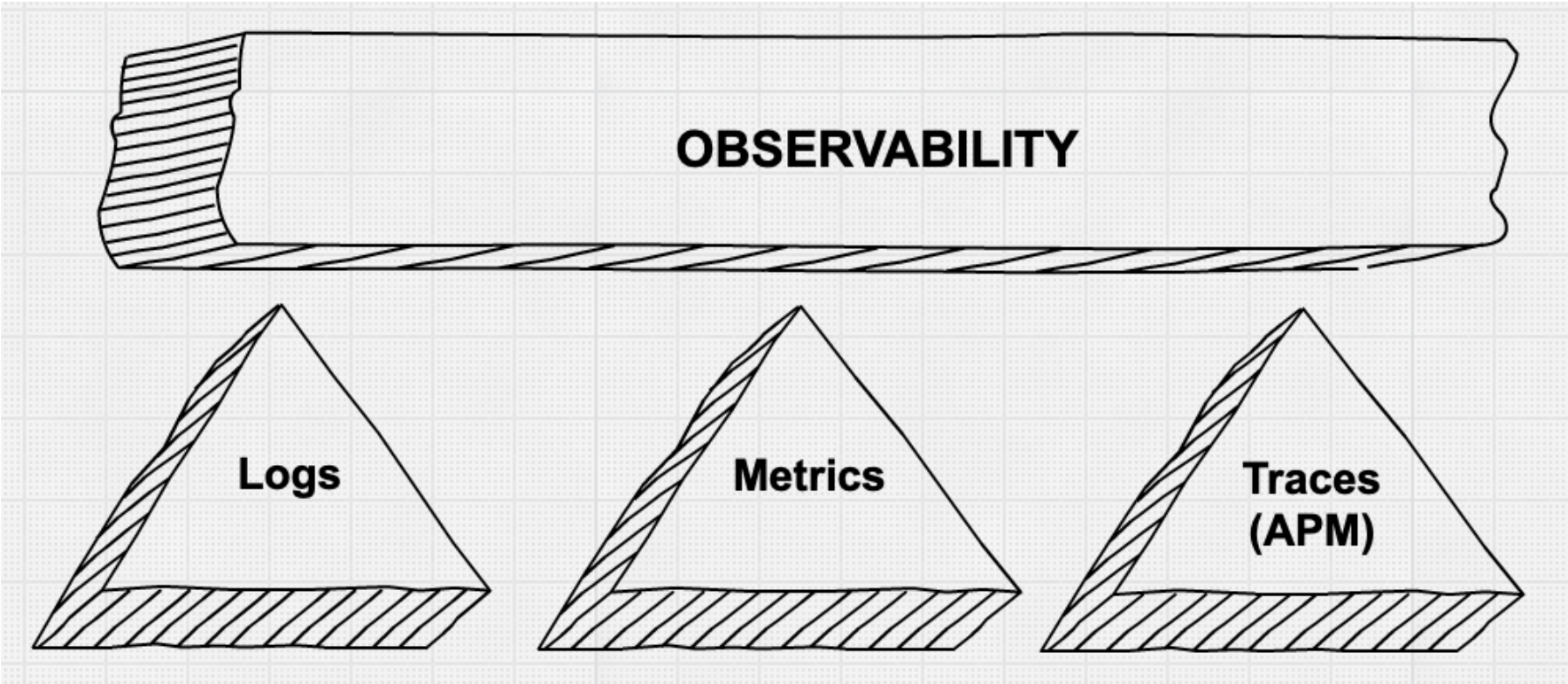
Elastic Stackで始めるアプリケーション監視

Jun Ohtani, Community Advocate
2019/10/04

about

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

Observability



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

elastic

Kibana、ログだけじゃないし
監視系の話もできないとなぁ

elastic

これだ！

（インスパイアされてみました）

