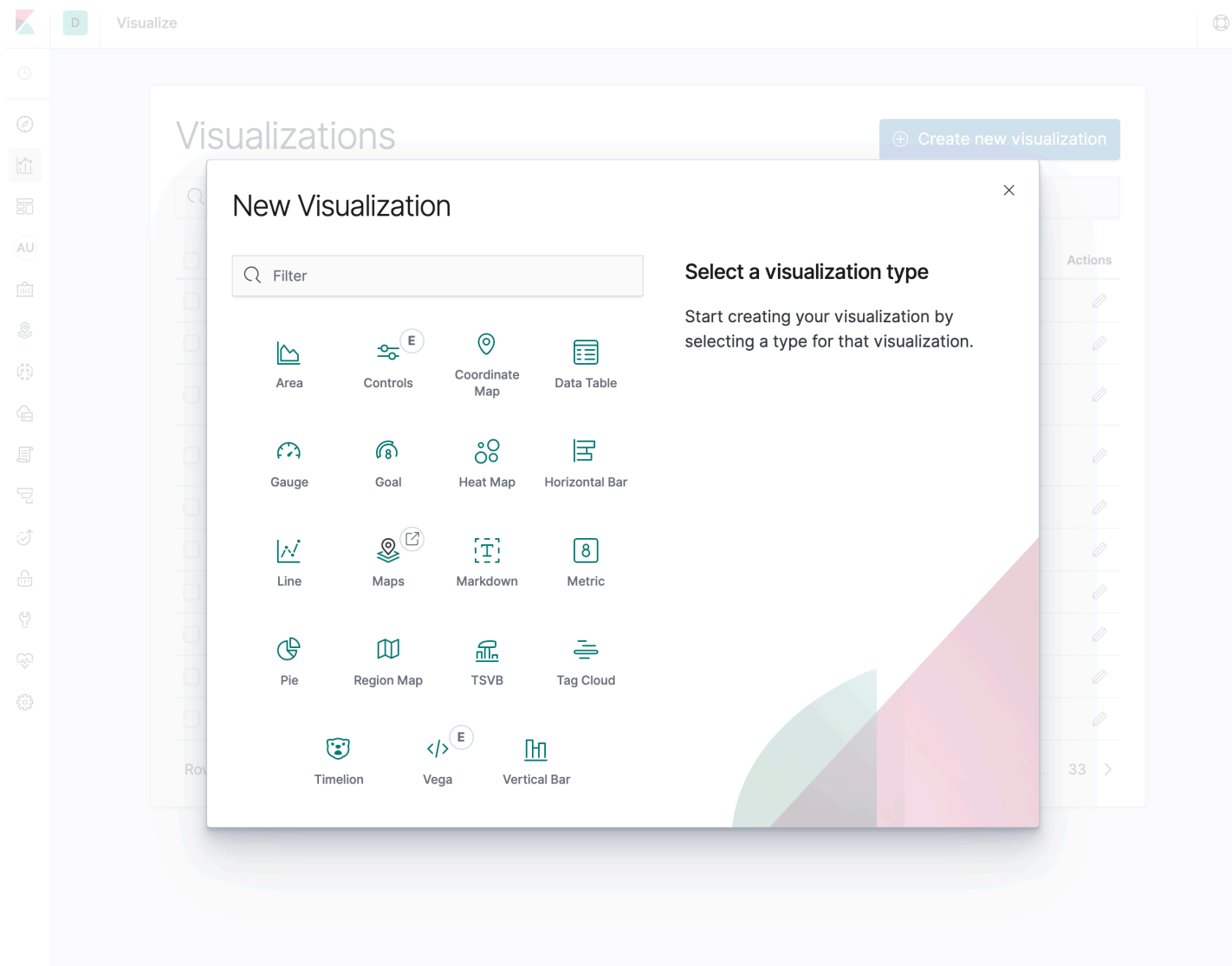
<input type="checkbox"/>	Title	Type	Actions
<input type="checkbox"/>	Cache Hits, Misses [Metricbeat CoreDNS] ECS	Line	
<input type="checkbox"/>	API Server Requests [Metricbeat Kubernetes] ECS	TSVB	
<input type="checkbox"/>	API Server Top clients by number of requests [Metricbeat Kubernetes] ECS	TSVB	
<input type="checkbox"/>	API Server Top clients by resource [Metricbeat Kubernetes] ECS	TSVB	
<input type="checkbox"/>	Accepts and Handled Rate [Metricbeat Nginx] ECS	TSVB	
<input type="checkbox"/>	Active connections [Metricbeat Nginx] ECS	TSVB	
<input type="checkbox"/>	Active servers in backend [Metricbeat HAProxy] ECS	TSVB	
<input type="checkbox"/>	Active size of transaction log [Metricbeat MSSQL] ECS	TSVB	
<input type="checkbox"/>	Alert Notifications [Metricbeat Prometheus]	TSVB	
<input type="checkbox"/>	Alive Connections [Metricbeat Zookeeper] ECS	TSVB	

Rows per page: 10

< 1 2 3 4 5 ... 33 >

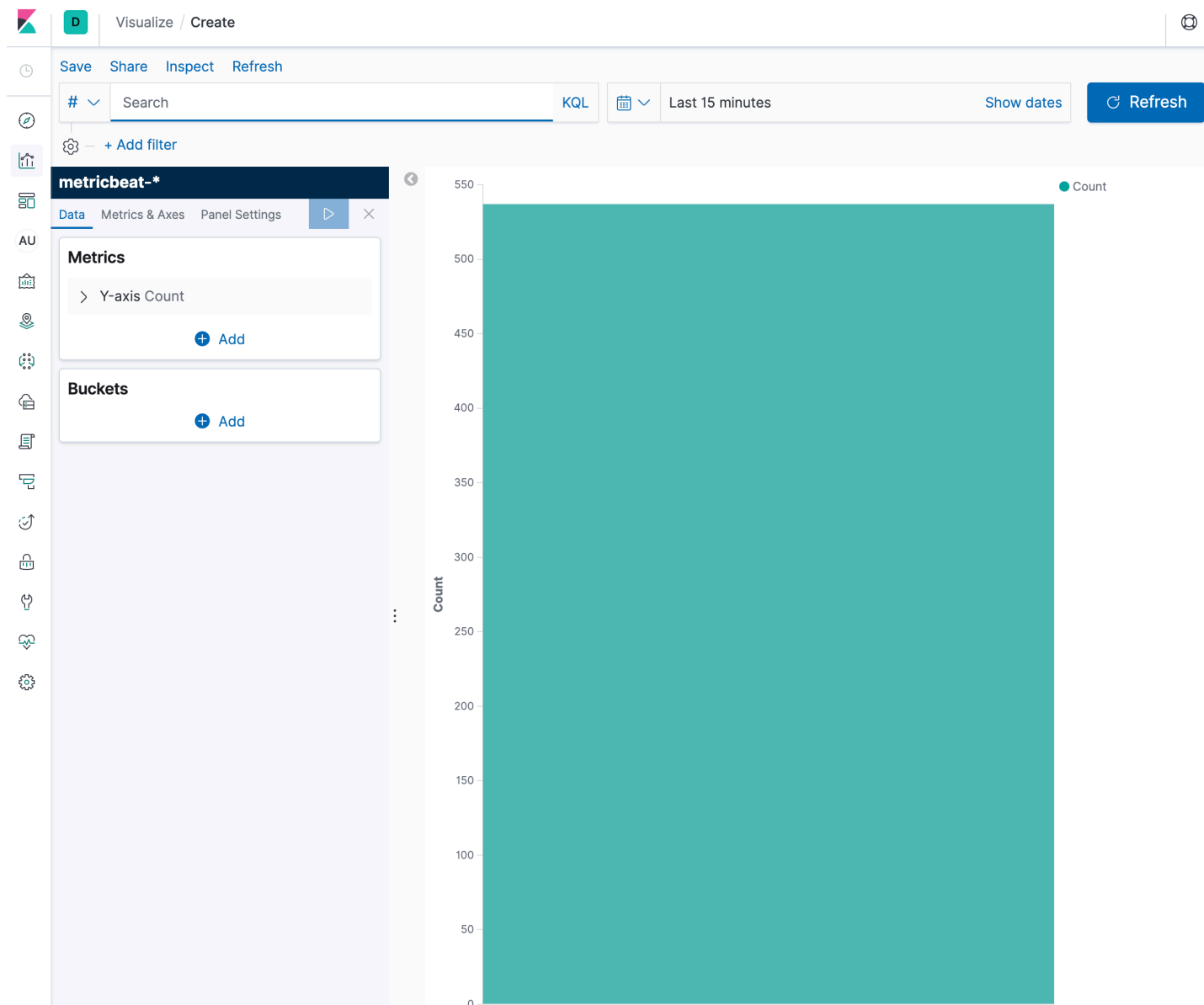
Visualize

- グラフをつくる
- 様々な種類のグラフ



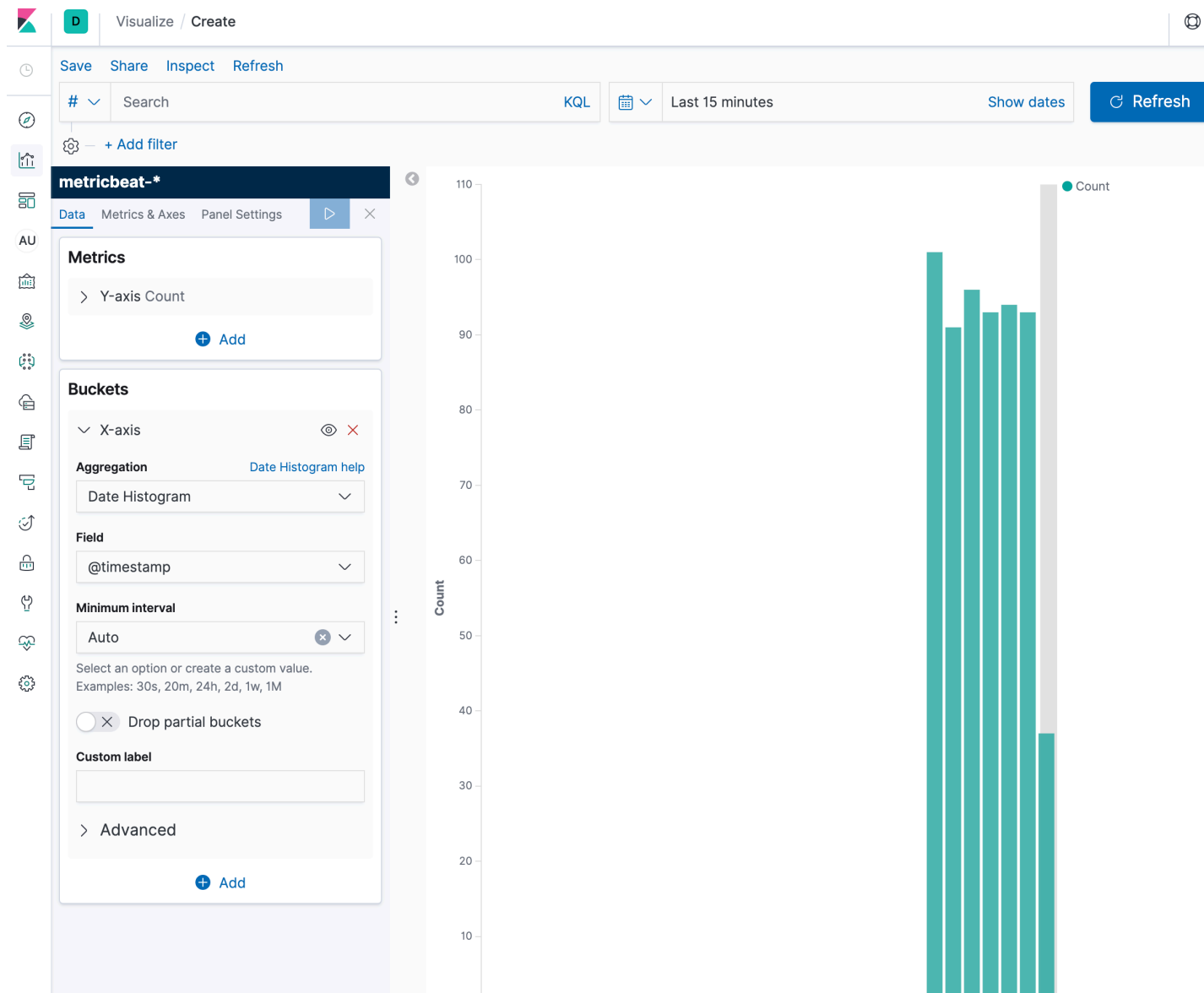
Visualize

- グラフをつくる
- 様々な種類のグラフ



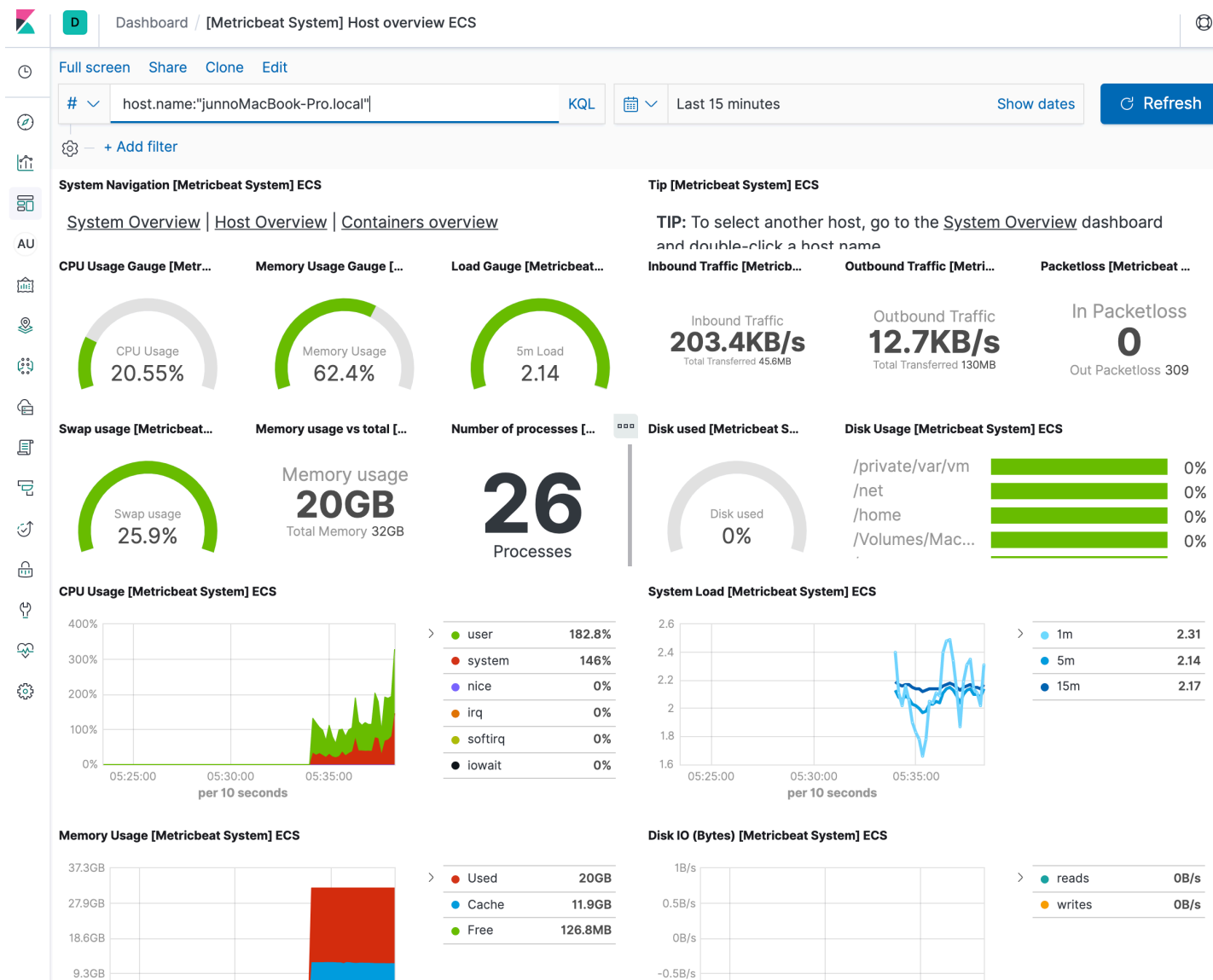
Visualize

- 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

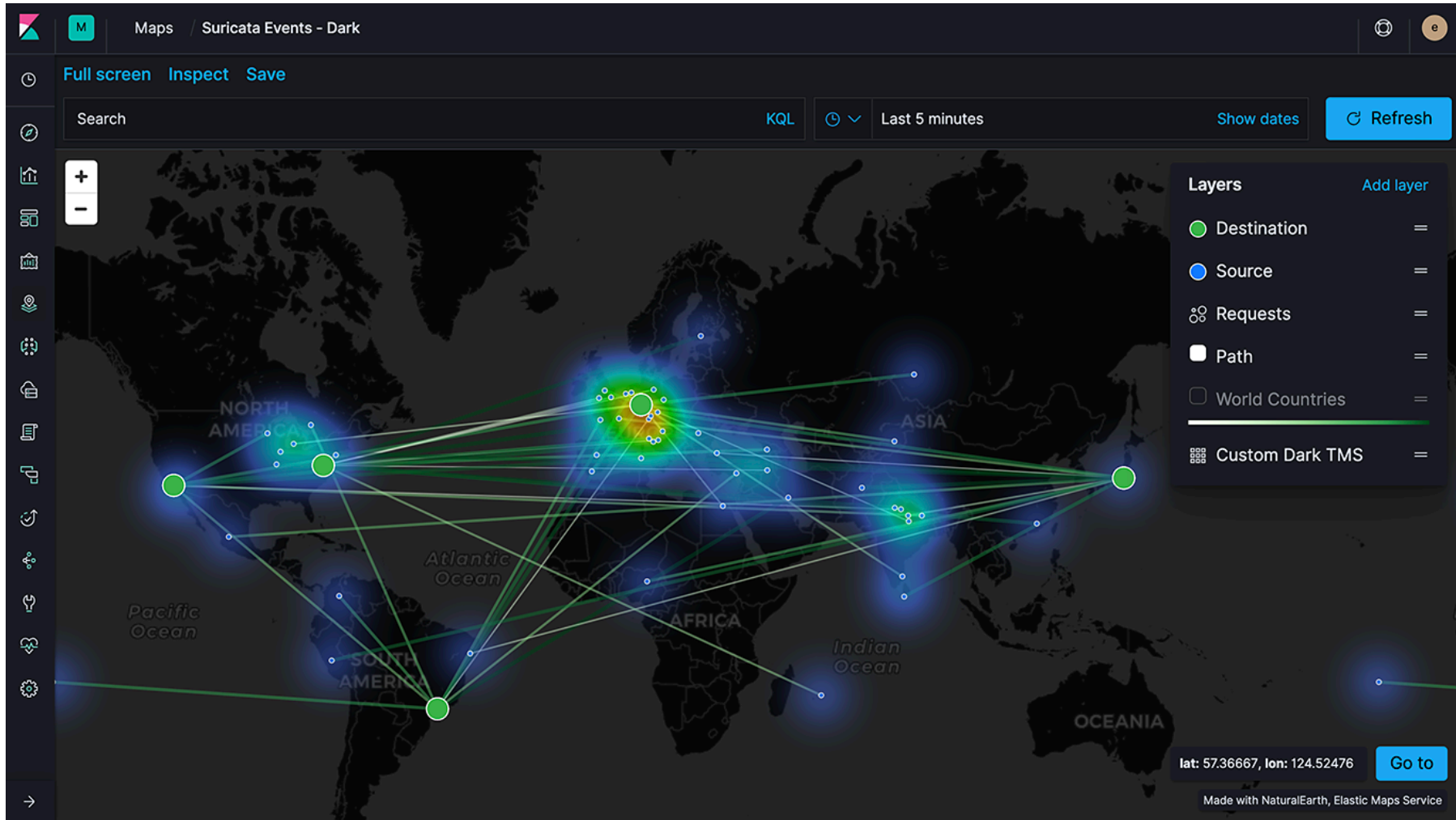
GA | Basic (free)

The dashboard displays the following information:

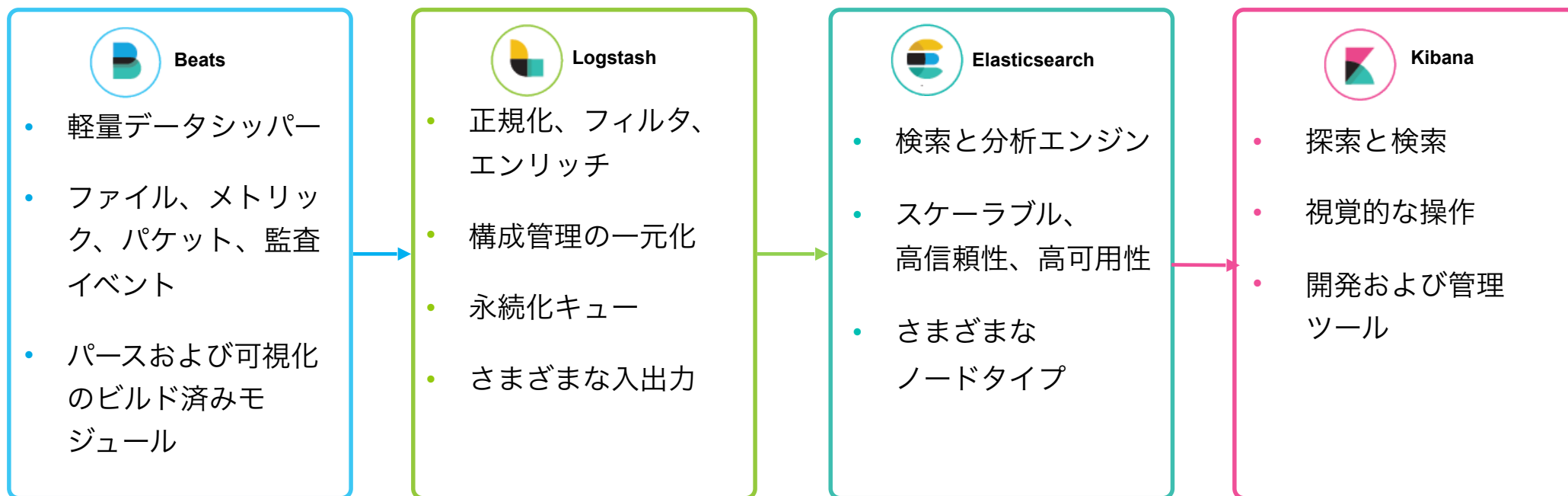
- Status Indicators:** Four items at the top with status icons: artifacts.elastic.co (red X), www.elastic.co (green check), cdn.elastic-elastic-elastic.org (green check), and elastic-elastic-elastic.org (green check).
- HTTP Status Summary:** A vertical list on the left shows counts for 5XX (7), 4XX (1), 3XX (0), and 2XX (221).
- MACHINE:** OS: ios, RAM: 10.0GB.
- REQUEST:** /styles/semantic-ui.css.
- GEO:** ORIGIN COUNTRY: PH, DESTINATION: IN.
- TOTAL ISSUES:** 27, accompanied by a flame icon and a bar chart.
- BYTES TRANSFERRED:** 1.28MB, accompanied by a donut chart and a line graph.
- TOTAL VISITORS:** 229, accompanied by a donut chart and a line graph.