アジェンダ

- 監視とは？
- Elastic Stackとは？
- 様々な観点からのアプリケーションの監視
- さらに色々試してみるには？

監視とは？


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

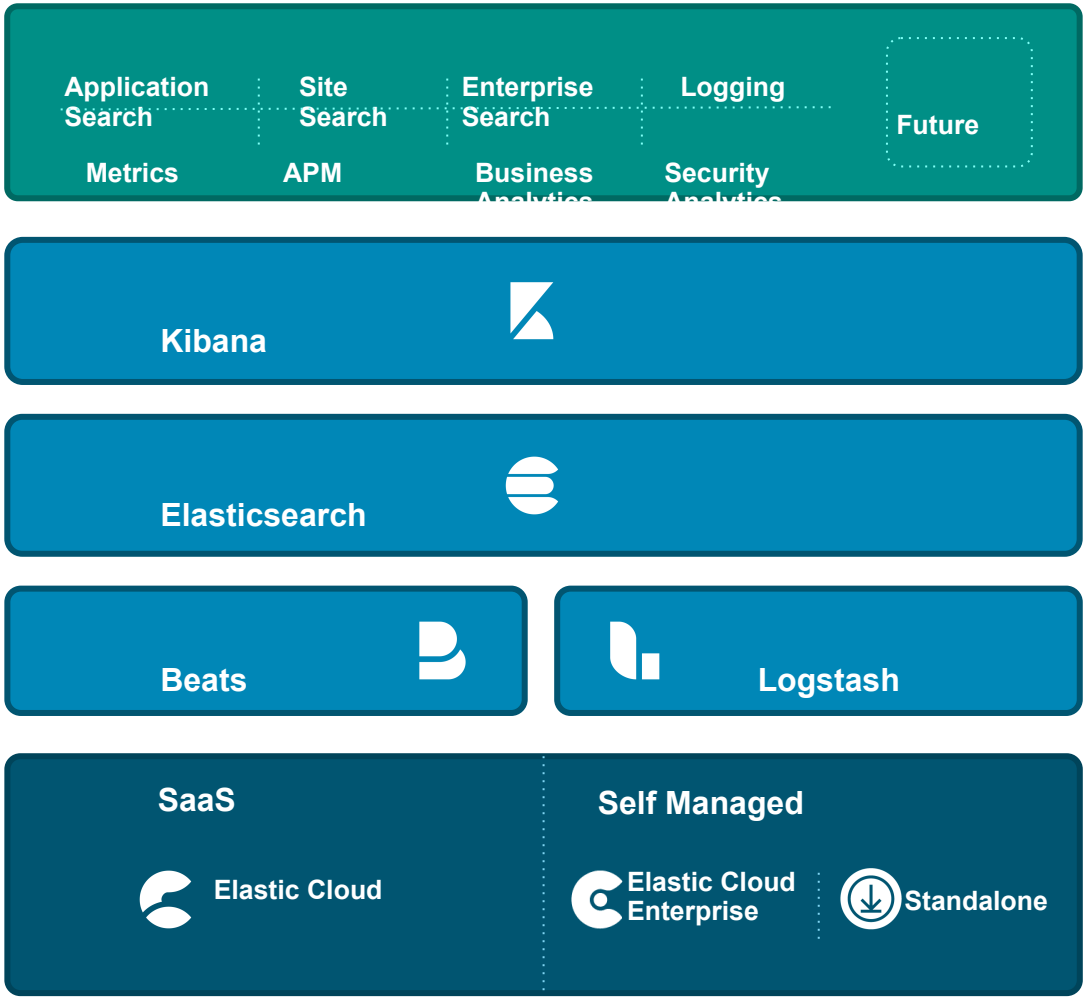
elastic

マイクロサービス？？？

elastic

Elastic Stackとは？

Elastic Stack



ソリューション

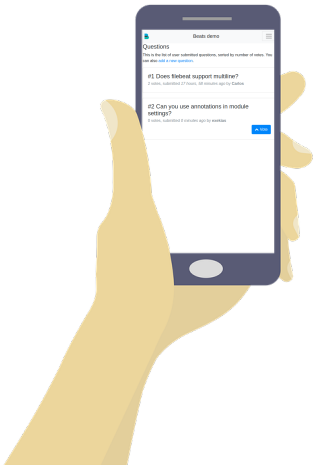
可視化、管理

保存、検索、分析

インジェスト

デプロイ

デモサイト



GCEインスタンス

NGINX

APM Ruby

Filebeat

Metricbeat

Packetbeat

Auditbeat

GCEインスタンス

Heartbeat

Filebeat

Metricbeat

Packetbeat

Auditbeat

elastic

デモサイト

https://www.johtani.dev

アプリケーションの監視ポイント

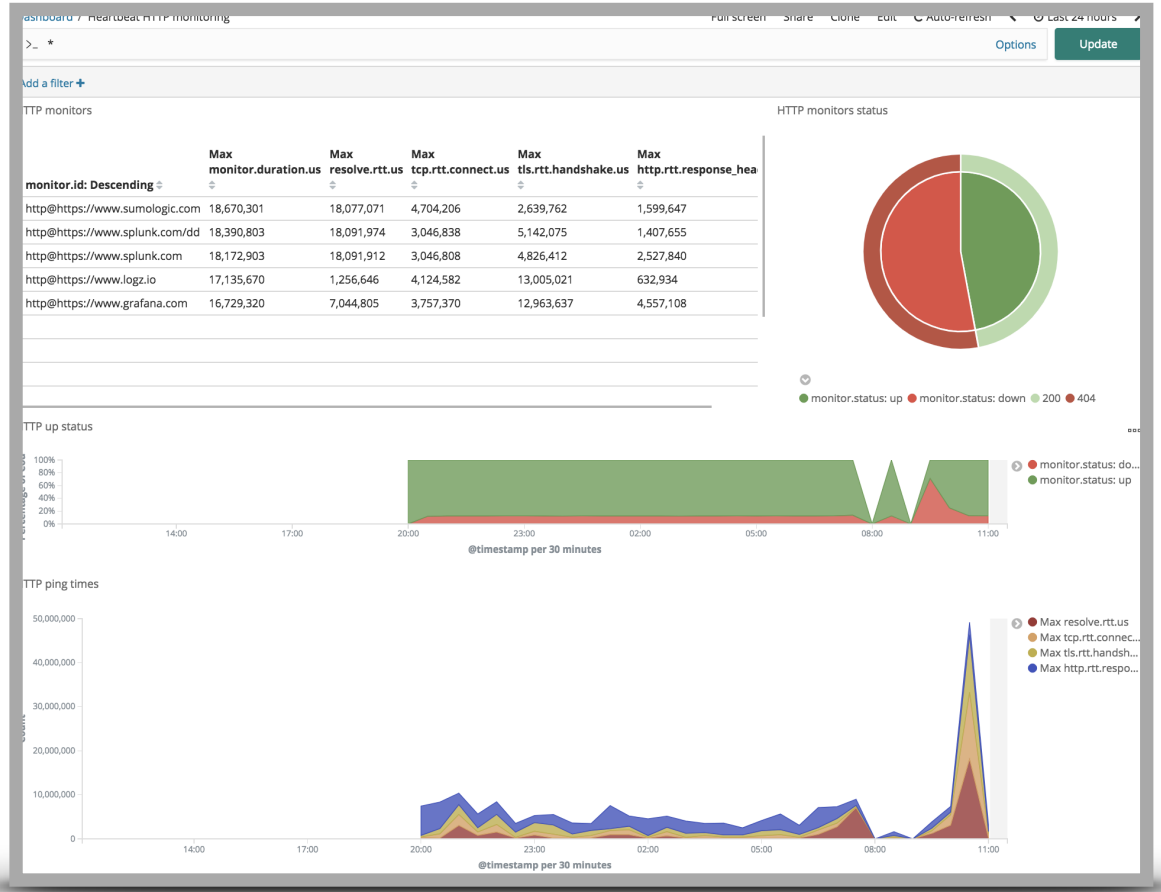
elastic

監視ポイント

- 外形監視
- メトリック（メトリクス）
  - サーバー、アプリケーション