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

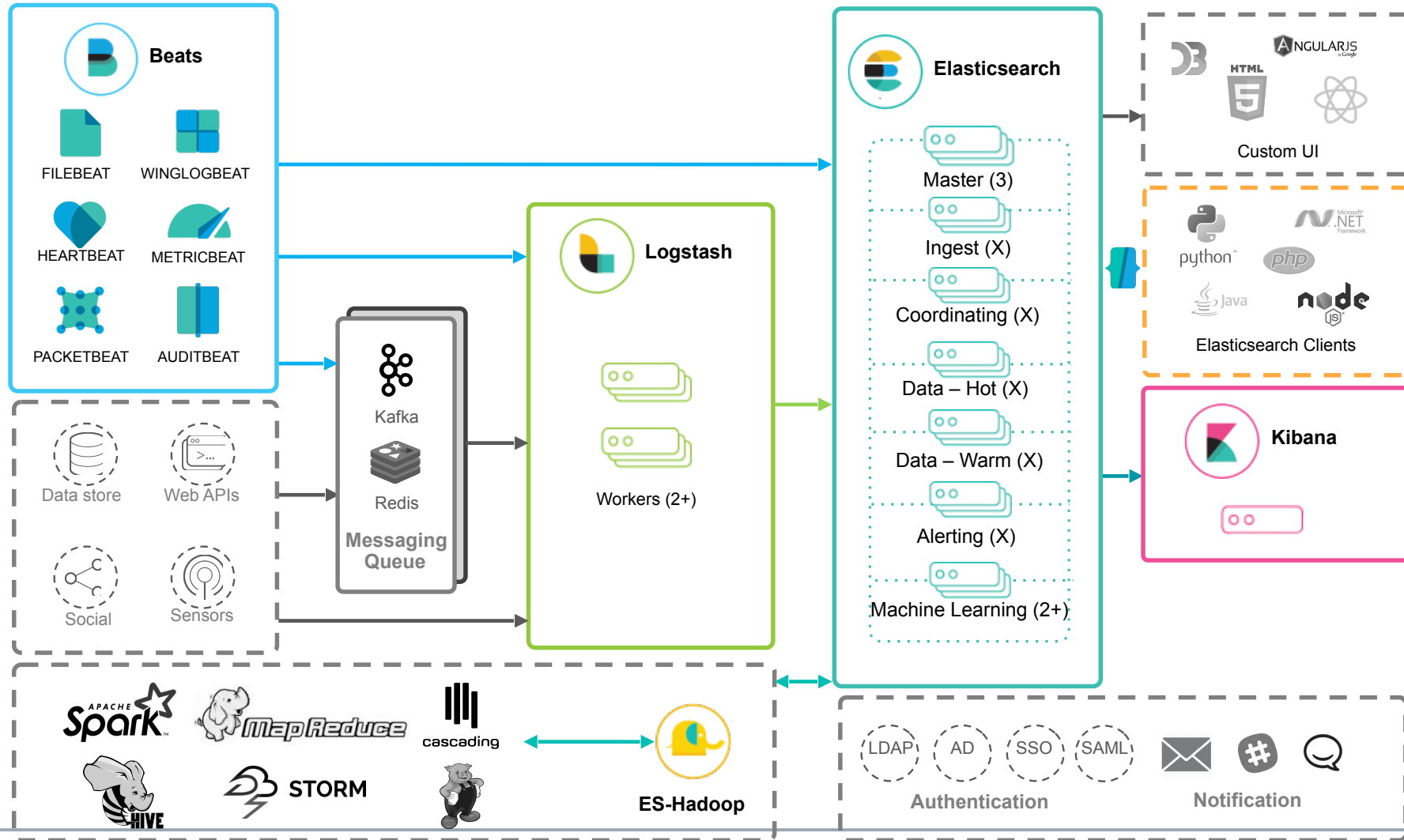
GA | Basic (free)



論理的な処理のパイプライン



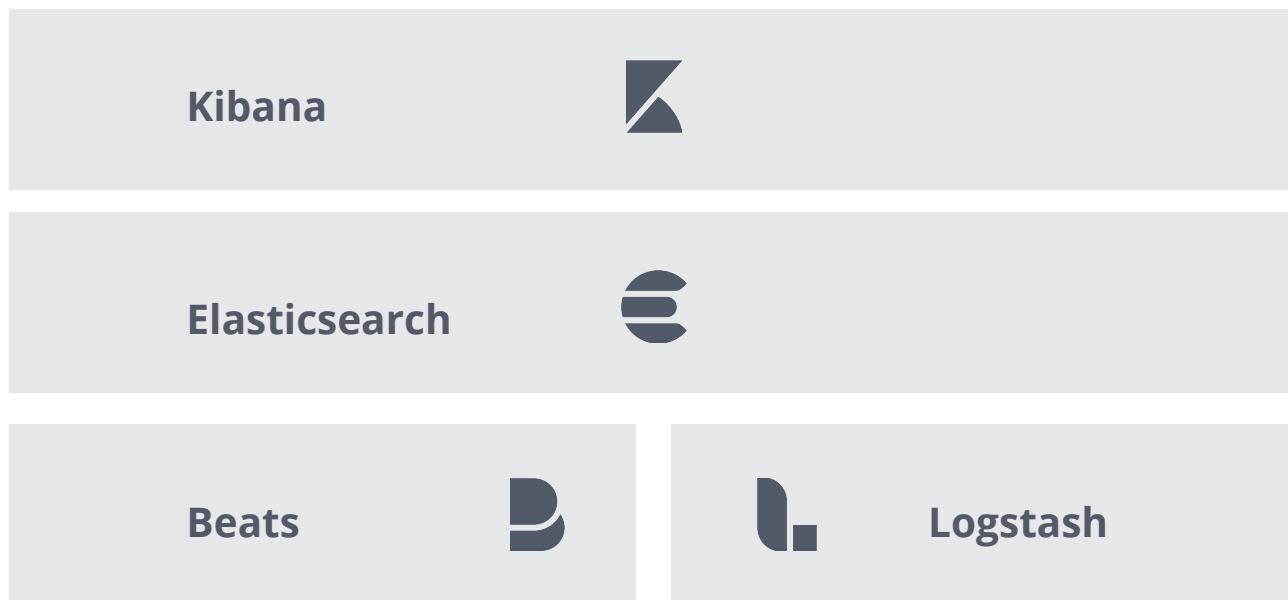
ログやメトリックのためのElastic Stackの構成



デプロイの選択肢

ソリューション


Elastic Stack



可視化 & 管理

保管、検索、分析

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.

The screenshot shows the 'Create deployment' interface for the Elasticsearch Service. The left sidebar contains navigation links: Deployments, Custom plugins, Account, and Help. The main content area is titled 'Create deployment' and includes a descriptive paragraph: 'Take the template that pre-configures the Elastic Stack and make it yours. Adjust capacity and performance, change the level of fault tolerance, add more features, and much more. [Learn more ...](#)'

There are two configuration sections:

- Data 1 configuration:** Shows the instance type 'aws.data.highio.i3' with roles 'Master', 'Data', and 'Ingest'. It describes it as 'An I/O optimized Elasticsearch instance running on an AWS i3.' It includes a 'Fault tolerance' section with radio buttons for 1 zone, 2 zones (selected), and 3 zones. A 'RAM per Node' slider is set to 15 GB, with a 'Nodes' input field set to 1. Below the slider, it lists options: 1 GB, 2 GB, 4 GB, 8 GB, 15 GB, 29 GB, 58 GB. The 'RAM per Zone' is 15 GB. A summary shows: 15 GB RAM, 450 GB storage, 1 node, 2 zones = 30 GB RAM, 900 GB storage. A link for 'User setting overrides' is present.
- Machine Learning 1 configuration:** Shows the instance type 'aws.ml.m5' with the role 'Machine Learning'. It describes it as 'An Elasticsearch machine learning instance running on an AWS m5.' It includes a 'Fault tolerance' section with radio buttons for 1 zone (selected), 2 zones, and 3 zones. The 'RAM per Node' and 'Nodes' fields are partially visible.

On the right side, there is a 'Summary' table and an 'Architecture' diagram.

Name	Logging
Version	v6.4.2
ES data memory	30 GB
ES data storage	900 GB
Total memory	32 GB
Total storage	904 GB
Hourly rate	\$0.6939
Monthly rate	\$506.55

The 'Architecture' diagram shows two zones. Zone 1 contains three nodes: 'aws.data.... 15 GB RAM' (blue circle), 'aws.ml.m5 1 GB RAM' (grey circle), and 'aws.kiban... 1 GB RAM' (pink circle). Zone 2 contains one node: 'aws.data' (blue circle).

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.

The screenshot displays the 'Deployments' page in the Elastic Cloud Enterprise interface. It features a search bar with 'login|' and a 'More filters' dropdown. A 'Create deployment' button is visible in the top right. Below the search bar, it states 'Showing all 4 matching deployments'. Four deployment cards are shown, each with a green checkmark in the top right corner. Each card lists the deployment name, ID, and version, followed by a table of node configurations.

Deployment Name	ID	Version	Node Type	Configuration
logging heavy uc	26701e	v6.4.2	data.default	16 GB RAM, 2 nodes, 2 zones
			master	6 GB RAM, 3 nodes, 3 zones
			data.highstorage	16 GB RAM, 2 nodes, 2 zones
				Plus 2 more ...
logging-and-metrics	97b432	v5.6.11	data.default	1 GB RAM, 1 node, 1 zone
			Kibana	Included
logging-metrics-cluster-6	ff4dc0	v6.4.1	data.default	4 GB RAM, 1 node, 1 zone
			Kibana	Included
my-logging-cluster	92178c	v6.4.1	data.default	8 GB RAM, 2 nodes, 2 zones
			ml	8 GB RAM, 2 nodes, 2 zones
			master	24 GB RAM, 3 nodes, 3 zones
				Plus 2 more ...

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

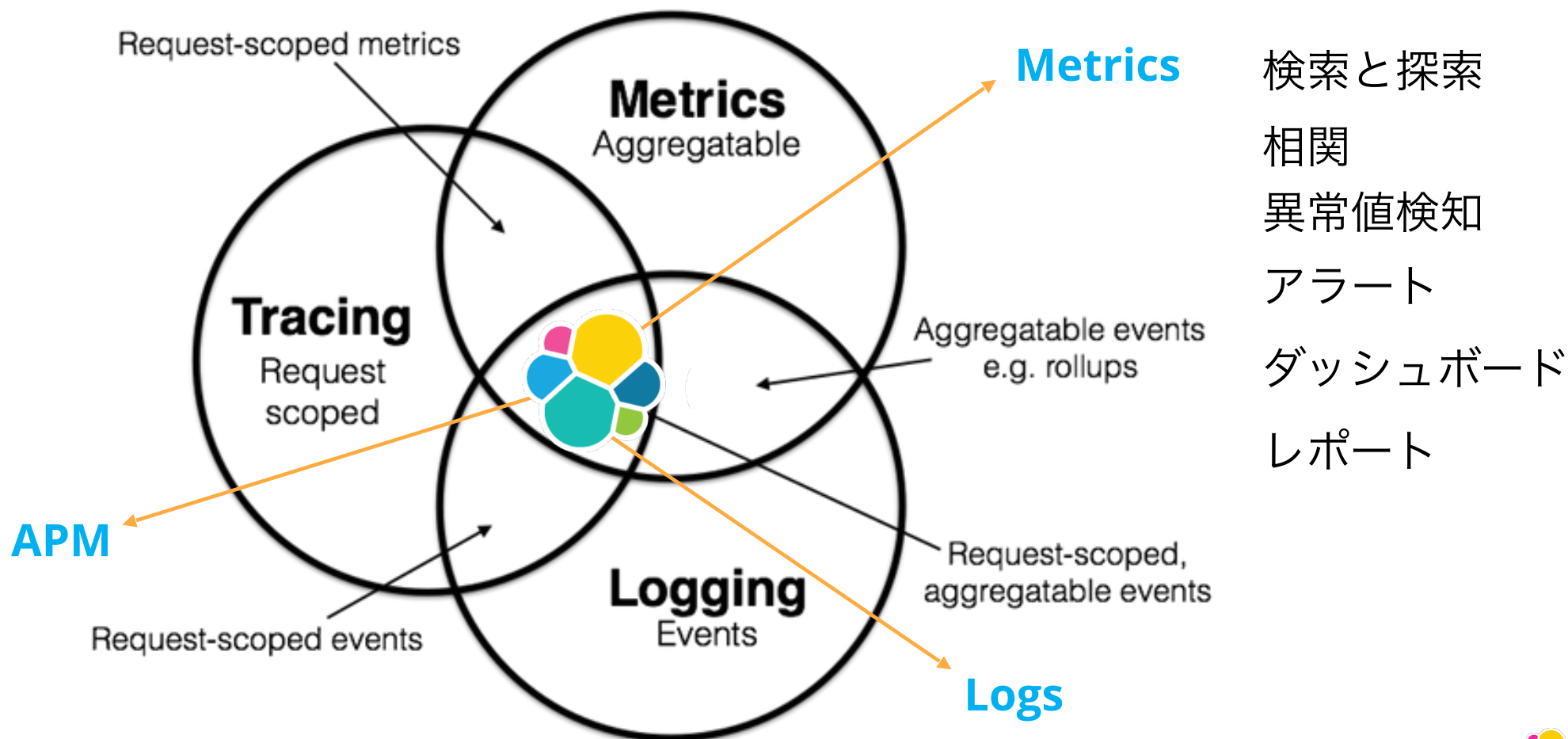
ElasticsearchとKibanaのoperatorを公式にサポート([ECK](#)):

1. 利用方法:

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

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



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かが重要か

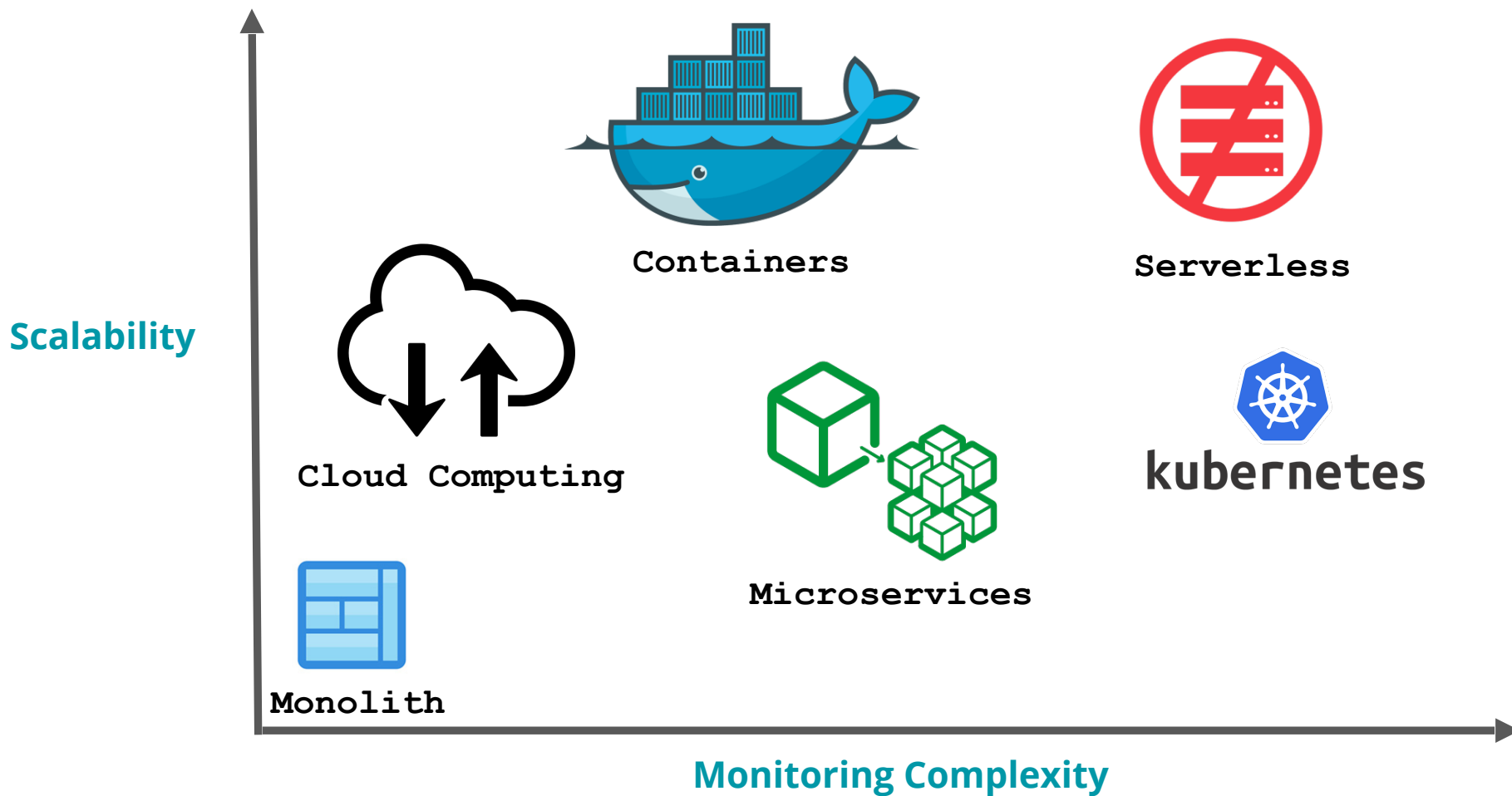
- エコシステムの健全性を示す相関的なデータに基づいた明確で意味のあるハイレベルなメトリックを測定
- リアルタイムな探索や重要なイベントをアラートするために異常値を自動で検知
- ハイレベルからディープダイブや、さまざまなデータをいつでも高速かつスケーラブルに関連付け、横断的な探索を可能にし、「何？」や「なぜ？」の答えるを効率よく探す

References:

Google SRE Handbook : <https://landing.google.com/sre/sre-book/toc/index.html>

Cindy Sridharan : <https://medium.com/@copyconstruct/monitoring-and-observability-8417d1952e1c>