- ログ
- アプリケーションのリリースタイミング
- 分散トレーシング

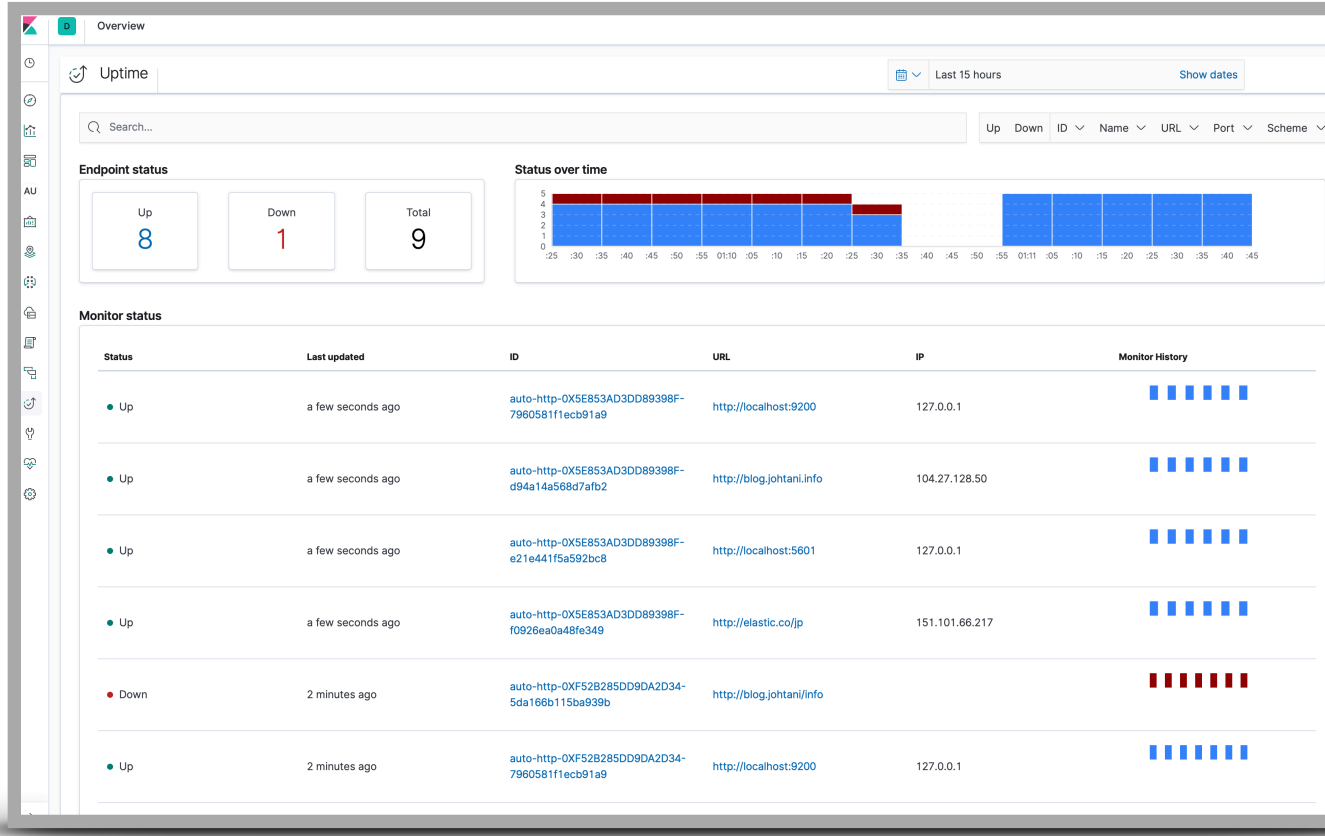
Heartbeat

Lightweight Shipper for Uptime Monitoring



Uptime UI

Dedicated Uptime Monitoring UI for Kibana



Metricbeat

lots of **modules**


System


Apache


Docker

NGINX


HAProxy


Kafka


MongoDB

MySQL


PostgreSQL


Prometheus


Jolokia

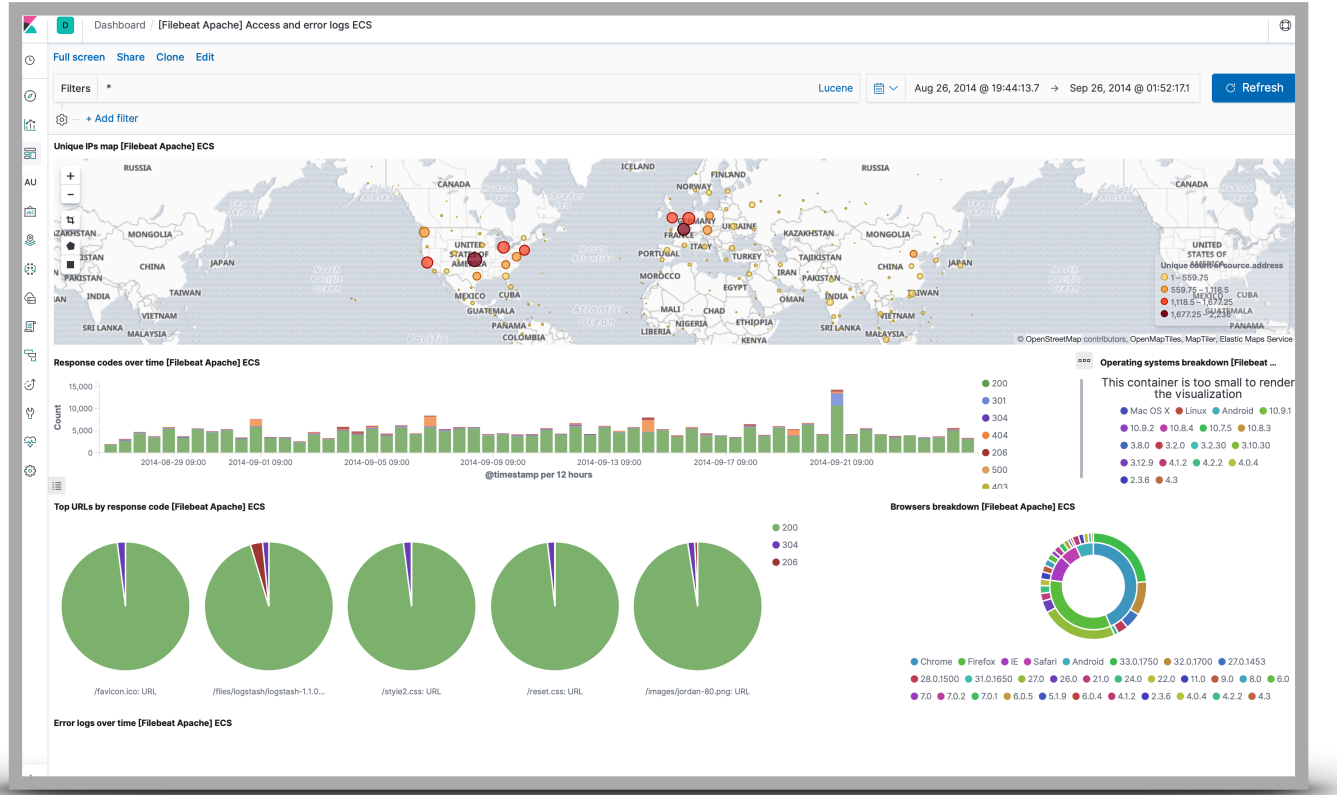

Add your own

Metricbeat モジュール

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

Filebeat

tail log from **file**



Filebeat

many **modules**

Apache

Nginx

Auditd

MySQL

Filebeat modules - v7.0.0

Apache module

Auditd module

Elasticsearch module