アーキテクチャの進化に関する監視の観点



現状：サイロ化されたツール群

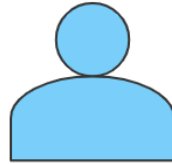
Development
Team



APM Tool

リアルユーザー監視
トランザクション性能監視
分散トレーシング

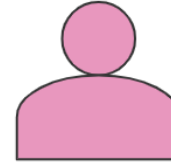
Ops: Monitoring
Team



Uptime Tool

死活監視
レスポンス時間

Ops: Monitoring
Team



Metrics Tool

コンテナメトリック
ホストメトリック
DBメトリック
ネットワークメトリック
ストレージメトリック

Ops: Logging
Team

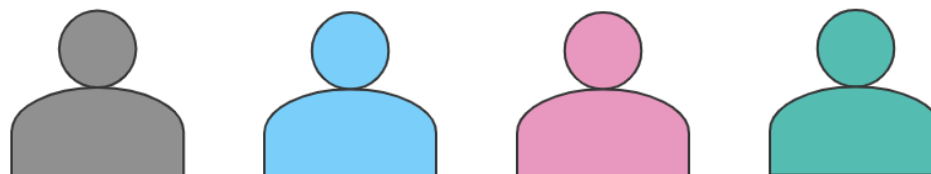


Logs Tool

ウェブログ
アプリログ
DBログ
コンテナログ

Elastic Stackを利用したオプザバビリティ

Dev & Ops Teams



APM Data

Uptime Data

Metrics Data

Log Data

リアルユーザー監視
トランザクション性能監視
分散トレーシング

死活監視
レスポンス時間

コンテナ/ホストメトリック
ネットワークメトリック
DB/ストレージメトリック

ウェブログ
アプリ/DB/コンテナログ
PaaSログ

Kibana

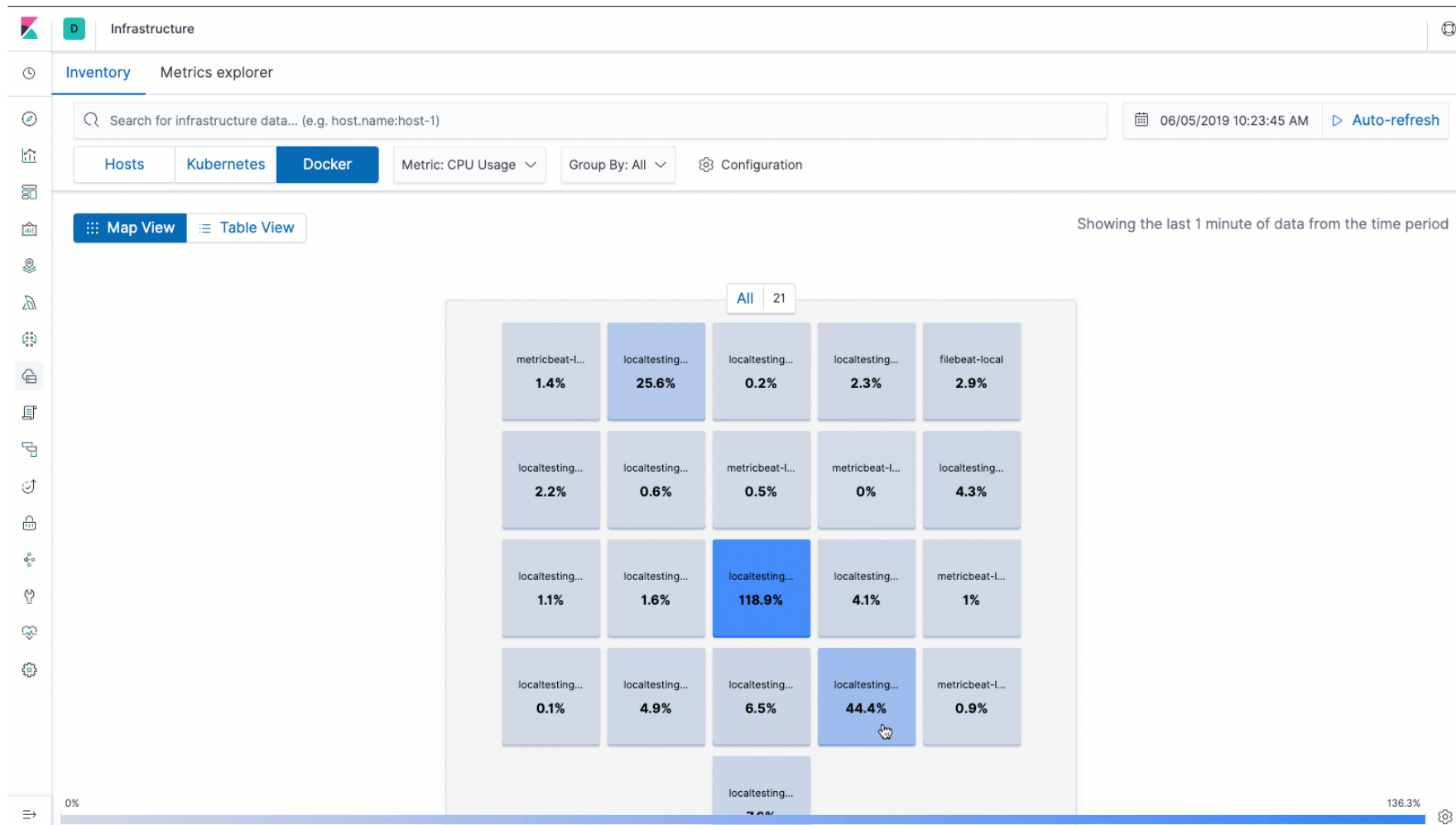


Elasticsearch



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

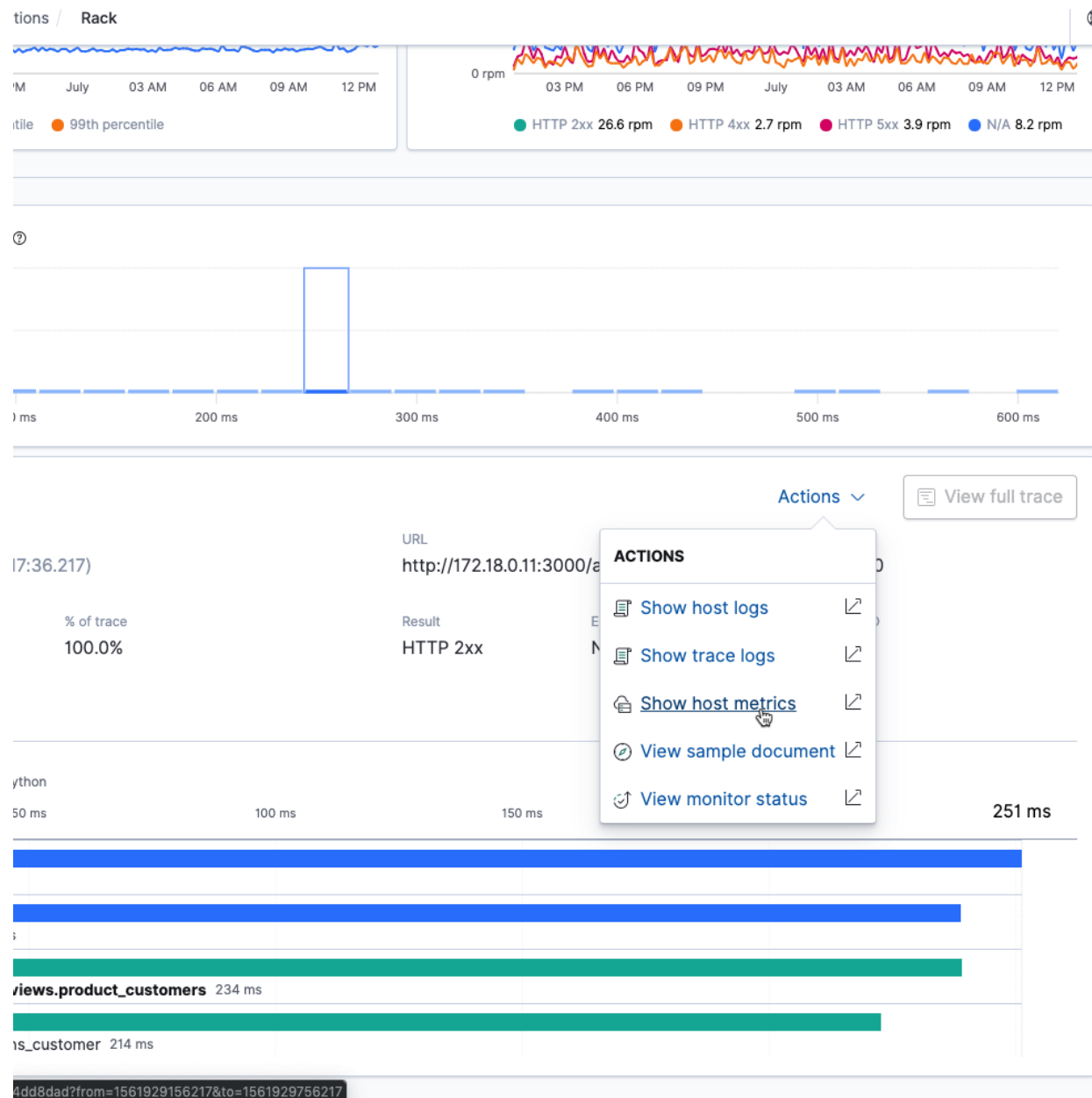


統一されたObservability

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

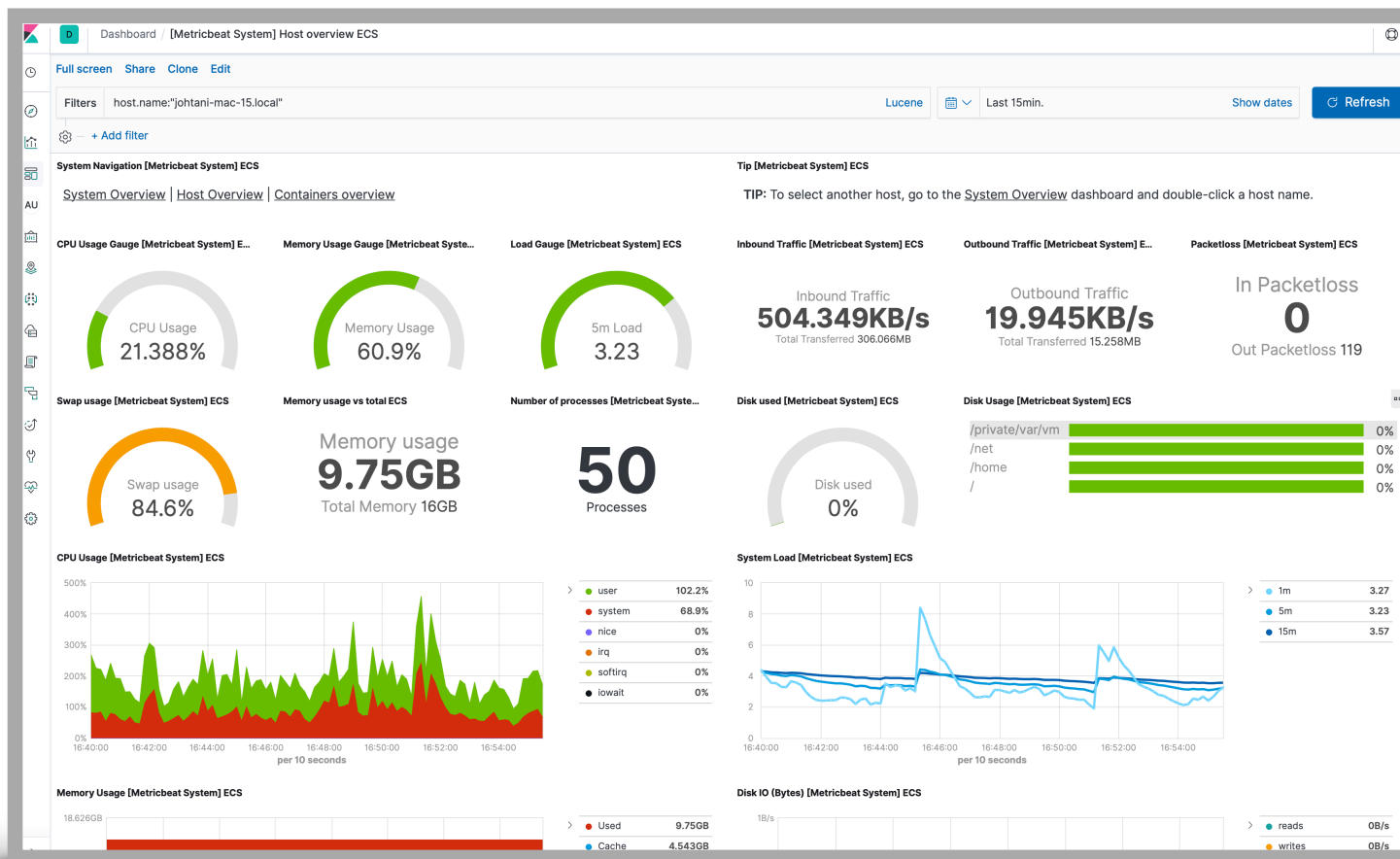
Kibanaひとつですべてをカバー

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

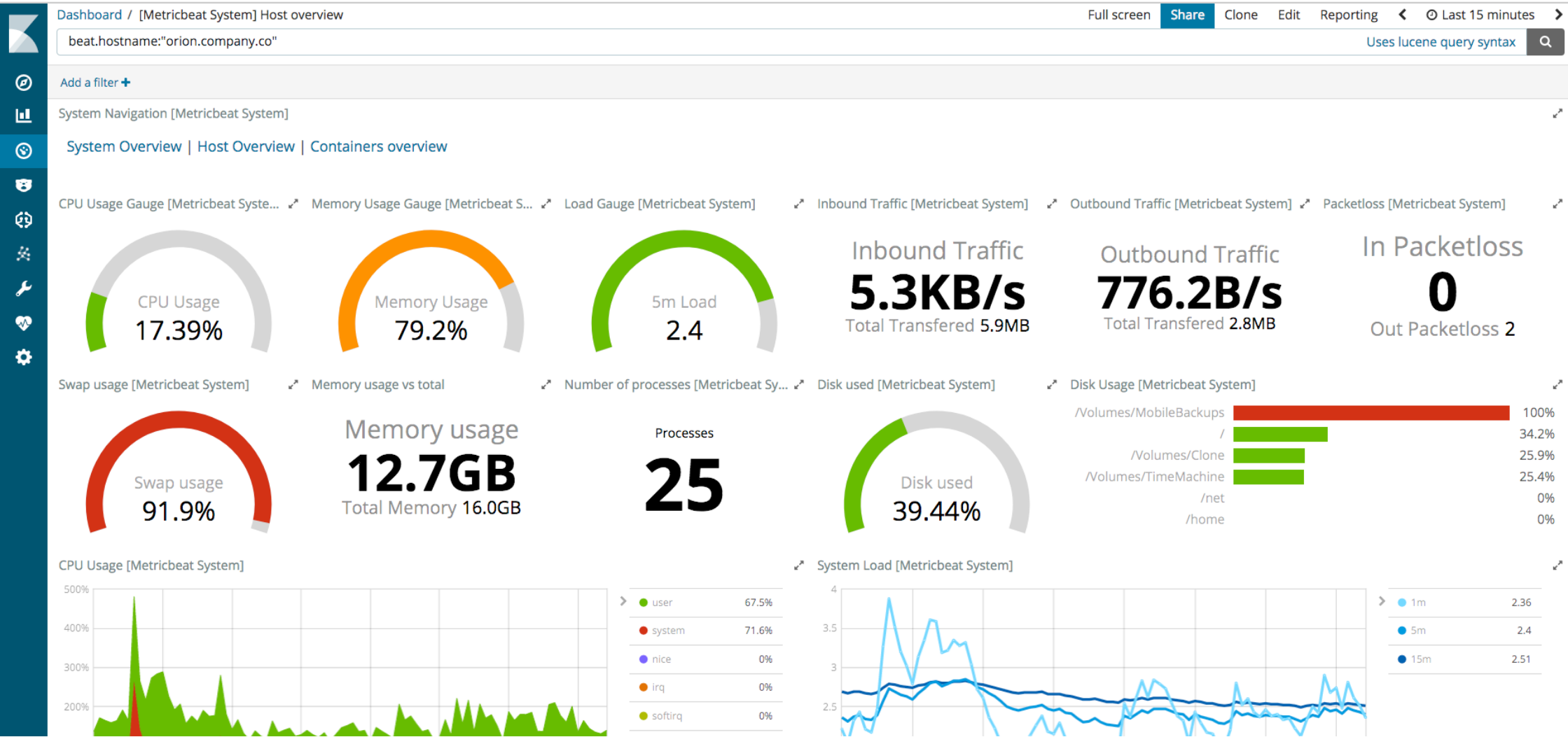


Metricbeat

多くの モジュール

 Aerospike metrics Fetch internal metrics from the Aerospike server.	 Apache metrics Fetch internal metrics from the Apache 2 HTTP server.	 AWS metrics Fetch monitoring metrics for EC2 instances from the AWS APIs and Cloudwatch.	 Ceph metrics Fetch internal metrics from the Ceph server.
CoreDNS metrics Fetch monitoring metrics from the CoreDNS server.	 Couchbase metrics Fetch internal metrics from Couchbase.	 Docker metrics Fetch metrics about your Docker containers.	 Dropwizard metrics Fetch internal metrics from Dropwizard Java application.
 Elasticsearch metrics Fetch internal metrics from Elasticsearch.	 Etcd metrics Fetch internal metrics from the Etcd server.	 Golang metrics Fetch internal metrics from a Golang app.	 HAProxy metrics Fetch internal metrics from the HAProxy server.
 Kafka metrics Fetch internal metrics from the Kafka server.	 Kibana metrics Fetch internal metrics from Kibana.	 Kubernetes metrics Fetch metrics from your Kubernetes installation.	 Logstash metrics Fetch internal metrics from a Logstash server.
 Memcached metrics Fetch internal metrics from the Memcached server.	Microsoft SQL Server Metrics Fetch monitoring metrics from a Microsoft SQL Server instance	 MongoDB metrics Fetch internal metrics from MongoDB.	Munin metrics Fetch internal metrics from the Munin server.
 MySQL metrics Fetch internal metrics from MySQL.	 Nginx metrics Fetch internal metrics from the Nginx HTTP server.	 PHP-FPM metrics Fetch internal metrics from PHP-FPM.	 PostgreSQL metrics Fetch internal metrics from PostgreSQL.
 Prometheus metrics Fetch metrics from a Prometheus exporter.	 RabbitMQ metrics Fetch internal metrics from the RabbitMQ server.	 Redis metrics Fetch internal metrics from Redis.	System metrics Collect CPU, memory, network, and disk statistics from the host.
 Uptime Monitors Monitor services for their availability	uWSGI metrics Fetch internal metrics from the uWSGI server.	vSphere metrics Fetch internal metrics from vSphere.	 Windows metrics Fetch internal metrics from Windows.
Zookeeper metrics Fetch internal metrics from a Zookeeper server.			

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？

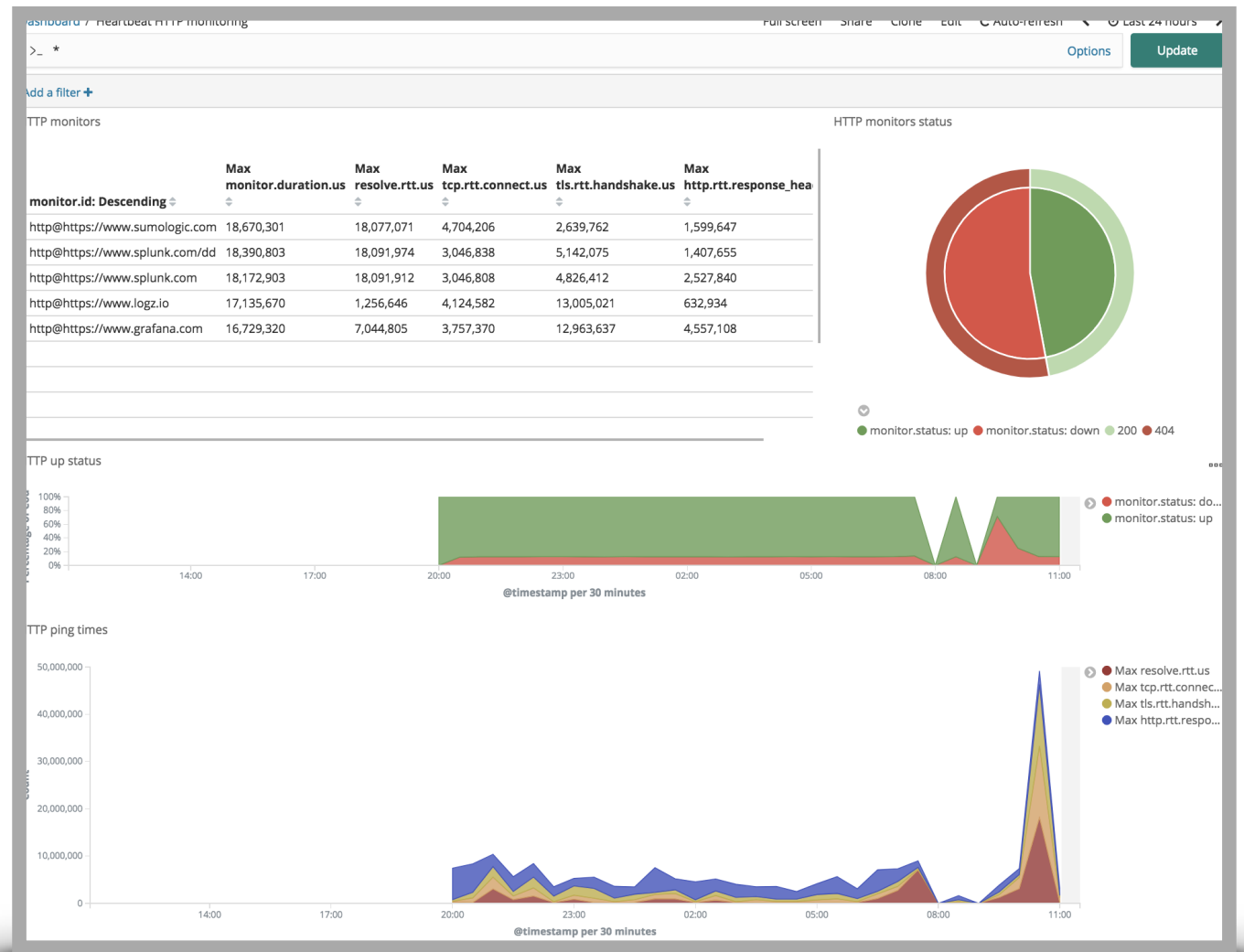
- 手軽にデータの取得から可視化までを提供する仕組み
 - 対象とするシステム、ミドルウェアごとに提供
- 事前に定義された取得データ
 - データソースごとに項目を選別済み、定義
- サンプルとなるグラフおよびダッシュボード
 - Kibanaのグラフ、ダッシュボードも定義済み

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

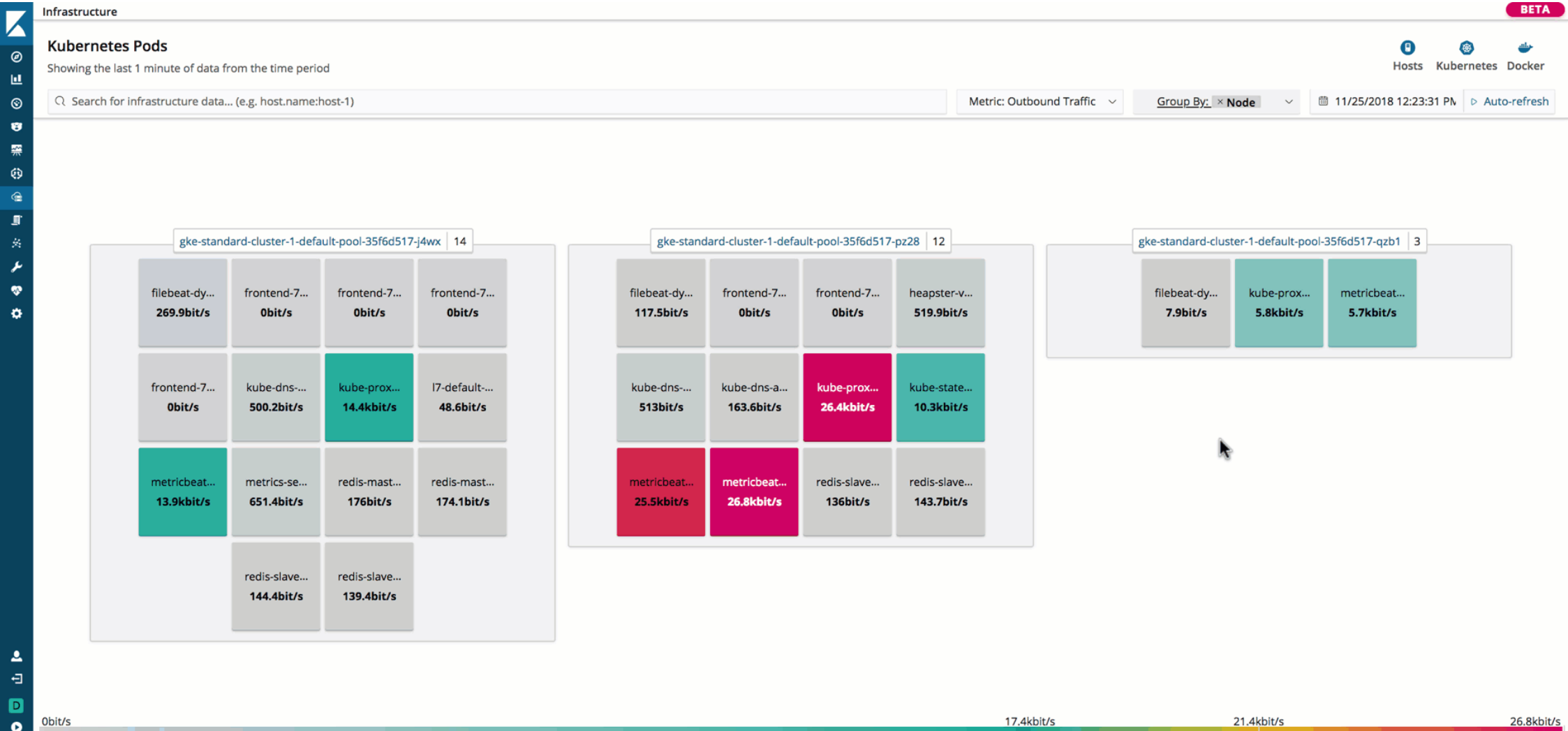
外形監視の 専用UI

The screenshot displays the Uptime UI dashboard. At the top, there's a navigation bar with 'Overview' and 'Uptime' tabs. A search bar and a filter for 'Last 15 hours' are present. The 'Endpoint status' section shows 8 Up, 1 Down, and a Total of 9. The 'Status over time' chart shows a bar chart with blue bars for 'Up' and red bars for 'Down' over a 45-minute period. The 'Monitor status' table lists individual monitors with their status, last updated time, ID, URL, IP, and monitor history.

Status	Last updated	ID	URL	IP	Monitor History
● Up	a few seconds ago	auto-http-0X5E853AD3DD89398F-7960581f1ecb91a9	http://localhost:9200	127.0.0.1	■ ■ ■ ■ ■ ■ ■ ■
● Up	a few seconds ago	auto-http-0X5E853AD3DD89398F-d94a14a568d7afb2	http://blog.johtani.info	104.27.128.50	■ ■ ■ ■ ■ ■ ■ ■
● Up	a few seconds ago	auto-http-0X5E853AD3DD89398F-e21e441f5a592bc8	http://localhost:5601	127.0.0.1	■ ■ ■ ■ ■ ■ ■ ■
● Up	a few seconds ago	auto-http-0X5E853AD3DD89398F-f0926ea0a48fe349	http://elastic.co/jp	151.101.66.217	■ ■ ■ ■ ■ ■ ■ ■
● Down	2 minutes ago	auto-http-0XF52B285DD9DA2D34-5da166b115ba939b	http://blog.johtani/info		■ ■ ■ ■ ■ ■ ■ ■
● Up	2 minutes ago	auto-http-0XF52B285DD9DA2D34-7960581f1ecb91a9	http://localhost:9200	127.0.0.1	■ ■ ■ ■ ■ ■ ■ ■

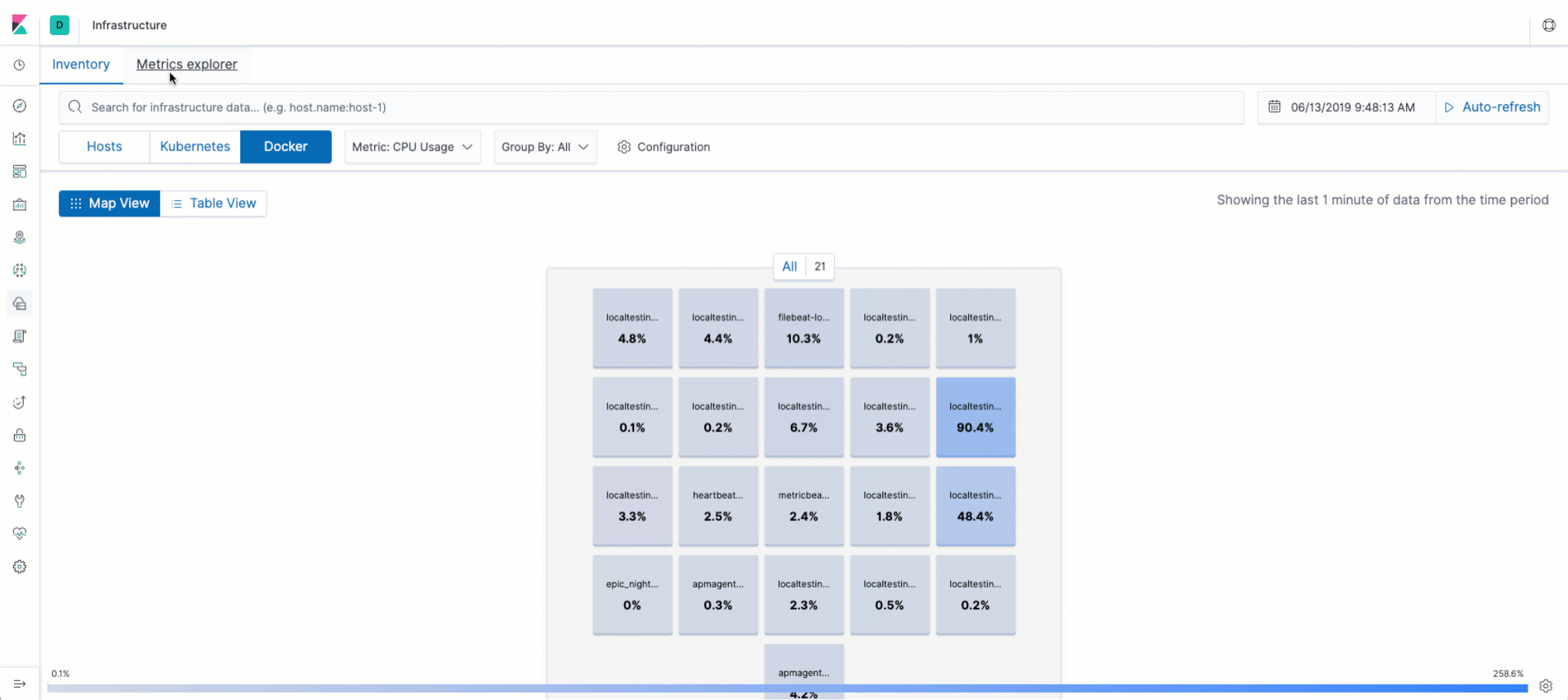
インフラUI

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

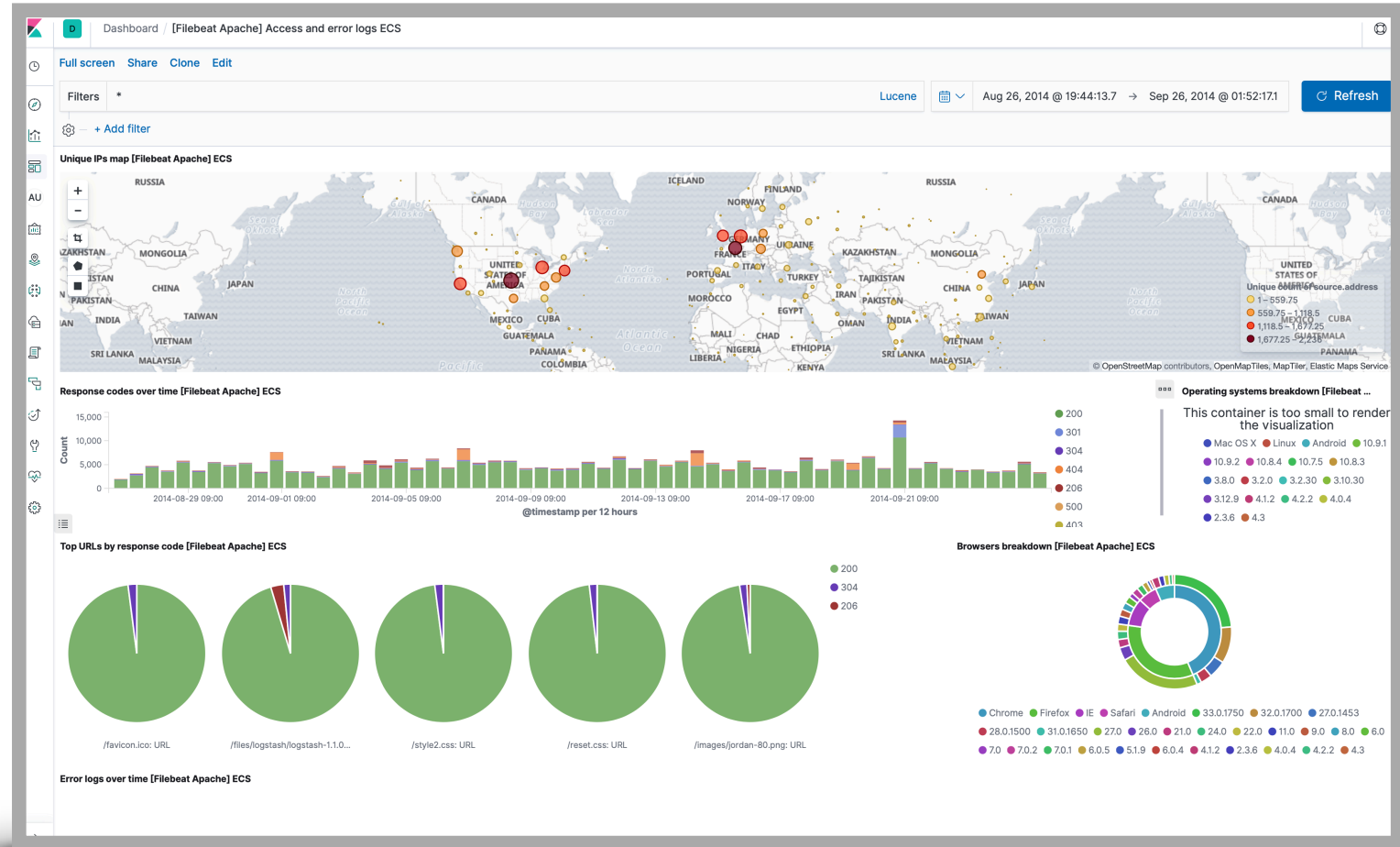


ログ

Filebeat & Auditbeat

Filebeat

ファイルから
ログを収集



Filebeat

多くの
モジュール

Add Data to Kibana

All **Logging** Metrics SIEM Sample data



Apache logs

Collect and parse access and error logs created by the Apache HTTP server.

Cloudwatch Logs

Collect Cloudwatch logs with Functionbeat



Elasticsearch logs

Collect and parse logs created by Elasticsearch.

IIS logs

Collect and parse access and error logs created by the IIS HTTP server.



Kafka logs

Collect and parse logs created by Kafka.



Logstash logs

Collect and parse debug and slow logs created by Logstash itself.



MySQL logs

Collect and parse error and slow logs created by MySQL.

Nats logs

Collect and parse logs created by Nats.



Nginx logs

Collect and parse access and error logs created by the Nginx HTTP server.



PostgreSQL logs

Collect and parse error and slow logs created by PostgreSQL.



Redis logs

Collect and parse error and slow logs created by Redis.

System logs

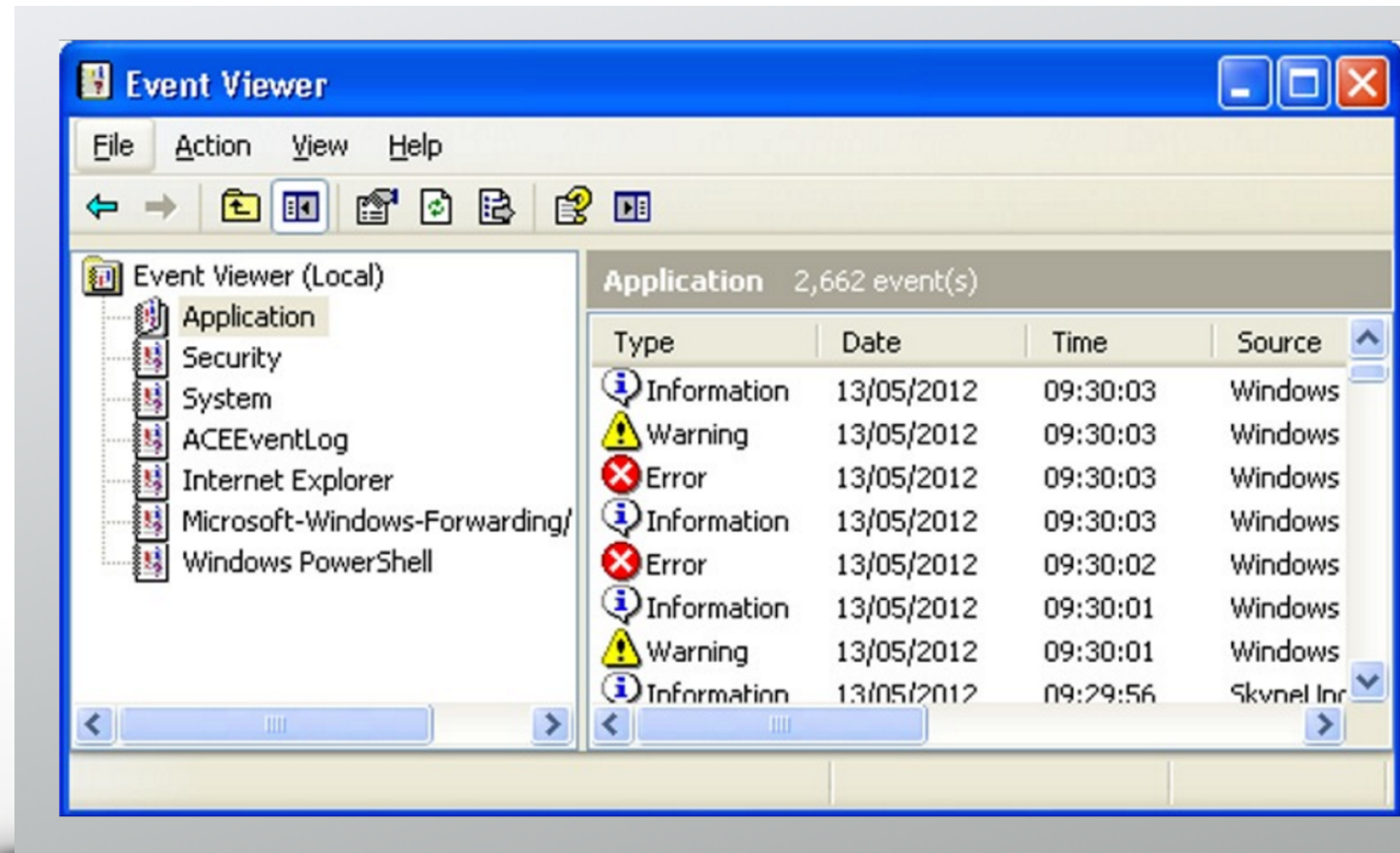
Collect and parse logs written by the local Syslog server.

Traefik logs

Collect and parse access logs created by the Traefik Proxy.

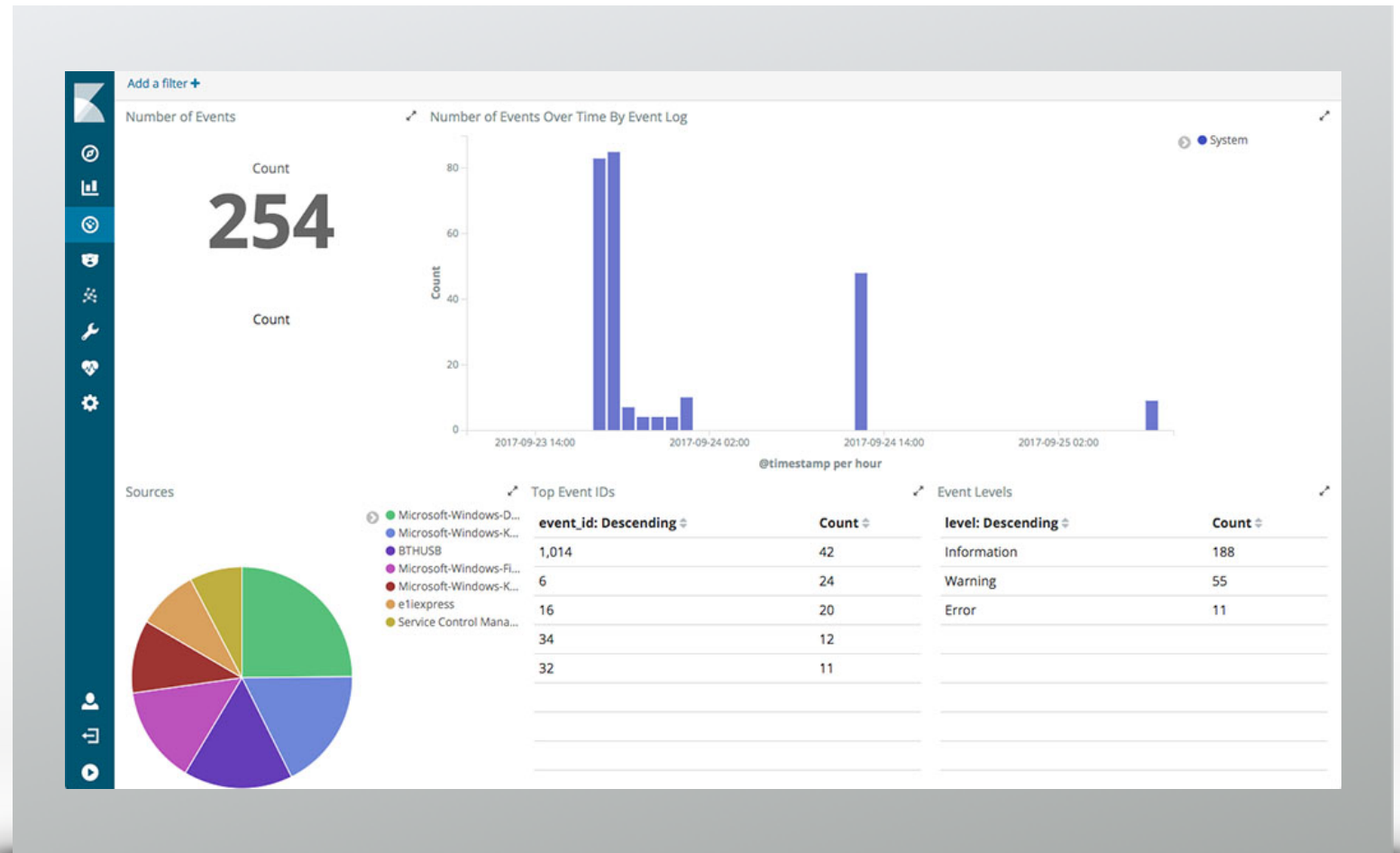
winlogbeat

Welcome
to **1998**



winlogbeat

Now



Packetbeat

Capture the Packet

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:03:59.594512 IP 172.31.98.131.65048 > nuq04s19-in-f21.1e100.net.https: UDP, length 24
10:03:59.692308 IP nuq04s19-in-f21.1e100.net.https > 172.31.98.131.65048: UDP, length 36
10:03:59.726313 IP 172.31.98.131.60568 > r-199-59-148-82.twtrr.com.https: Flags [..], ack 1987017713, win 4096, length 0
10:03:59.801353 IP r-199-59-148-82.twtrr.com.https > 172.31.98.131.60568: Flags [..], ack 1, win 1456, options [nop,nop,TS val 1737158165 ecr 10654051019], length 0
10:03:59.912168 IP pc-in-f189.1e100.net.https > 172.31.98.131.60078: Flags [P.], seq 391100909:391100994, ack 1961900067, win 1651, options [nop,nop,TS val 182273890 ecr 1065405539], length 85
10:03:59.912231 IP 172.31.98.131.60078 > pc-in-f189.1e100.net.https: Flags [..], ack 85, win 4093, options [nop,nop,TS val 1065411882 ecr 182273890], length 0
10:04:00.383581 IP 172.31.98.131.57399 > google-public-dns-a.google.com.domain: 48543+ PTR? 131.98.31.172.in-addr.arpa. (44)
10:04:00.466579 IP google-public-dns-a.google.com.domain > 172.31.98.131.57399: 48543 NXDomain 0/0/0 (44)
10:04:00.467926 IP 172.31.98.131.52072 > google-public-dns-a.google.com.domain: 9347, PTR? 53.239.125.74.in-addr.arpa. (44)
10:04:00.568610 IP google-public-dns-a.google.com.domain > 172.31.98.131.52072: 9347 1/0/0 PTR nuq04s19-in-f21.1e100.net. (83)
10:04:00.569672 IP 172.31.98.131.59451 > google-public-dns-a.google.com.domain: 63862+ PTR? 82.148.59.199.in-addr.arpa. (44)
10:04:00.676625 IP google-public-dns-a.google.com.domain > 172.31.98.131.59451: 63862 1/0/0 PTR r-199-59-148-82.twtrr.com. (83)
10:04:00.677667 IP 172.31.98.131.52322 > google-public-dns-a.google.com.domain: 26687+ PTR? 189.28.125.74.in-addr.arpa. (44)
10:04:00.769797 IP google-public-dns-a.google.com.domain > 172.31.98.131.52322: 26687 1/0/0 PTR pc-in-f189.1e100.net. (78)
10:04:01.230731 IP 172.31.98.131.49573 > pb-in-f95.1e100.net.http: Flags [..], ack 3226625146, win 4096, length 0
10:04:01.340942 IP pb-in-f95.1e100.net.http > 172.31.98.131.49573: Flags [..], ack 1, win 341, options [nop,nop,TS val 4158964323 ecr 1065277921], length 0
10:04:01.367354 IP 172.31.98.131.59991 > pc-in-f125.1e100.net.jabber-client: Flags [..], ack 1, seq 53622692:53622809, ack 3725017102, win 65535, length 117
10:04:01.511794 IP pc-in-f125.1e100.net.jabber-client > 172.31.98.131.59991: Flags [P.], seq 3:134, ack 117, win 65100, length 133
10:04:01.511834 IP 172.31.98.131.59991 > pc-in-f125.1e100.net.jabber-client: Flags [..], ack 134, win 65535, length 0
10:04:01.770555 IP 172.31.98.131.49474 > google-public-dns-a.google.com.domain: 40324+ PTR? 8.8.8.8.in-addr.arpa. (38)
10:04:01.871839 IP google-public-dns-a.google.com.domain > 172.31.98.131.49474: 40324 1/0/0 PTR google-public-dns-a.google.com. (82)
10:04:01.872628 IP 172.31.98.131.50753 > google-public-dns-a.google.com.domain: 14329+ PTR? 95.79.194.173.in-addr.arpa. (44)
10:04:01.907102 IP 172.31.98.131.49578 > 199.27.79.134.http: Flags [..], ack 682580952, win 4096, length 0
```

The screenshot shows the Wireshark interface with the following details:

- Filter: ip.addr == 192.168.1.6
- Packet List Table:

No.	Time	Source	Destination	Protocol	Info
19511	995.233580000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19512	995.233597000	192.168.1.6	192.168.1.6	ICMP	Redirect (Redirect for host)
19513	995.233631000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19514	995.248689000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19515	995.248710000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19516	995.260447000	192.168.1.6	82.192.95.92	TCP	55552 > http [FIN, ACK] Seq=208 Ack=1154 Win=16368 Len=0
19520	995.312985000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521	995.313009000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522	995.314343000	192.168.1.6	82.192.95.92	TCP	55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523	995.314363000	192.168.1.6	82.192.95.92	TCP	[TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524	995.324651000	82.192.95.92	192.168.1.6	TCP	http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525	995.324680000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527	995.325988000	192.168.1.6	82.192.95.92	TCP	[TCP segment of a reassembled PDU]
19528	995.326010000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529	995.326263000	192.168.1.6	82.192.95.92	HTTP	POST /cgi-bin/iavs4stats.cgi HTTP/1.1 (iavs4/stats)
19530	995.326278000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
19531	995.375631000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532	995.376291000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533	995.380658000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534	995.380678000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535	995.382891000	82.192.95.92	192.168.1.6	HTTP	HTTP/1.1 204 No Content
19536	995.382911000	82.192.95.92	192.168.1.6	HTTP	[TCP Retransmission] HTTP/1.1 204 No Content
19539	995.505191000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540	995.505232000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550	996.308269000	192.168.1.6	149.7.96.236	TCP	55553 > mtap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551	996.308324000	192.168.1.6	192.168.1.6	ICMP	Redirect (Redirect for host)
19552	996.308363000	192.168.1.6	149.7.96.236	TCP	55553 > mtap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
- Packet 19552 details:
 - Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
 - Ethernet II, Src: HonHaiPr_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewaf_43:90:de (08:15:af:43:90:de)
 - Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)
 - Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23
- Raw data: 0000 00 15 af 43 90 de c0 cb 38 26 b5 30 08 00 45 00 ...C... 86.0.E.

Packetbeat

パケットを
キャプチャ



どういう仕組み？

- 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

Machine Learning / File Data Visualizer (Experimental) 30 seconds

Job Management Anomaly Explorer Single Metric Viewer Data Visualizer Settings

File contents

First 999 lines

```
1 93.180.71.3 - - [17/May/2017:08:05:32 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"
2 93.180.71.3 - - [17/May/2017:08:05:23 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"
3 80.91.33.133 - - [17/May/2017:08:05:24 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.17)"
4 217.168.17.5 - - [17/May/2017:08:05:34 +0000] "GET /downloads/product_1 HTTP/1.1" 200 490 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"
5 217.168.17.5 - - [17/May/2017:08:05:09 +0000] "GET /downloads/product_2 HTTP/1.1" 200 490 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"
6 93.180.71.3 - - [17/May/2017:08:05:57 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"
7 217.168.17.5 - - [17/May/2017:08:05:02 +0000] "GET /downloads/product_2 HTTP/1.1" 404 337 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"
8 217.168.17.5 - - [17/May/2017:08:05:42 +0000] "GET /downloads/product_1 HTTP/1.1" 404 332 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"
9 80.91.33.133 - - [17/May/2017:08:05:01 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.17)"
10 93.180.71.3 - - [17/May/2017:08:05:27 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"
11 217.168.17.5 - - [17/May/2017:08:05:12 +0000] "GET /downloads/product_2 HTTP/1.1" 200 3316 "-" "-"
12 188.138.60.101 - - [17/May/2017:08:05:49 +0000] "GET /downloads/product_2 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.9.7.9)"
```

Summary

Number of lines analyzed	999
Format	semi_structured_text
Grok pattern	%{COMBINEDAPACHELOG}
Time field	timestamp
Time format	dd/MMM/YYYY:HH:mm:ss Z

[Override settings](#)

File stats

t agent

Progress: File processed, Index created, Ingest pipeline created, Data uploaded, Index pattern created

Import complete

Index	test_logs
Index pattern	test_logs
Ingest pipeline	test_logs-pipeline
Documents ingested	51462

View index in Discover | Create new ML job | Open in Data Visualizer | Index Management | Index Pattern Management

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

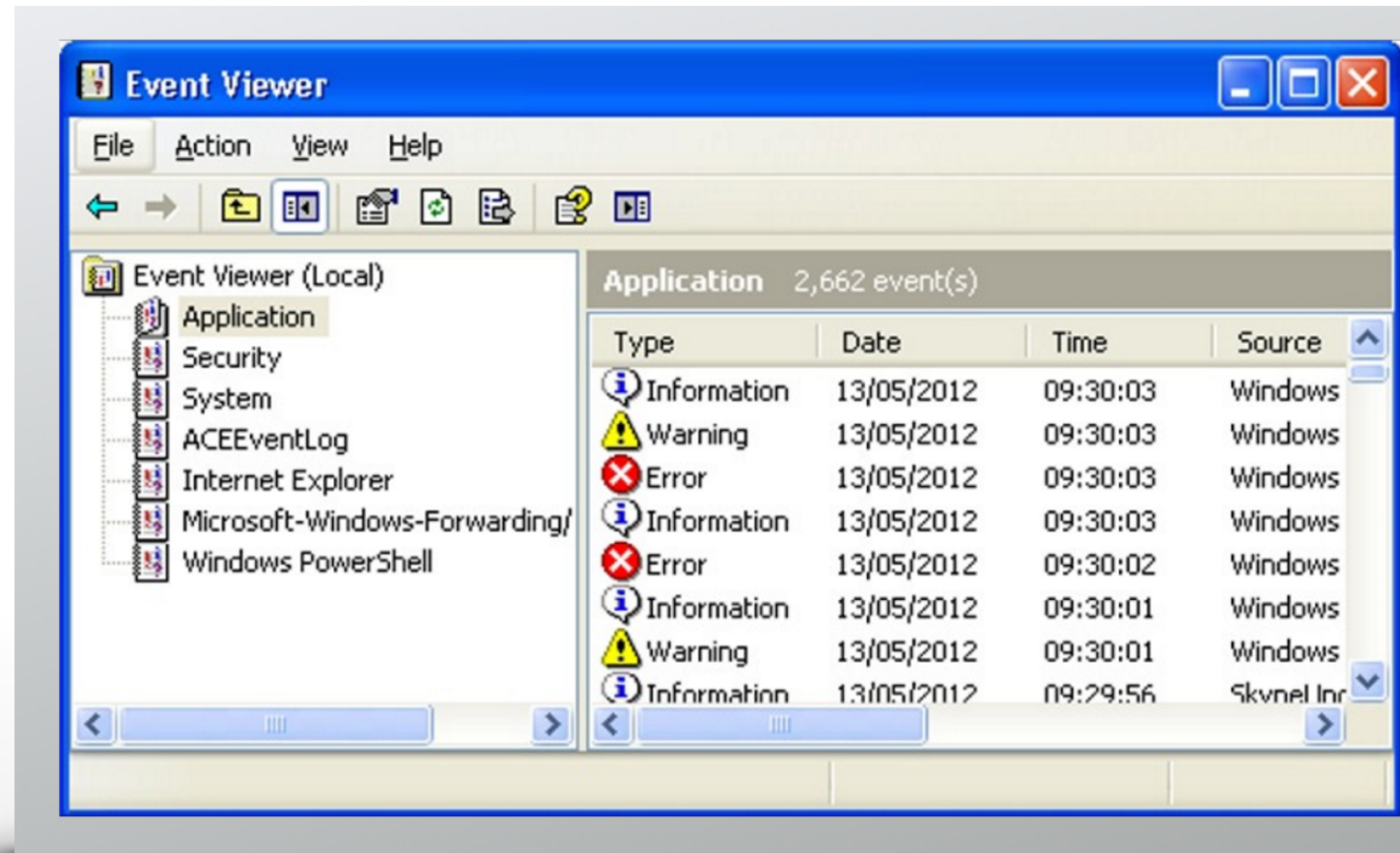
The screenshot displays the Logs Solution interface. At the top, there is a search bar containing the text '404'. To the right of the search bar are buttons for 'Customize', 'streaming...', and 'Stop streaming'. Below the search bar is a vertical sidebar with various icons. The main area shows a list of log entries, each with a timestamp and a log message. The log messages are filtered to show only those containing '404'. The log entries are as follows:

Timestamp	Log Message
2018-10-26 15:40:43.073	{ "type": "response", "@timestamp": "2018-10-26T22:40:42Z", "tags": [], "pid": 1, "method": "post", "headers": { "host": "104.197.165.132", "length": "1348", "accept": "*/*", "origin": "http://104.197.165.132:5601", "kbn-xsr": "(Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36", "type": "application/json", "referer": "http://104.197.165.132:5601/app/infra", "a": "US,en;q=0.9"}, "remoteAddress": "47.134.161.222", "userAgent": "47.134.161.222", "statusCode": 200, "responseTime": 404, "contentLength": 9, "message": "POST /api/infra/graphql" }
2018-10-26 16:00:11.000	apache2 47.134.161.222 - "GET /hellothere HTTP/1.1" 404 436
2018-10-27 10:44:39.000	apache2 61.216.152.133 - "POST /10 HTTP/1.1" 404 428
2018-10-27 13:29:47.000	apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/phpmyadmin/ HTTP/1.1" 404 207
2018-10-27 13:29:47.000	apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/PMA/ HTTP/1.1" 404 206
2018-10-27 13:29:48.000	apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/dbadmin/ HTTP/1.1" 404 206
2018-10-27 13:29:48.000	apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/pma/ HTTP/1.1" 404 206
2018-10-27 13:29:48.000	apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/db/ HTTP/1.1" 404 206
2018-10-27 17:00:11.000	apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/phpmyadmin/ HTTP/1.1" 404 207
2018-10-27 17:00:11.000	apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/PMA/ HTTP/1.1" 404 206
2018-10-27 17:00:11.000	apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/dbadmin/ HTTP/1.1" 404 206
2018-10-27 17:00:11.000	apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/pma/ HTTP/1.1" 404 206
2018-10-27 17:00:11.000	apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/db/ HTTP/1.1" 404 206
2018-10-27 17:21:13.000	apache2 81.7.14.241 - "HEAD /robots.txt HTTP/1.0" 404 170
2018-10-27 17:31:01.000	apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/phpmyadmin/ HTTP/1.1" 404 207
2018-10-27 17:31:01.000	apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/PMA/ HTTP/1.1" 404 206
2018-10-27 17:31:01.000	apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/dbadmin/ HTTP/1.1" 404 206
2018-10-27 17:31:02.000	apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/pma/ HTTP/1.1" 404 206
2018-10-27 17:31:02.000	apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/db/ HTTP/1.1" 404 206

At the bottom of the interface, there is a status bar that reads 'Streaming new entries' and 'last updated 1s ago'.

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

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

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"
    }
  }
}
```

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/20100101 Firefox/5.0"
```


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} %{HTTPOUSER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb} %{NOTSPACE:request} (?: HTTP/%{NUMBER:httpversion})? % {DATA:rawrequest})" %{NUMBER:response} (?:%{NUMBER:bytes} -)

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>

The screenshot shows the Grok Debugger interface within the Kibana Dev Tools. The interface is divided into several sections:

- Sample Data:** A text area containing a single log entry: `1 55.3.244.1 GET /index.html 15824 0.043`
- Grok Pattern:** A text area containing a Grok pattern: `1 %{IP:client} %{WORD:method} %{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}`
- Custom Patterns:** A section with a dropdown arrow and the text "Custom Patterns".
- Simulate:** A blue button labeled "Simulate".
- Structured Data:** A text area showing the structured output of the Grok pattern:

```
1 {
2   "duration": "0.043",
3   "request": "/index.html",
4   "method": "GET",
5   "bytes": "15824",
6   "client": "55.3.244.1"
7 }
```

The interface also features a sidebar on the left with various icons for navigation and a top bar with the "Dev Tools" label and tabs for "Console", "Search Profiler", and "Grok Debugger".



APM

Elastic APM

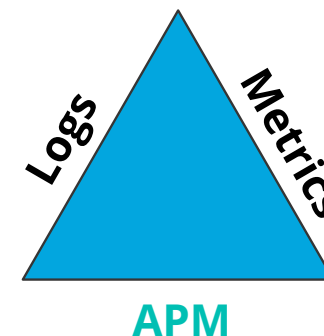
Application Performance Monitoring (APM)

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



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

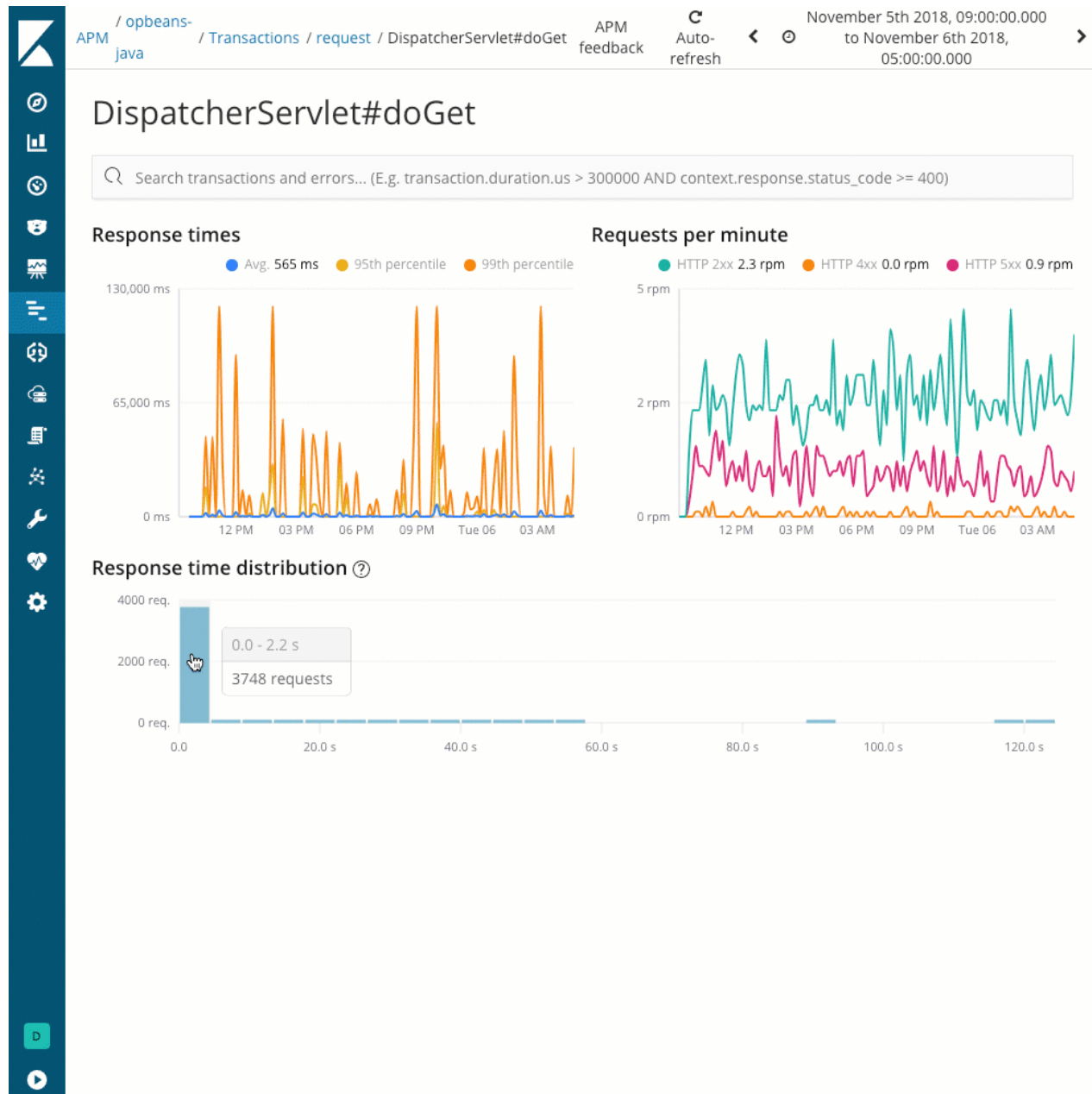
専用 UI

Streamline APM workflows
分散トレーシング

APM以外との連携

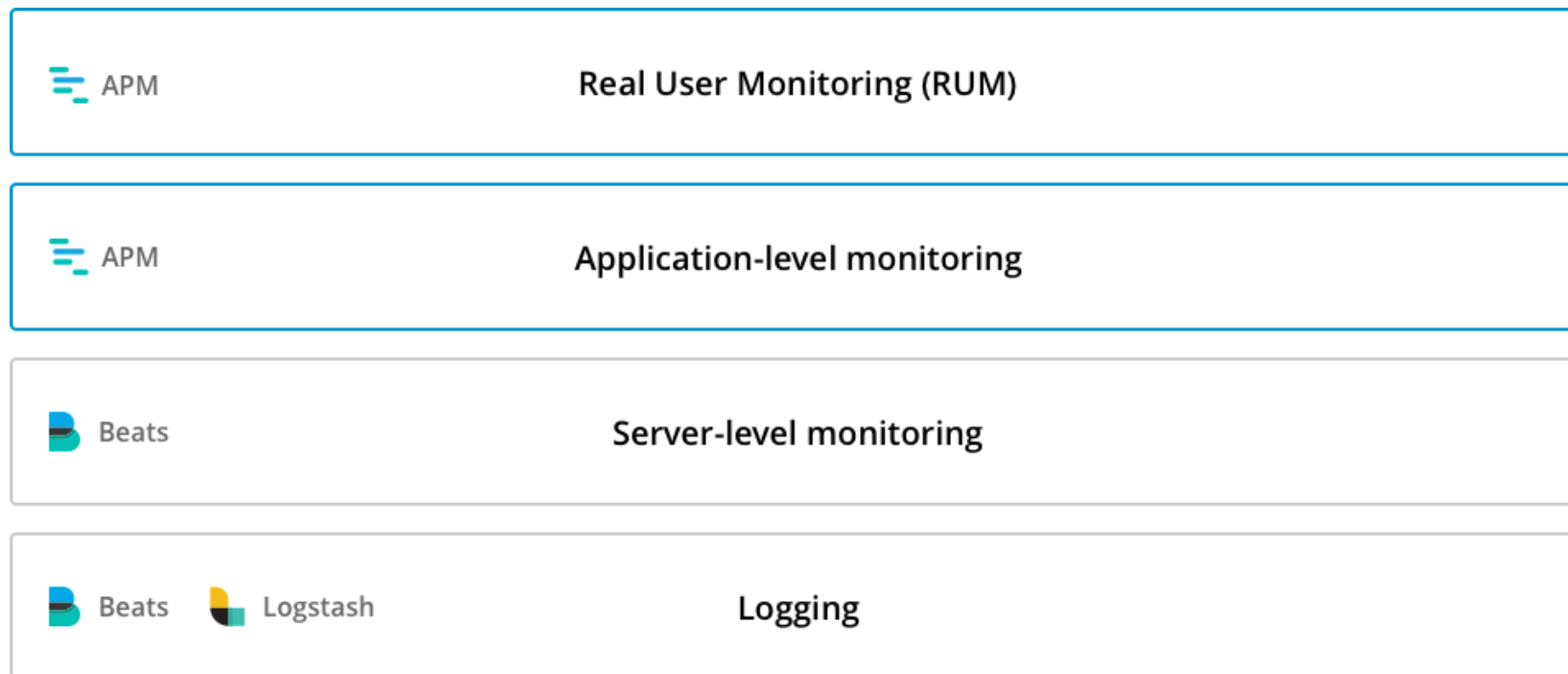
他のデータとの関連

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

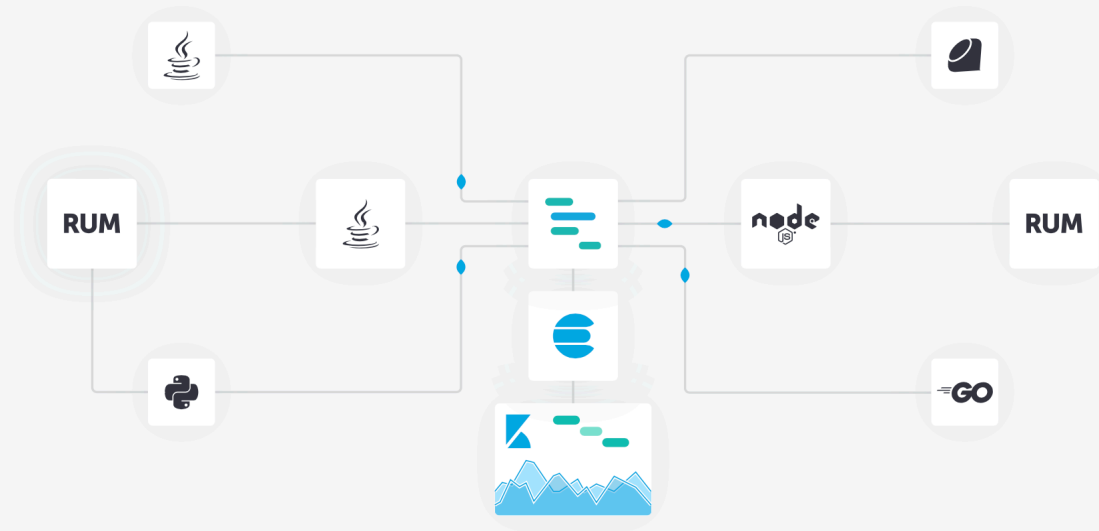


RUM



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)

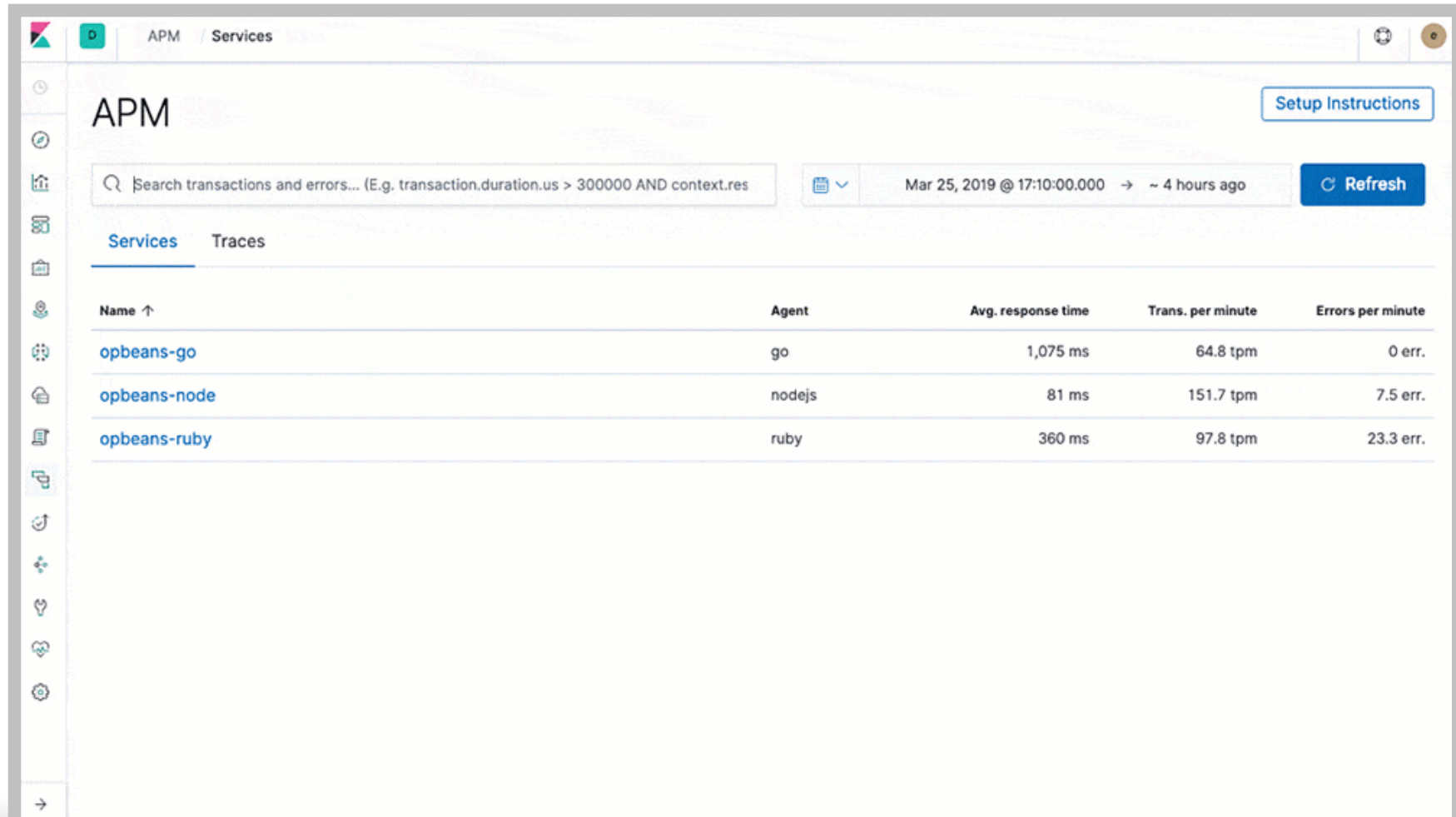
ログやシステムのメトリックをElasticsearchに取り込みましたか？
ElasticのAPMで、アプリケーションのメトリックも取り込むことができます。
初期設定に、4行コードを加えるだけ。
問題箇所をすばやく確認し、自信をもってコードをプッシュできます。



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](#)

Elastic APM



The screenshot shows the Elastic APM 'Services' page. At the top, there is a search bar with the text 'Search transactions and errors... (E.g. transaction.duration.us > 300000 AND context.res)'. To the right of the search bar, there is a date range selector set to 'Mar 25, 2019 @ 17:10:00.000' and a 'Refresh' button. Below the search bar, there are two tabs: 'Services' (selected) and 'Traces'. The main content area displays a table with the following data:

Name ↑	Agent	Avg. response time	Trans. per minute	Errors per minute
opbeans-go	go	1,075 ms	64.8 tpm	0 err.
opbeans-node	nodejs	81 ms	151.7 tpm	7.5 err.
opbeans-ruby	ruby	360 ms	97.8 tpm	23.3 err.

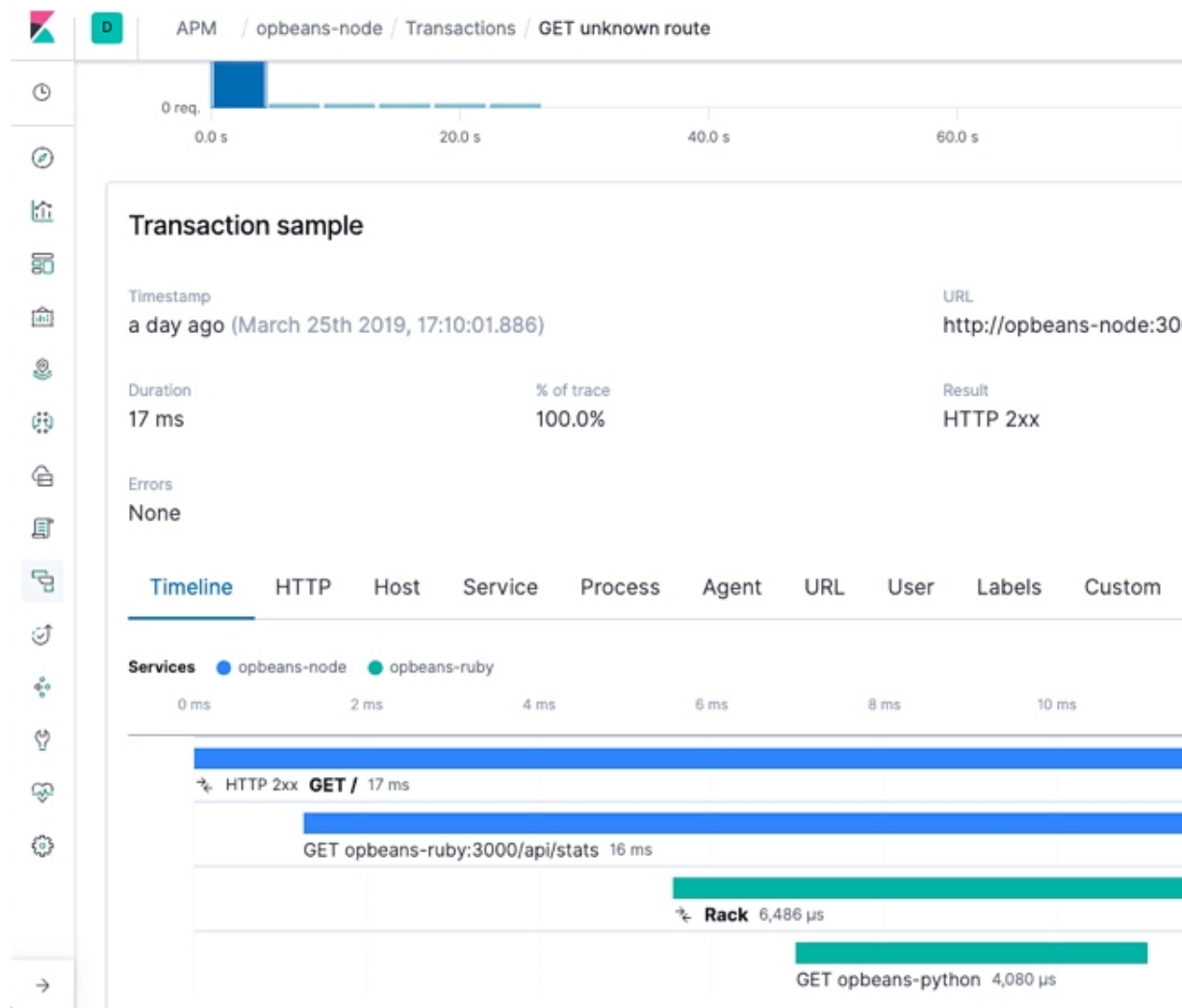
分散トレーシング

GA I 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

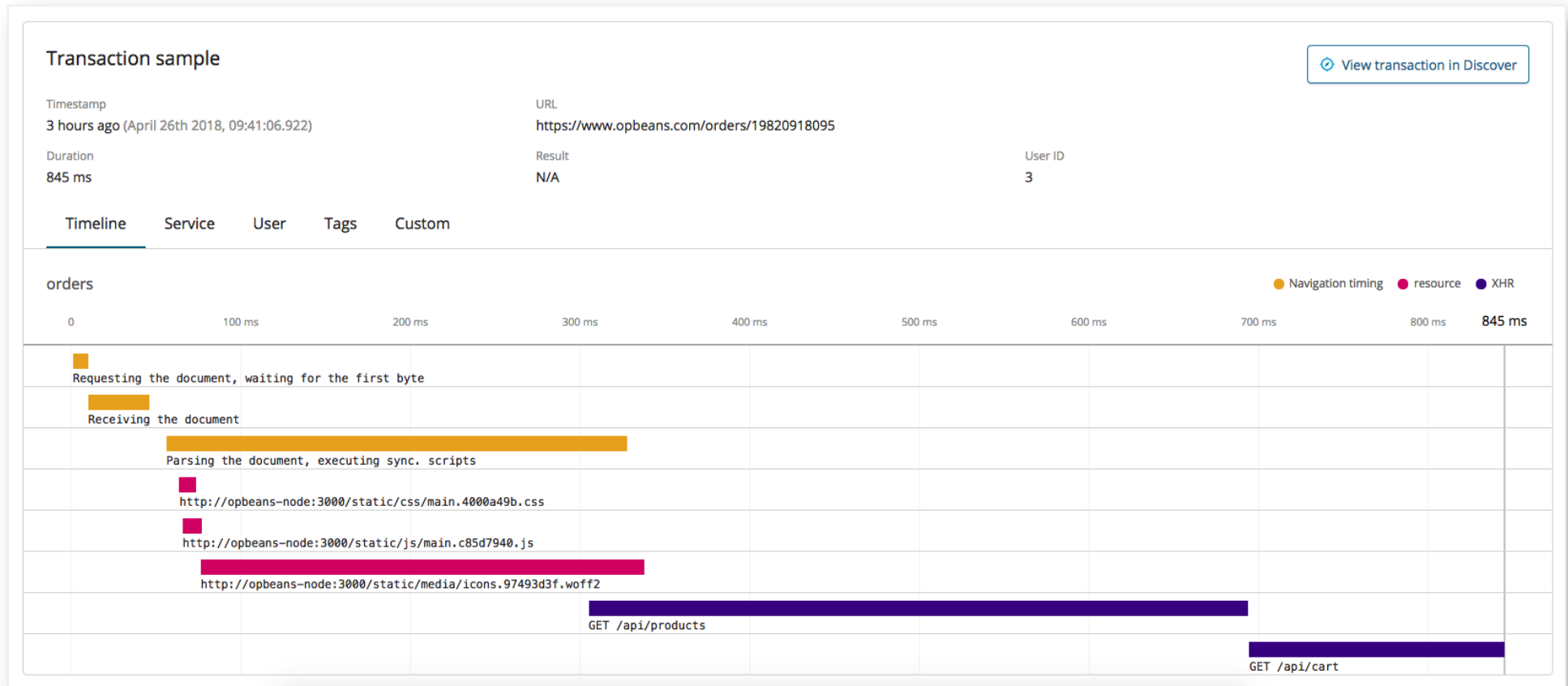
サブコンテキスト内のトレースに遷移

OpenTracing 互換

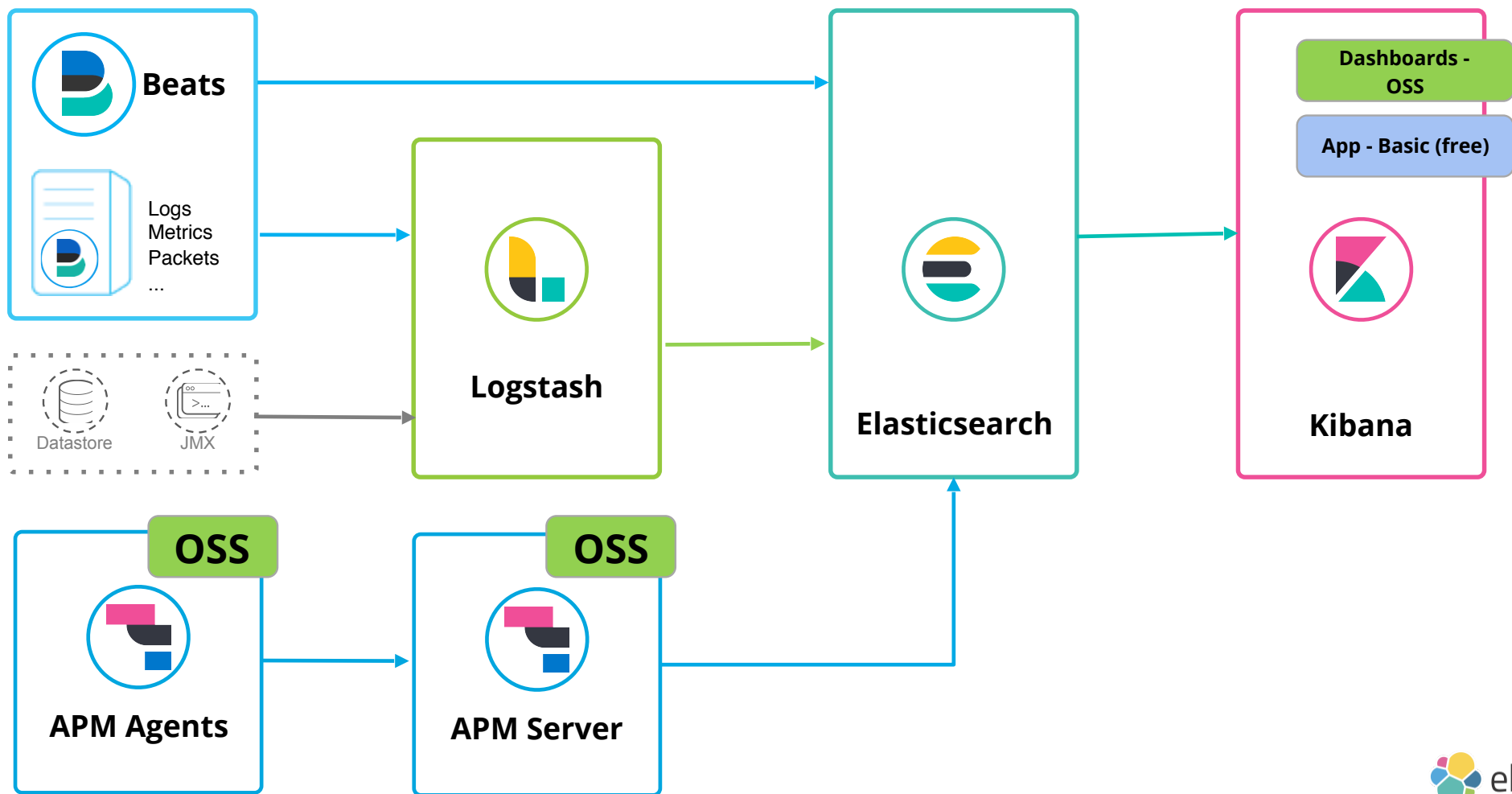


RUM (リアルユーザー監視)

ブラウザでの処理時間を計測



構成例



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
<code>destination.ip</code>	IP address of the destination. Can be one or multiple IPv4 or IPv6 addresses.	ip
<code>destination.hostname</code>	Hostname of the destination.	keyword
<code>destination.port</code>	Port of the destination.	long
<code>destination.mac</code>	MAC address of the destination.	keyword
<code>destination.domain</code>	Destination domain.	keyword
<code>destination.subdomain</code>	Destination subdomain.	keyword

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

-  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

The screenshot shows the 'Add Data to Kibana' interface in Kibana. The page title is 'Add Data to Kibana' and the breadcrumb is 'Home'. There are four tabs: 'All', 'Logging', 'Metrics', and 'Sample data'. The 'All' tab is selected. The dashboard displays a grid of 16 data source cards, each with an icon, a title, and a brief description of what it does. The cards are arranged in a 4x4 grid. The data sources include: Aerospike metrics, Apache logs, Apache metrics, APM, Ceph metrics, Couchbase metrics, Docker metrics, Dropwizard metrics, Elasticsearch logs, Elasticsearch metrics, Etcd metrics, Golang metrics, HAProxy metrics, IIS logs, Kafka logs, Kafka metrics, Kibana metrics, Kubernetes metrics, Logstash logs, and Logstash metrics.

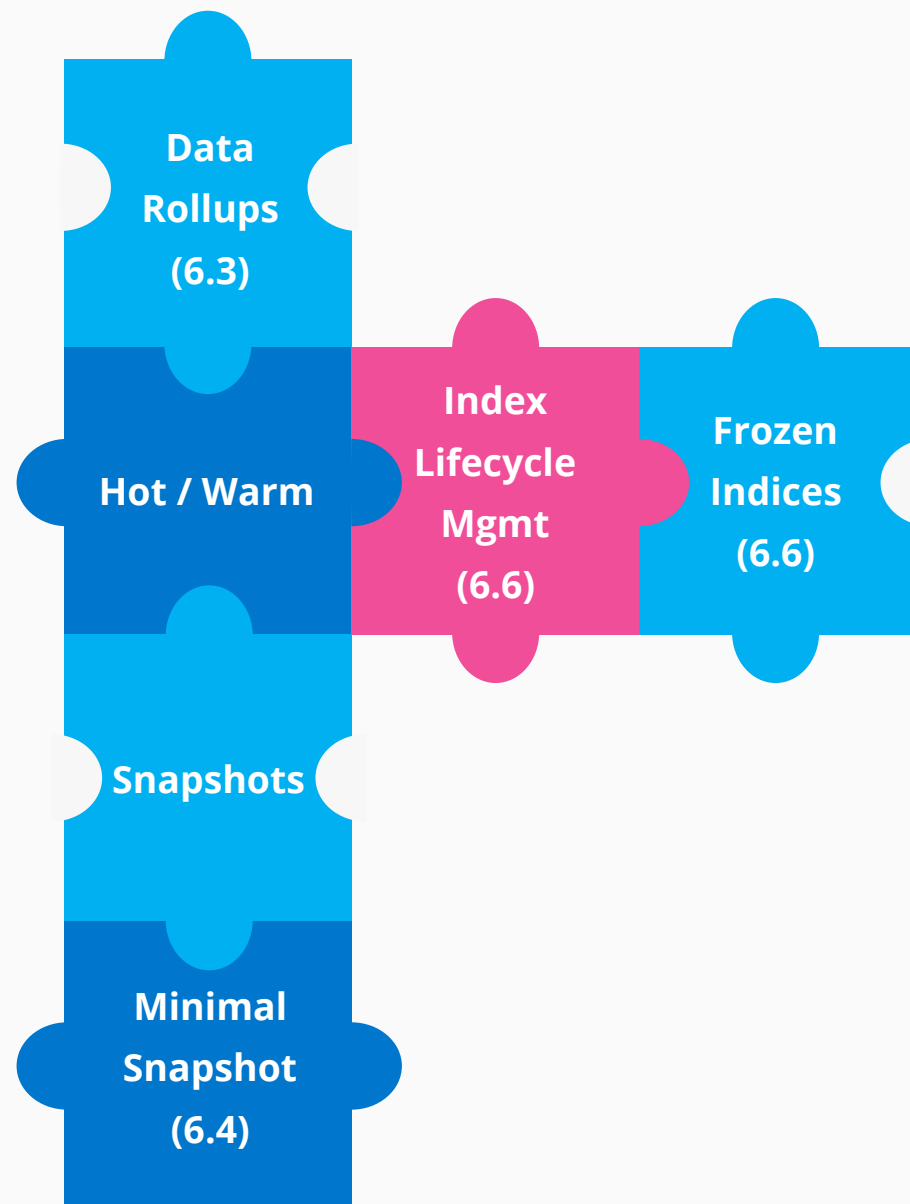
Icon	Source Name	Description
	Aerospike metrics	Fetch internal metrics from the Aerospike server.
	Apache logs	Collect and parse access and error logs created by the Apache HTTP server.
	Apache metrics	Fetch internal metrics from the Apache 2 HTTP server.
	APM	Collect in-depth performance metrics and errors from inside your applications.
	Ceph metrics	Fetch internal metrics from the Ceph server.
	Couchbase metrics	Fetch internal metrics from Couchbase.
	Docker metrics	Fetch metrics about your Docker containers.
	Dropwizard metrics	Fetch internal metrics from Dropwizard Java application.
	Elasticsearch logs	Collect and parse logs created by Elasticsearch.
	Elasticsearch metrics	Fetch internal metrics from Elasticsearch.
	Etcd metrics	Fetch internal metrics from the Etcd server.
	Golang metrics	Fetch internal metrics from a Golang app.
	HAProxy metrics	Fetch internal metrics from the HAProxy server.
	IIS logs	Collect and parse access and error logs created by the IIS HTTP server.
	Kafka logs	Collect and parse logs created by Kafka.
	Kafka metrics	Fetch internal metrics from the Kafka server.
	Kibana metrics	Fetch internal metrics from Kibana.
	Kubernetes metrics	Fetch metrics from your Kubernetes cluster.
	Logstash logs	Collect and parse debug and slow logs created by Logstash.
	Logstash metrics	Fetch internal metrics from Logstash.

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

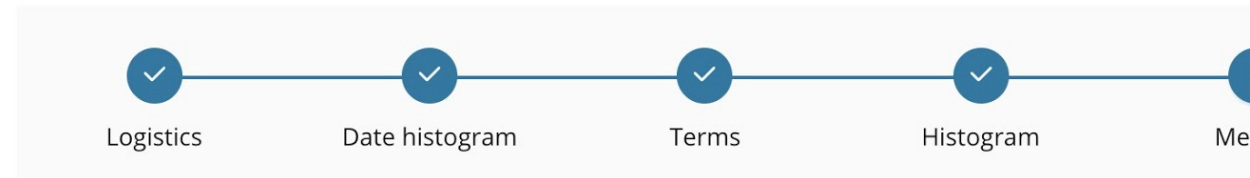
Kibana Support

Rollups Management UI

Visualize rolled up data

Rollup jobs / Create

Create rollup job



Metrics (optional)

Select the metrics to collect while rolling up data. By default, only doc_counts are collected for each group.

Search

Field

bytes	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum
machine.ram	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum
memory	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum
phpmemory	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum

Rows per page: 200

< Back

Next >

Hot/Warm Architecture in EC / ECE

Optimize the use of compute resources and save \$\$\$

5 Optimize your deployment

I/O Optimized

Recommended

Use for search and general all-purpose workloads. Includes a balance of compute, memory, and storage.

[Default specs](#)



Compute Optimized

Run CPU-intensive workloads or run smaller workloads cost-effectively when you need less memory and storage.

[Default specs](#)



Memory Optimized

Perform memory-intensive operations efficiently, including workloads with frequent aggregations.

[Default specs](#)



Hot-Warm Architecture

Use for time-series analytics and logging workloads that benefit from automatic index curation.

[Default specs](#)



Deployments

Platform

- Summary
- Allocators

Create deployment template

1 Elasticsearch 2 **Index Curation** 3 Kibana & APM 4 Name

Index curation

New indices get created on hot nodes first and are moved to warm nodes later on, based on the choices you make here. [Learn more...](#)

Select where new indices will be created (hot)

Select where new indices will be moved to (warm)

Index pattern	Move indices ...
<input type="text" value="example-index1-*"/>	After 6 Days
<input type="text" value="different-index-*"/>	After 1 Month
<input type="text" value="filebeat-*"/>	After 2 Weeks
<input type="text" value="metricbeat-*"/>	After 2 Weeks
<input type="text" value="logstash-*"/>	After 2 Weeks

[+ Add index](#)

!* The Lifecycle of these index patterns is managed by Elasticsearch. [Learn more...](#)

[< Previous](#) [Next >](#)

Name: Elastic Test Depl...

Versions: All

Hourly Rate: \$0.1827

Monthly Rate: \$131.58

Architecture

Zone 1

- Blue
- Green
- Grey

Zone 2

- Blue
- Green

Legend:

- Blue: Data - Hot Instance | 64 GB
- Green: Data - Warm Instance | 8 GB
- Grey: ML | 4 GB

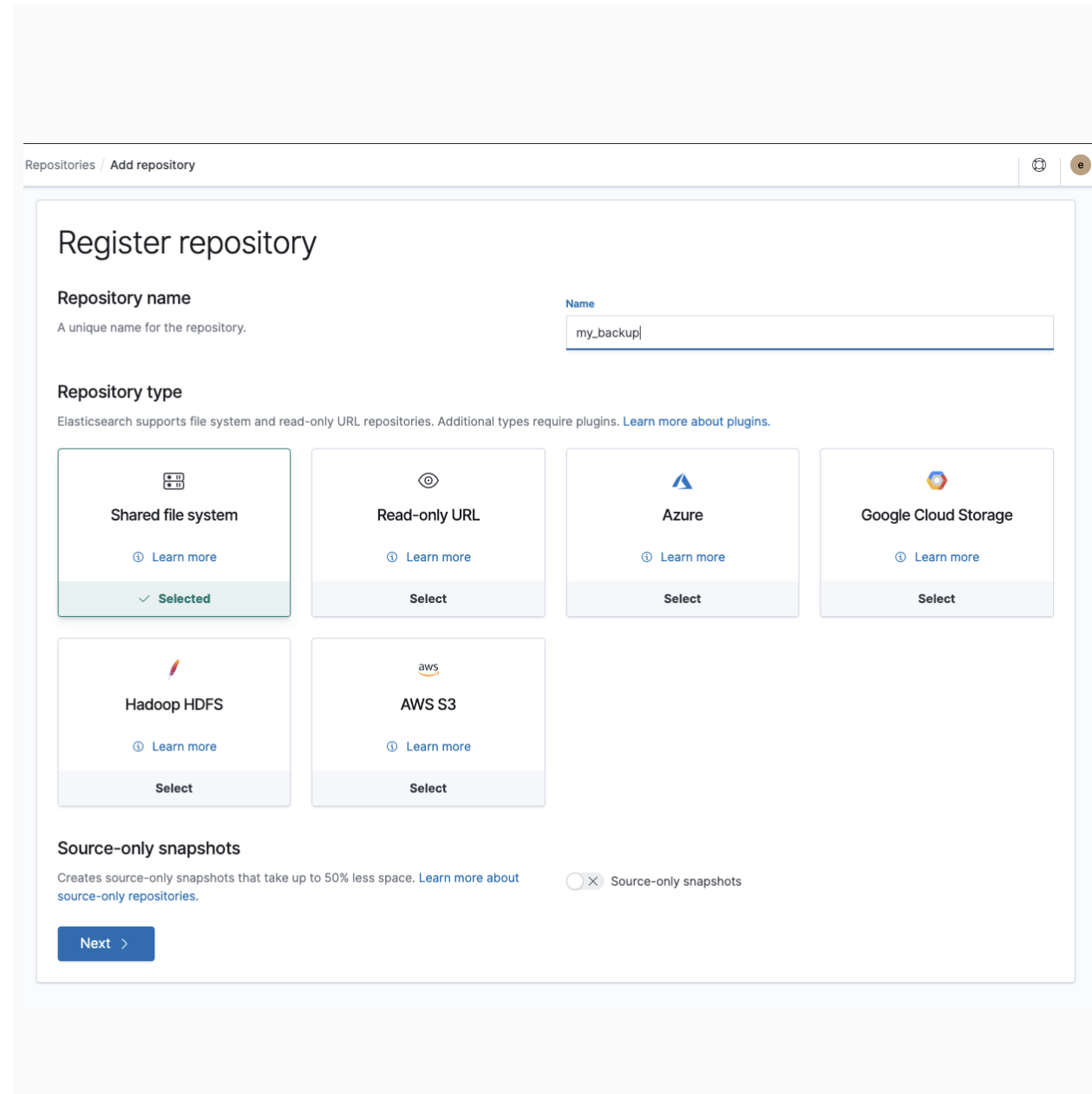
Snapshot UIs

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

Snapshot Repositories

Use repositories to store backups of your Elasticsearch indices and clusters.

[Snapshots](#) [Repositories](#)

Search...

Snapshot	Repository	Date created ↓
snapshotd-2019.05.23	fs-backups	23 May 2019 14:26:31
snapshotc-2019.05.23	fs-backups	23 May 2019 14:26:20
snapshotb-2019.05.23	fs-backups	23 May 2019 14:26:07
snapshota-2019.05.23	fs-backups	23 May 2019 14:25:29

Rows per page: 20

snapshotd-2019.05.23

fs-backups

Summary

Version / Version number
8.0.0 / 80000

State
✓ **Snapshot**

Indices (6)

- .kibana_
- .kibana_
- .security
- kibana_
- kibana_
- kibana_

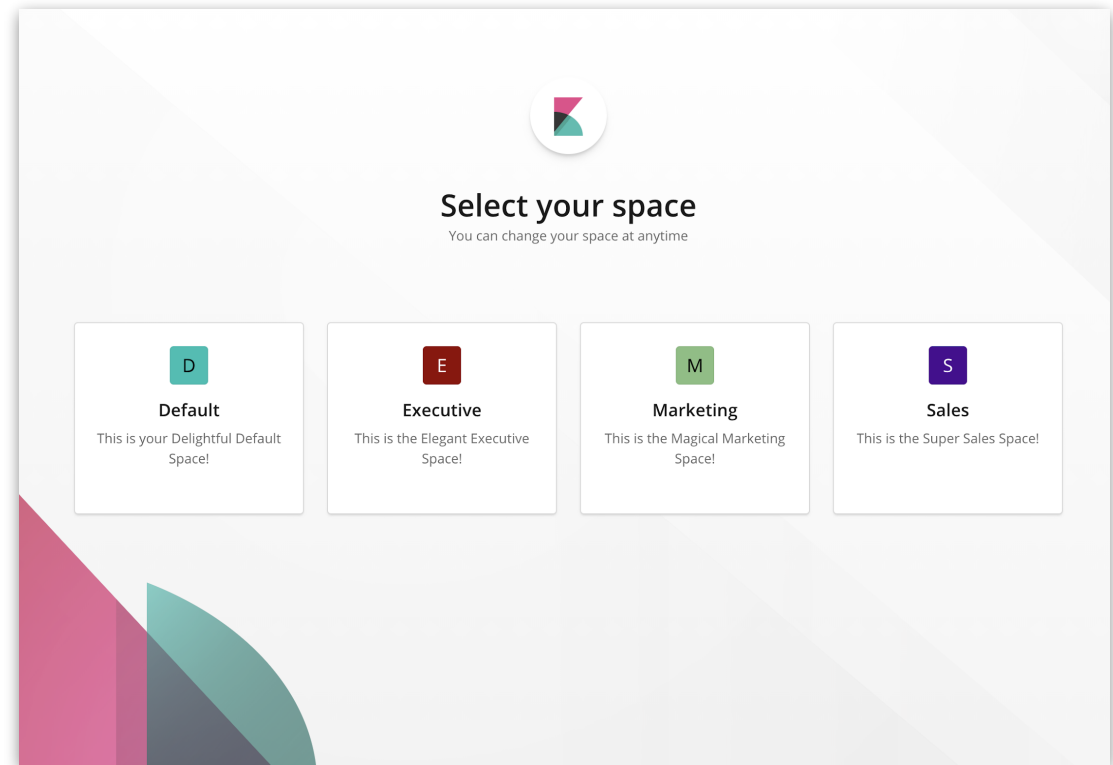
Start time
23 May 2019

Duration
1 second

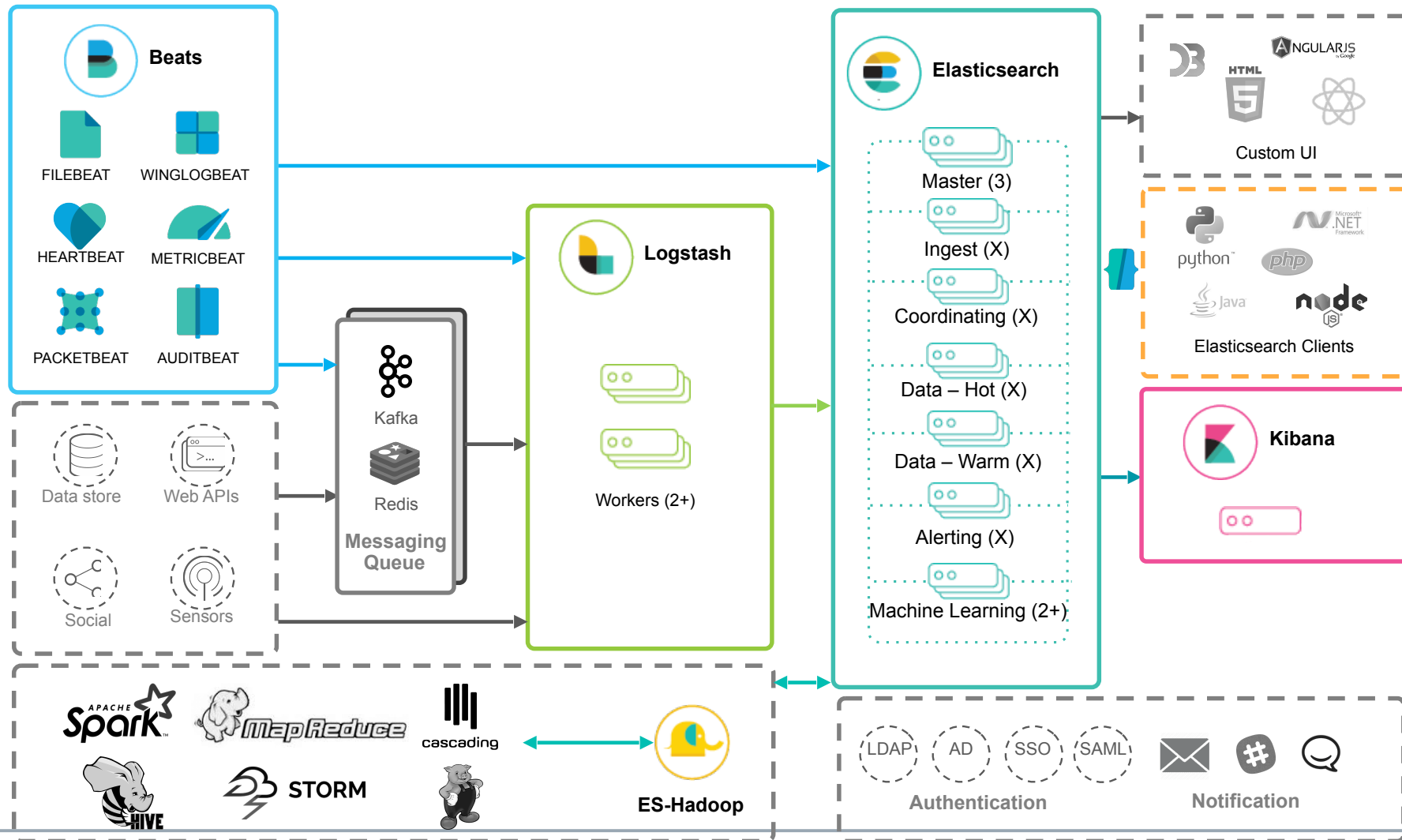
× Close

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



Typical Logging Deployment in the Enterprise



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

The screenshot displays the Kibana dashboard interface. On the left is a dark blue sidebar with the Kibana logo and a list of navigation items: Discover, Visualize, Dashboard (highlighted), Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. At the bottom of the sidebar are user options: Guest User, Logout, Privacy Statement, and Default. The main dashboard area has a header with the breadcrumb 'Dashboard / Welcome Dashboard', action buttons for 'Full screen', 'Share', 'Clone', 'Edit', 'Auto-refresh', and 'Last 15 minutes', a search bar containing '>_ \$earch... (e.g. status:200 AND extension:PHP)', and 'Options' and 'Refresh' buttons. Below the header is a grid of eight feature tiles:

- WELCOME**: Elastic Demo Gallery is a live read-only Kibana environment with a collection of little examples to let anyone experience different features of the Elastic Stack. Click on a tile to begin your own adventure.
- KIBANA VISUALIZATIONS**: Visual Explorations. Dive into the world of Kibana charts and visualizations with a sample dataset. [Explore Away](#)
- CANVAS**: Canvas. Create dynamic, multi-page, pixel-perfect displays for screens large and small. [Get Creative](#)
- ELASTIC APM**: Elastic APM. See how Elastic APM lets you track application performance metrics and more. [Open App](#)
- BEATS & LOGSTASH**: Beats & Logstash Modules. Modules give a 5-minute data-to-dashboard path for common data formats. Sample a few. [Sample it](#)
- MACHINE LEARNING**: Machine Learning. Explore the world of anomaly detection with preconfigured machine learning jobs. [Dive in](#)
- ELASTICSEARCH SQL**: Elasticsearch SQL. Get hands-on with querying Elasticsearch data using a SQL syntax. [Query it](#)
- INFRASTRUCTURE**: Infrastructure. Identify problems in real time by monitoring metrics and logs for common servers, containers, and services. [Jump in](#)

What's others?

セキュリティ、アラート、機械学習など

Spaces

Basic (free) / Gold

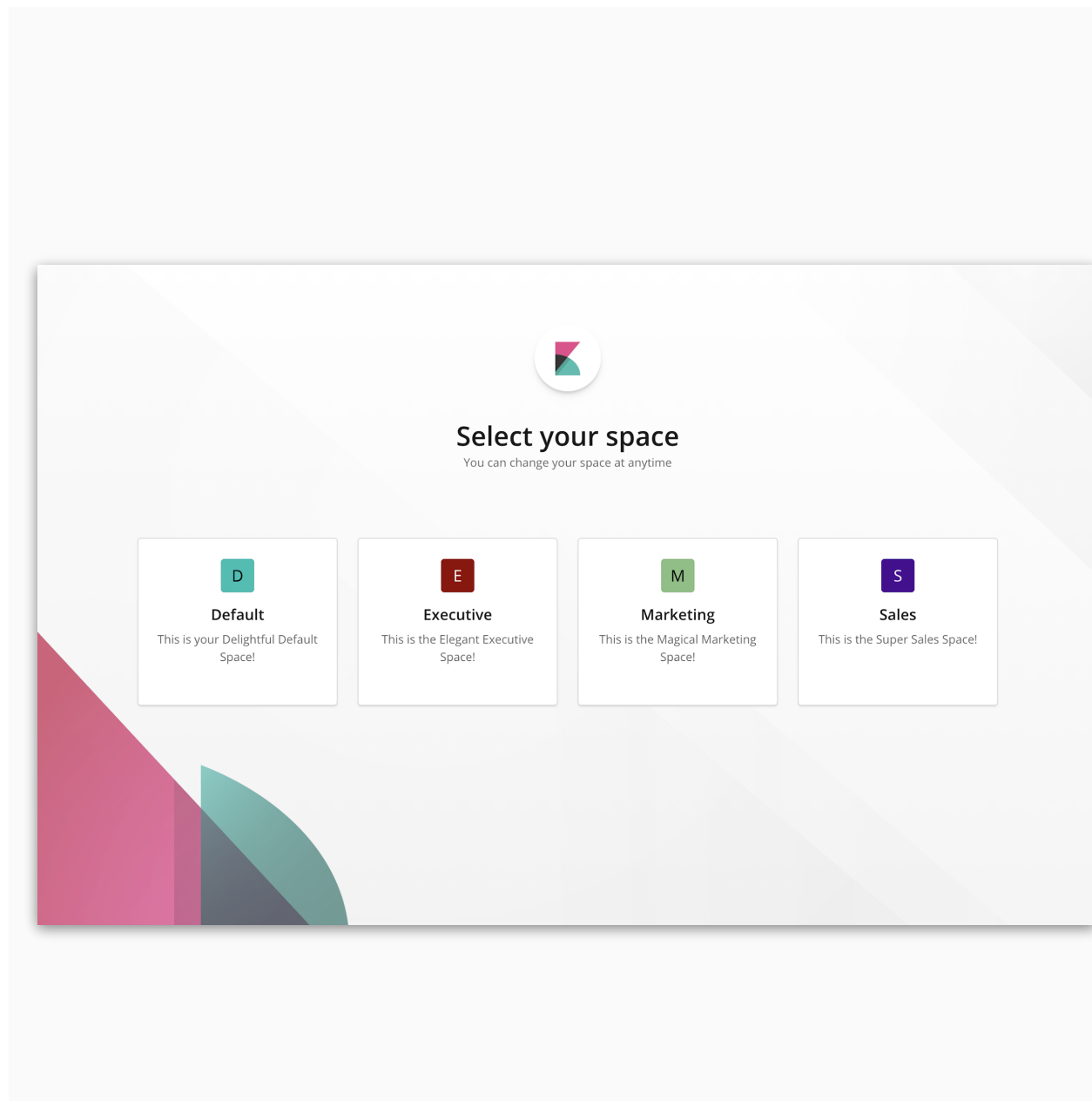
個別のスペースでグラフやダッシュボードを管理

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

Customize feature display (18 / 19 features visible) [hide](#)

Control which features are visible in this space.

The feature is hidden in the UI, but is not disabled.

Want to secure access? Go to [Roles](#).

Feature	Show? (change all)
Discover	<input checked="" type="checkbox"/>
Visualize	<input checked="" type="checkbox"/>
Dashboard	<input checked="" type="checkbox"/>
Dev Tools	<input type="checkbox"/>
Advanced Settings	<input checked="" type="checkbox"/>
Index Pattern Management	<input checked="" type="checkbox"/>
Saved Objects Management	<input checked="" type="checkbox"/>
Timelion	<input checked="" type="checkbox"/>
Graph	<input checked="" type="checkbox"/>
Stack Monitoring	<input checked="" type="checkbox"/>
Machine Learning	<input checked="" type="checkbox"/>
APM	<input checked="" type="checkbox"/>

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

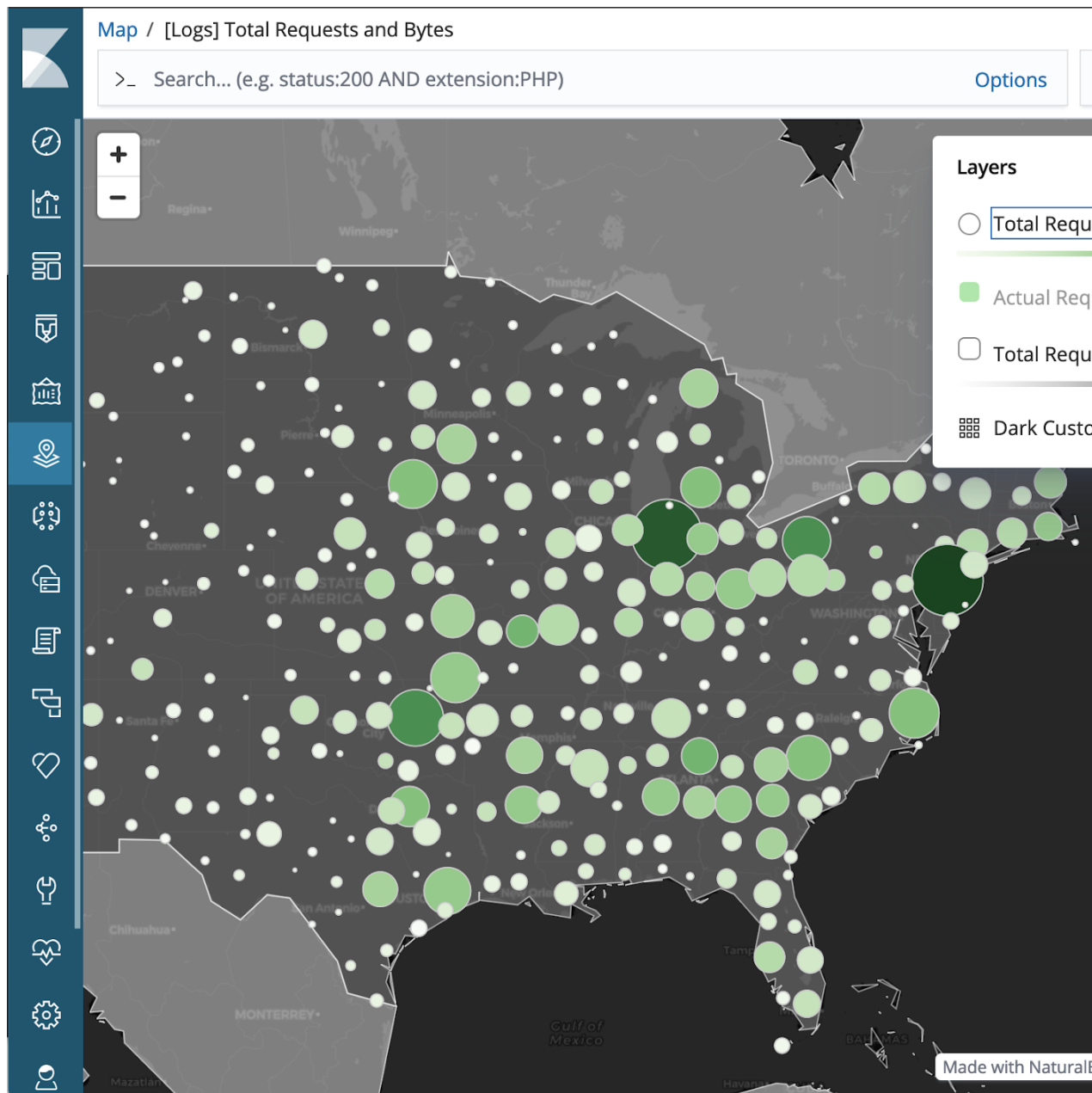
`geo_points` と `geo_shapes` 両方を Map上にそのまま表示可能

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 (dmccryptの利用)

その他にも (監査ログ、IP フィルタ...)

The screenshot shows the Kibana Security Roles configuration interface. The breadcrumb path is "Management / Security / Roles". The current page is "Users Roles". The role being configured is "coffeindex_writer".

Cluster Privileges:

- all
- monitor
- manage
- manage_security
- manage_index_templates
- manage_pipeline
- manage_ingest_pipelines
- transport_client
- manage_ml
- monitor_ml
- manage_watcher
- monitor_watcher

Kibana Privileges:

- all
- read

Run As Privileges:

Add a user...

Index Privileges:

Indices: elasticcoffee x

Privileges: write x create_index x

Granted Documents Query Optional

Granted Fields Optional

Buttons: Save, Cancel, +

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

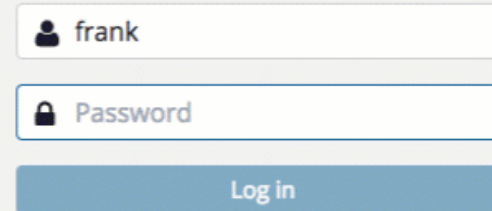
Kibanaのスペースとの統合

暗号化

通信 (TLS & SSL)

データ (dmccryptの利用)

その他にも (監査ログ、IP フィルタ...)



frank

Password

Log in



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

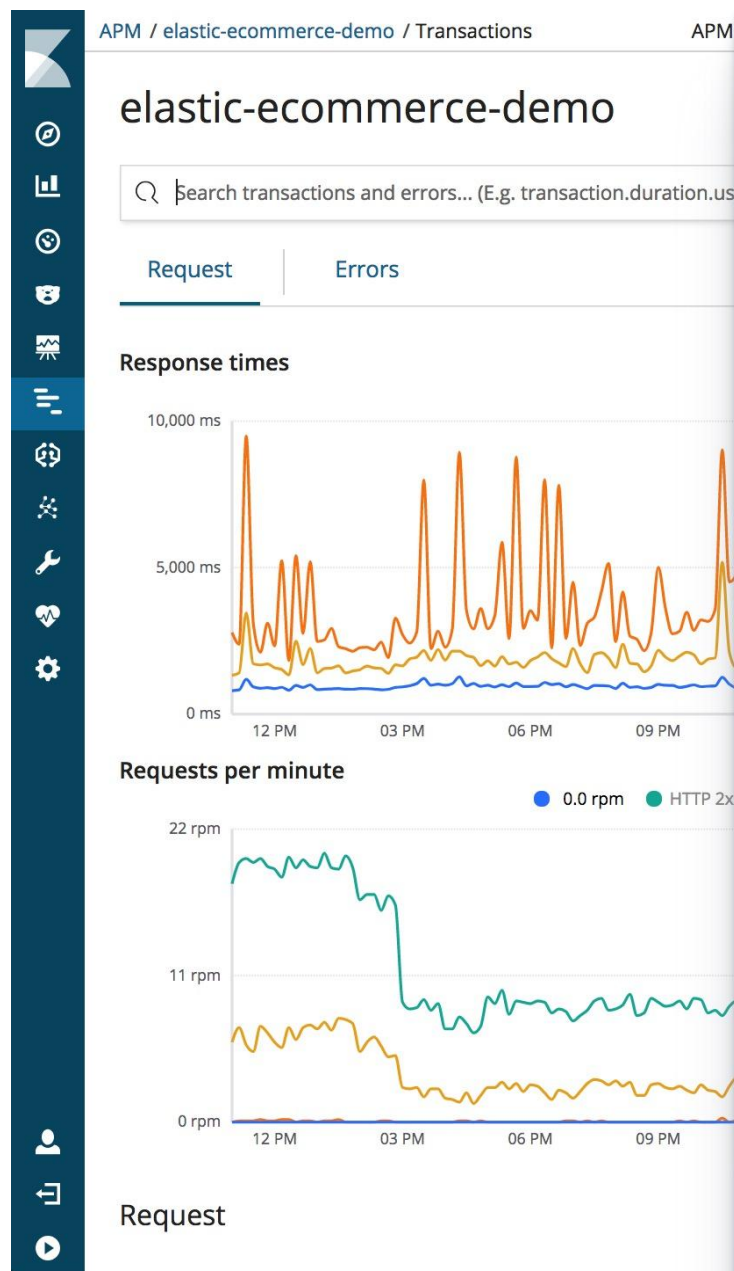
多くのユースケース

ITオペレーション

セキュリティ分析

ビジネスKPI

APM



Enable anomaly detection on response times

BETA

This integration will start a new Machine Learning job that is predefined to calculate anomaly scores on response times on APM transactions. Once enabled, the response time graph will show the expected bounds from the Machine Learning job and annotate the graph once the anomaly score is ≥ 75 .

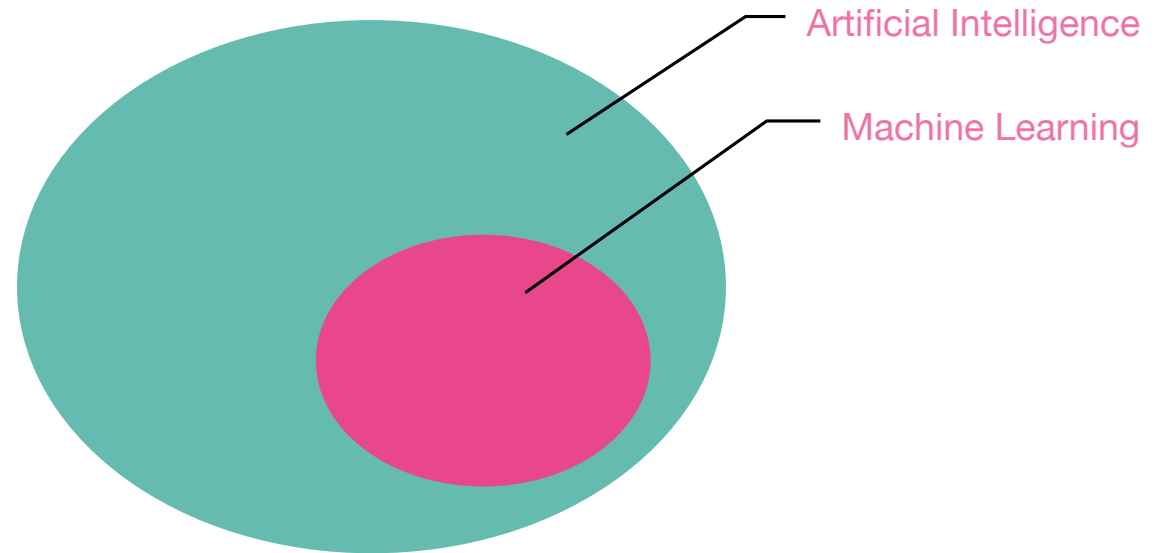
Jobs can be created per transaction type and based on the average response time. Once a job is created, you can manage it and see more details in the [Machine Learning jobs management page](#). It might take some time for the job to calculate the results. Please refresh the graph a few minutes after creating the job.

Create new job

What's Machine Learning?

- **Algorithms that**

- Learn from Data
- Using Statistical Techniques
- Without Explicit Programming



Elastic Machine Learning Scope

Image Classification **Recommendations**

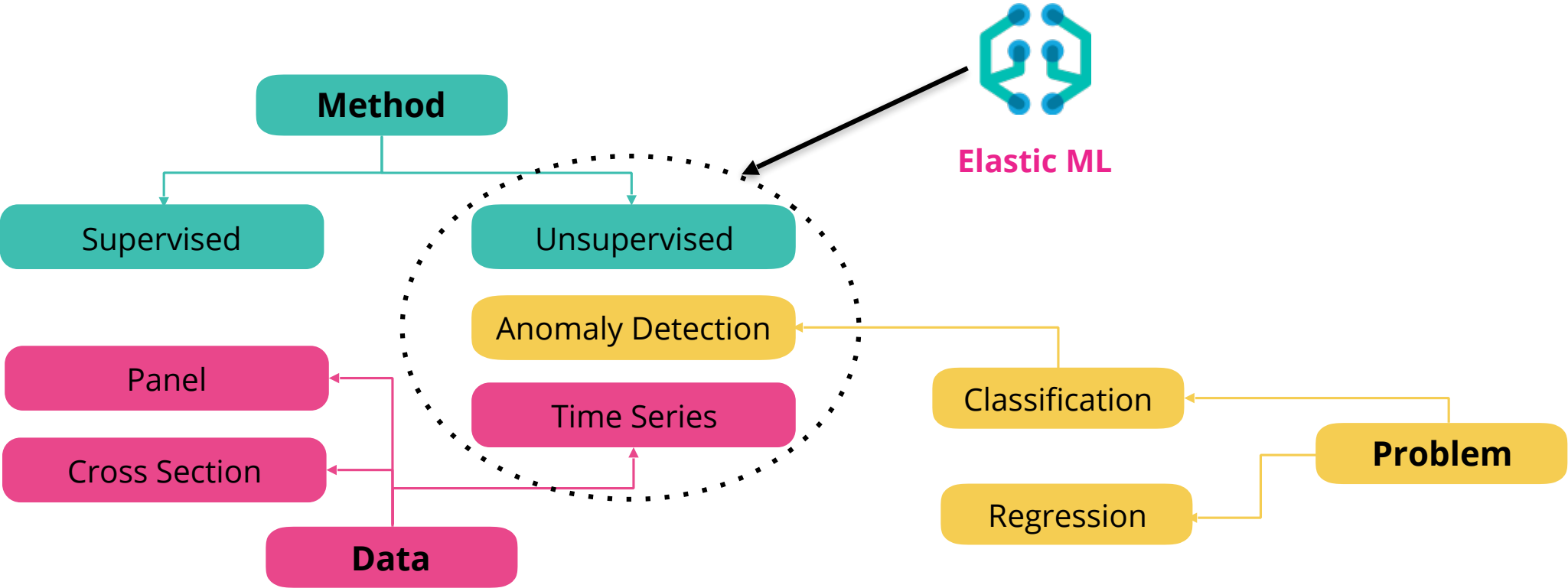
Autonomous cars Voice Recognition Predictive Medicine

Fraud detection **Anomaly Detection**

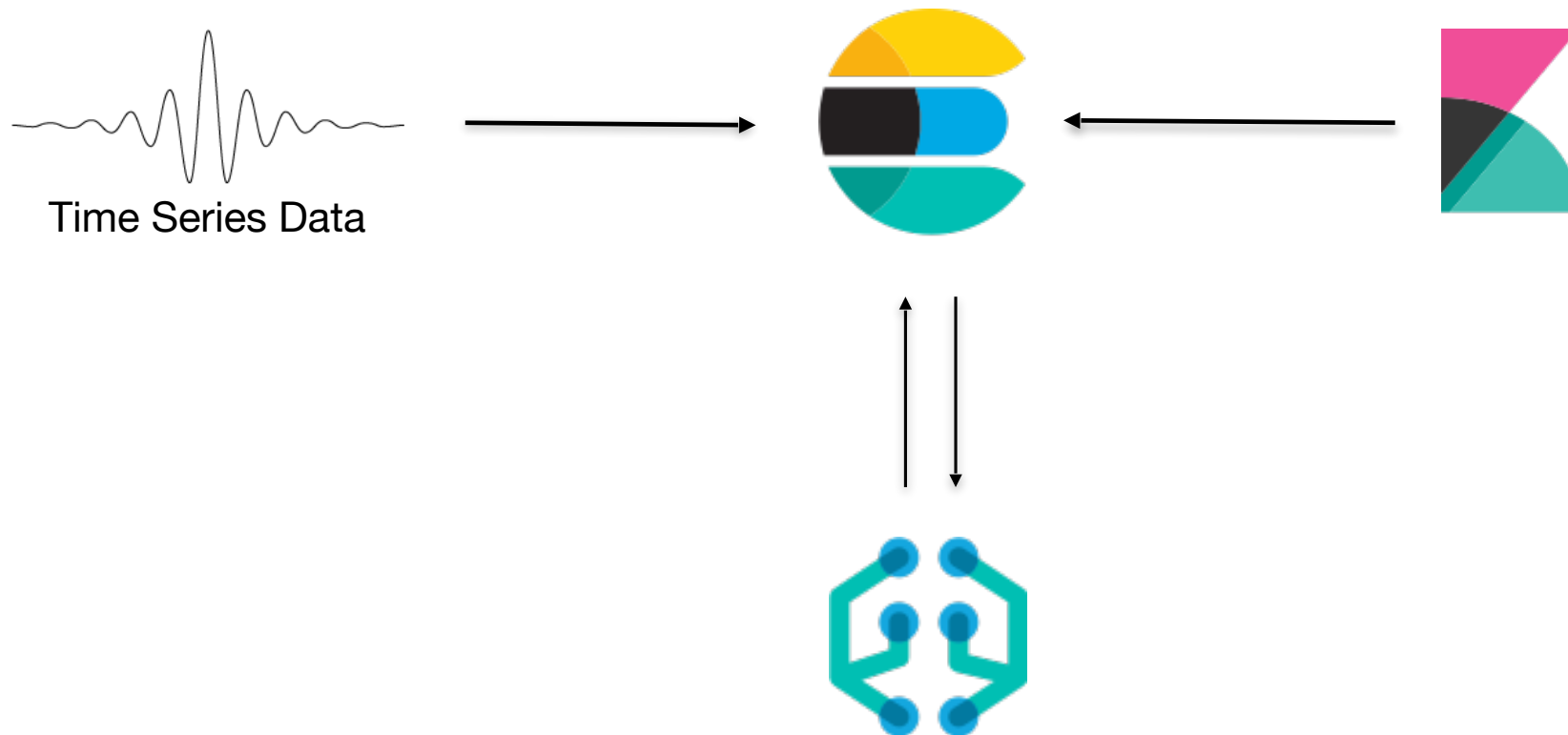
Learn to Rank Speech Recognition

Language Translation **Entity Resolution**

Elastic 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**

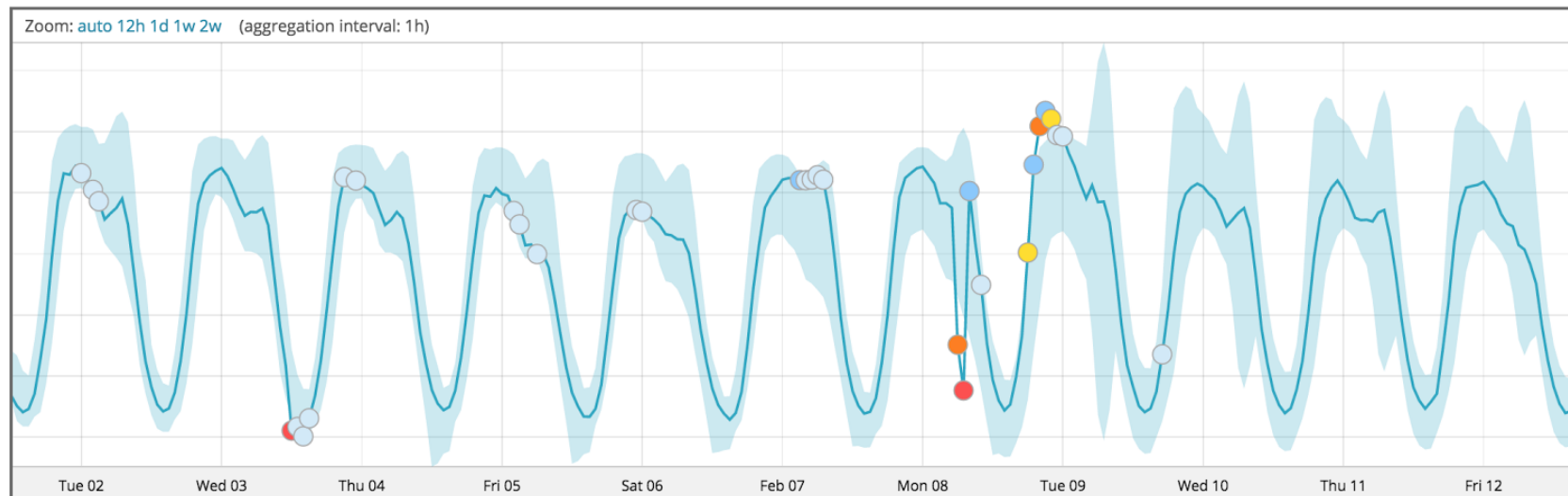
- Do I have systems that are compromised with malware?
- Which users could be an insider threat?

- **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?

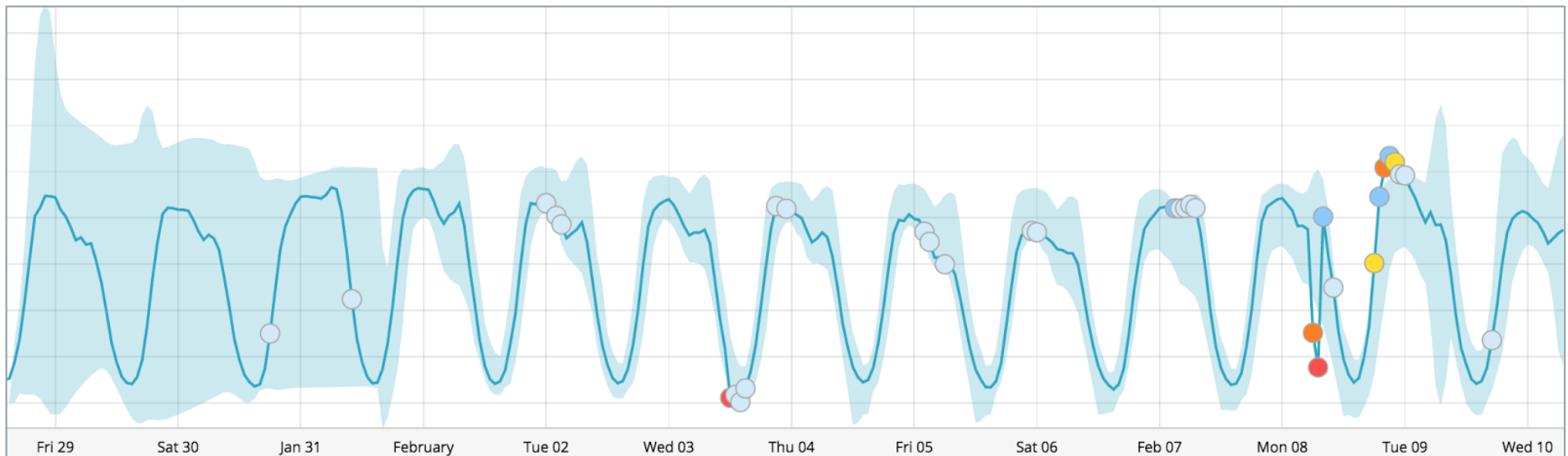
Elastic Machine Learning

- 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



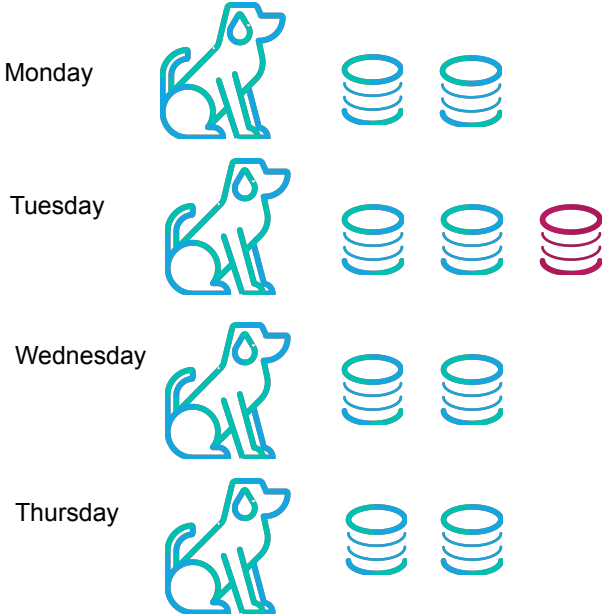
Elastic Machine Learning

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

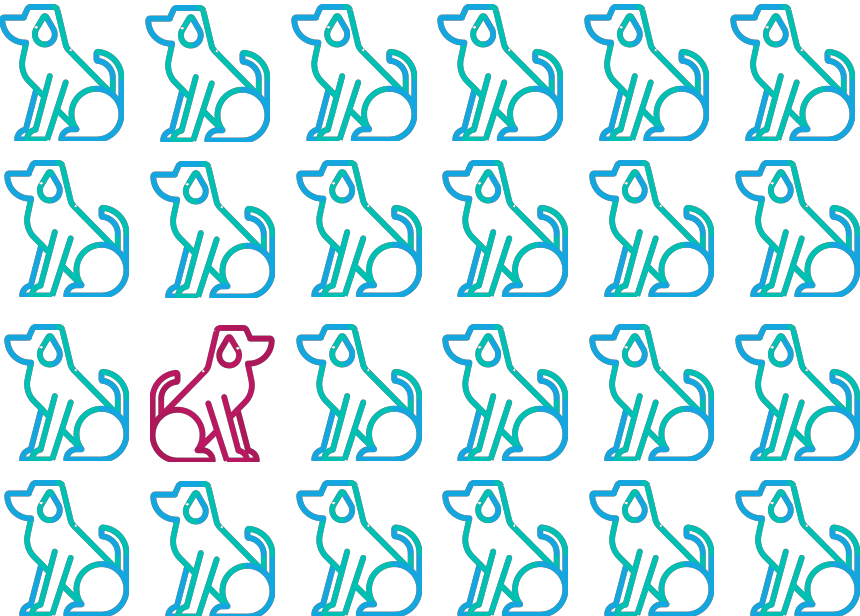


Population Analysis / Entity Behavior Analytics with ML

When something behaves like itself



When something behaves like its peers



The advantages of anomaly-driven alerting



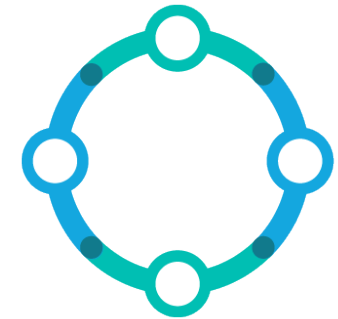
**Understand
Seasonality**



**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



apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

Name

apm-high-load-opbeans

Indices to query

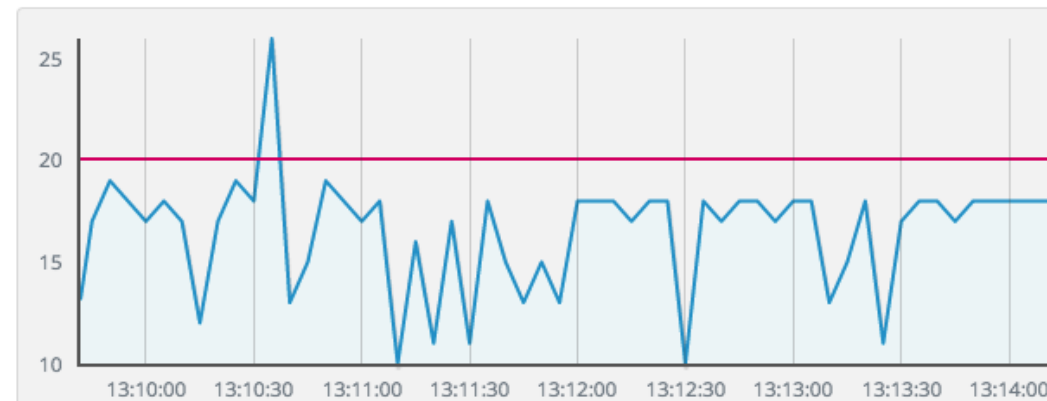
apm-*-transaction-* ✕

Use * to broaden your search query

Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

context.service.name (1 of 4): opbeans-node



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



apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

Name

apm-high-load-opbeans

Indices to query

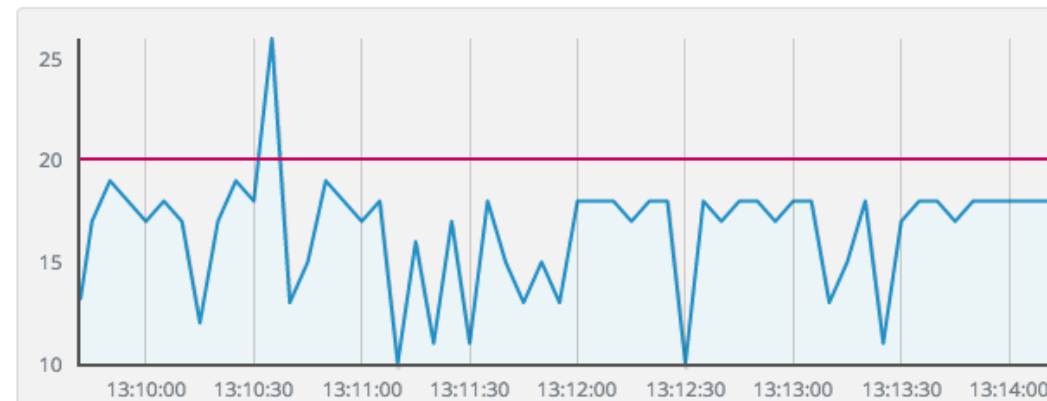
apm-*-transaction-* ✕

Use * to broaden your search query

Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

context.service.name (1 of 4): opbeans-node



Alert Users to Conditions

Host Behavior

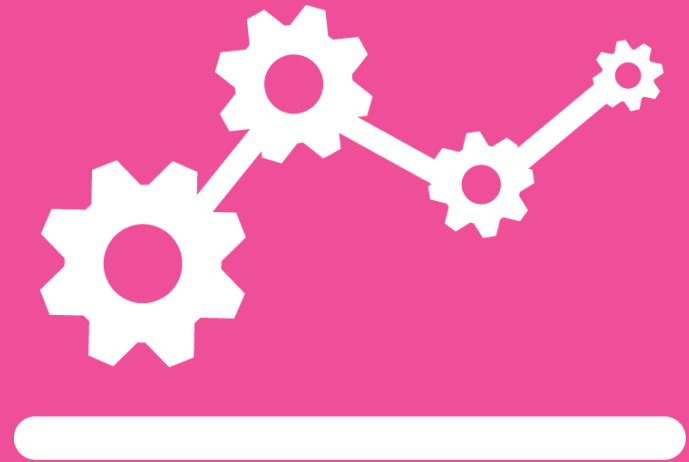
- Free disk space goes below 5%
- Process X starts on any server

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

Create a new threshold alert
Send out an alert when specific conditions are met. This will run once every 1 minute.

Name
CPU Utilization

Select an Index **Select a time field** **Run this watch every**

metricbeat-* x @timestamp 1 minutes

Broad searches can be done by adding * to your query

Matching the following condition

WHEN average() OF system.cpu.user.pct OVER all documents IS ABOVE 100 FOR THE LAST 5 minutes

Your index and condition combo did not return any data.

- E-mail
Disabled. Configure elasticsearch.yml.
- Logging
Add a new item to the logs.
- Slack
Send a message to a slack user or channel.

Add new action

Will perform 0 actions once met

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

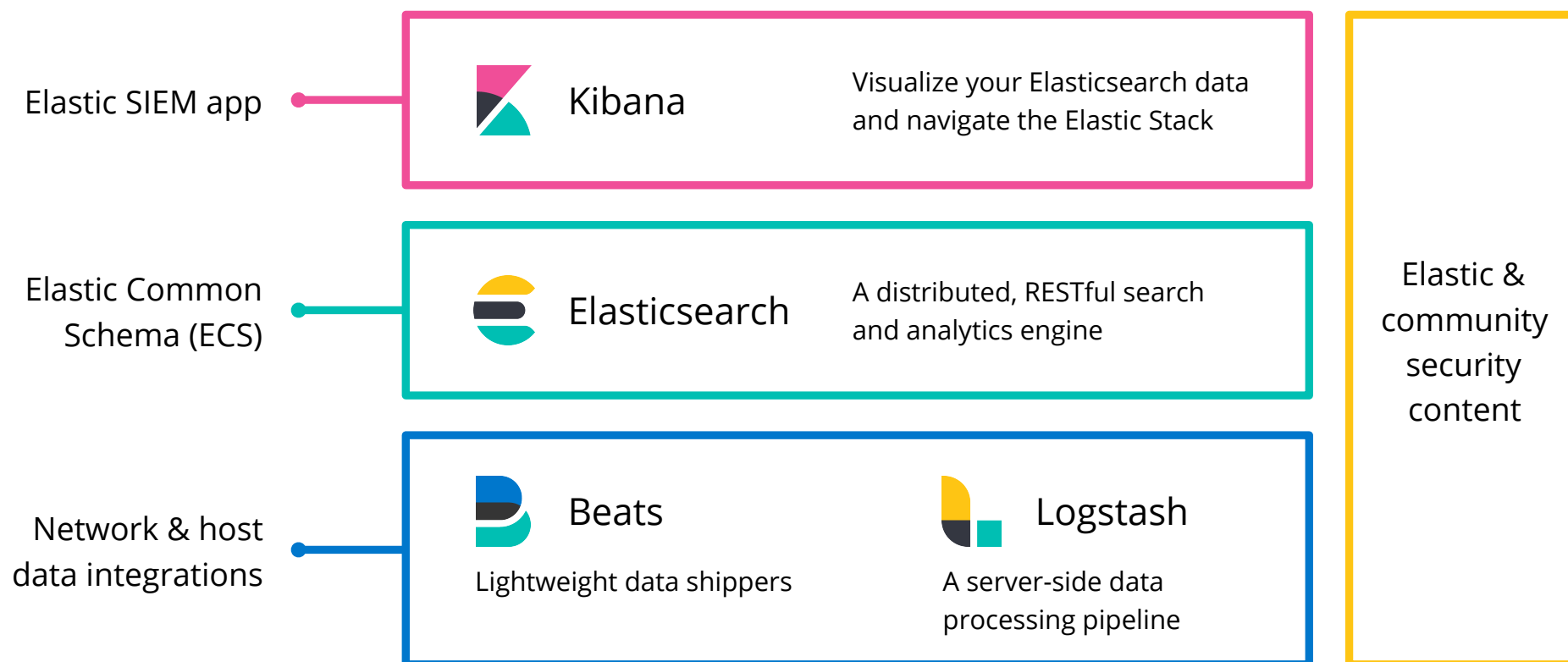
Rapid event triage and investigation





Elastic SIEM

A SIEM for Elastic Stack users everywhere



Elastic SIEM app (beta)

Triage and qualify security alerts
at the speed of thought

Analyst-friendly experience for investigating security alerts

Time-ordered events

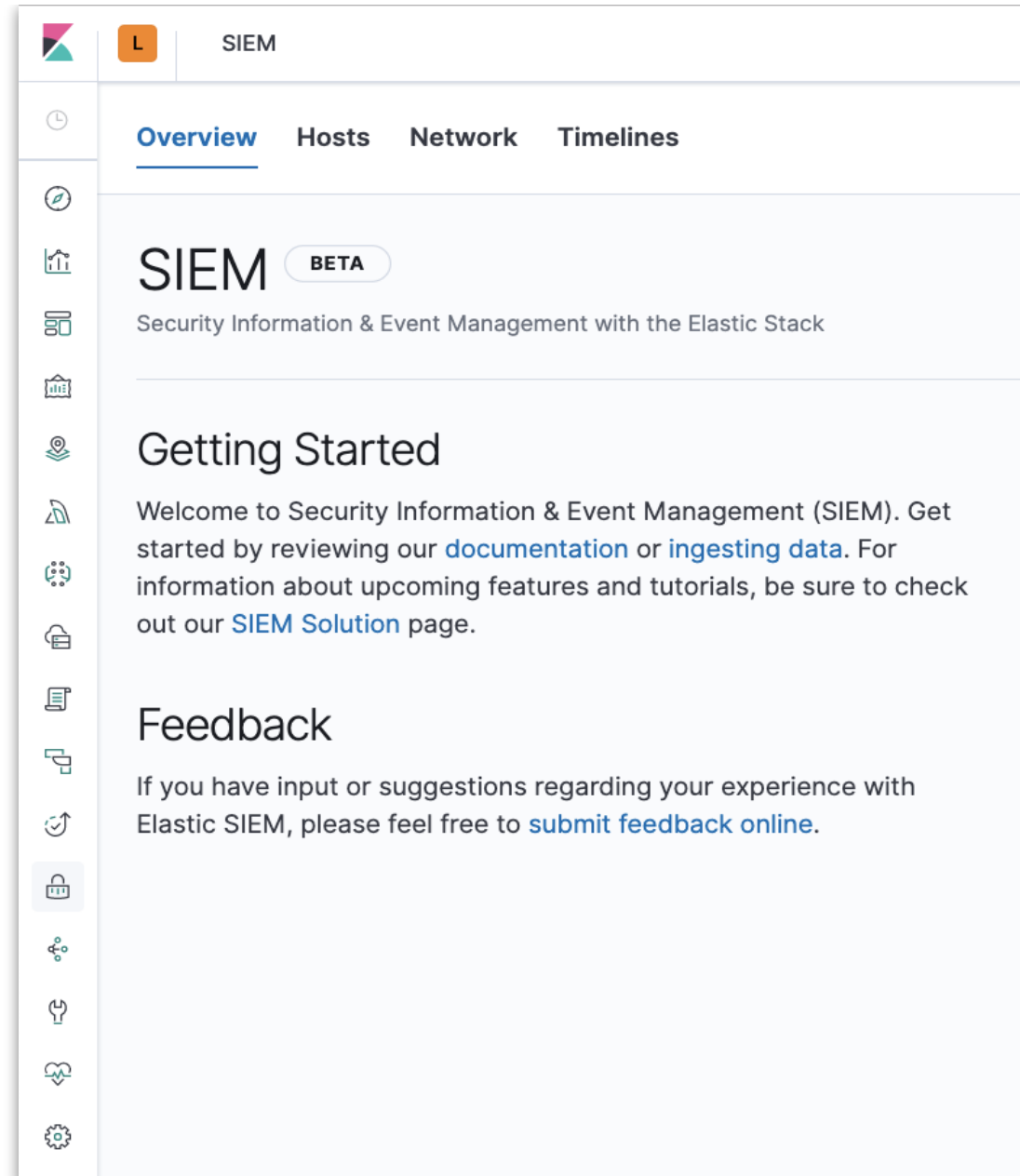
Drag-and-drop filtering

Multi-index search

Annotations, comments

Formatted event views

Persistent forensic data storage



The screenshot displays the Elastic SIEM app interface. At the top, there is a navigation bar with a logo, a user profile icon labeled 'L', and the text 'SIEM'. Below this is a secondary navigation bar with tabs for 'Overview', 'Hosts', 'Network', and 'Timelines'. The main content area features a large heading 'SIEM' with a 'BETA' badge, followed by the subtitle 'Security Information & Event Management with the Elastic Stack'. A section titled 'Getting Started' contains a welcome message and links to 'documentation' and 'ingesting data'. Below this is a 'Feedback' section with a link to 'submit feedback online'. A vertical sidebar on the left contains various icons for navigation and settings.

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

Source index filebeat-nginx-2019.02.05 showing 5 of 40 fields

@timestamp ↑	agent.type	http.response.body.bytes	http.response.status_co...	source.ip
January 9th 2019, 07:27:50	filebeat	410	200	35.224.108.130
January 9th 2019, 07:28:09	filebeat	410	200	35.224.108.130
January 9th 2019, 07:28:50	filebeat	410	200	35.224.108.130
January 9th 2019, 07:28:53	filebeat	410	200	35.224.28.11
January 9th 2019, 07:29:28	filebeat	319	200	185.246.208.82

Rows per page: 5

Data frame pivot preview

source.ip ↑	http.response.body.bytes.avg
1.2.241.97	194
1.214.221.2	194
14.102.189.231	194
14.139.184.212	166.4
18.228.119.52	171

Rows per page: 5



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