haproxy module

Icinga module

IIS module

Iptables module

Kafka module

Kibana module

Logstash module

MongoDB module

MySQL module

Nginx module

Osquery module

PostgreSQL module

Redis module

Santa module

Suricata module

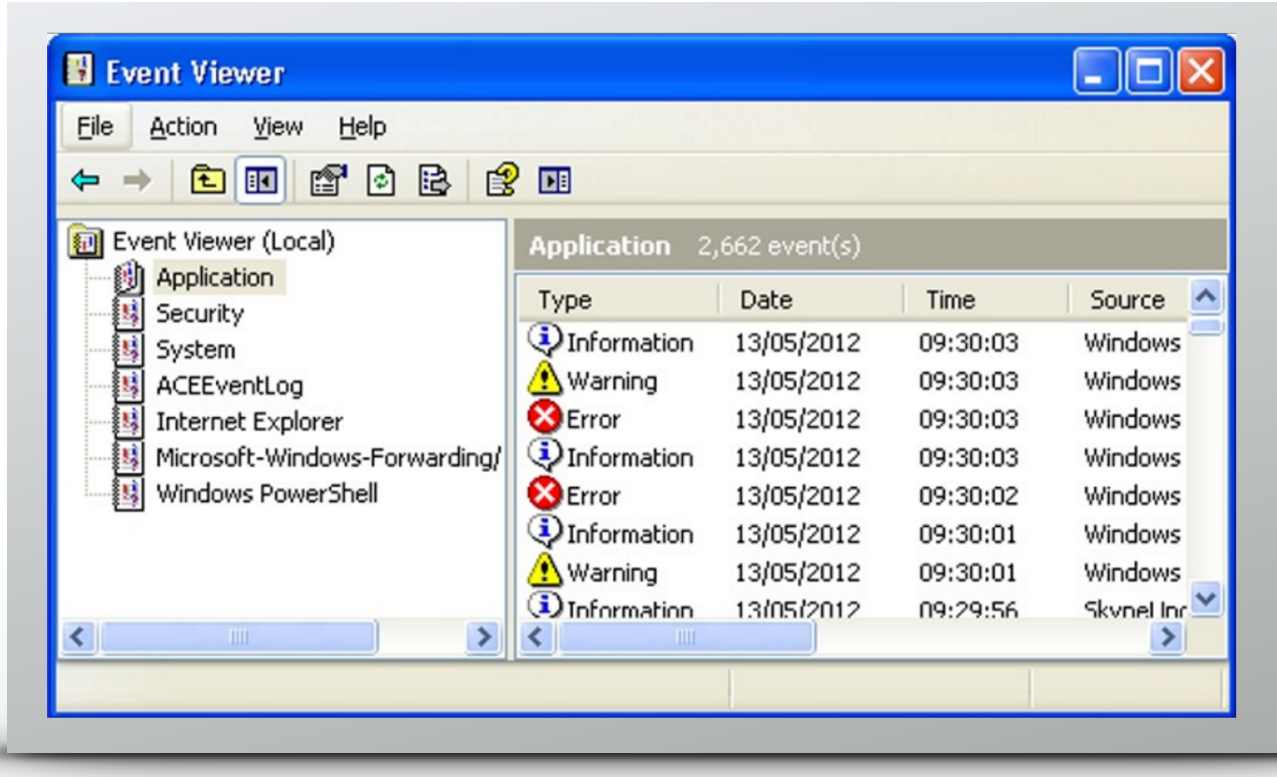
System module

Traefik module

Zeek (Bro) Module

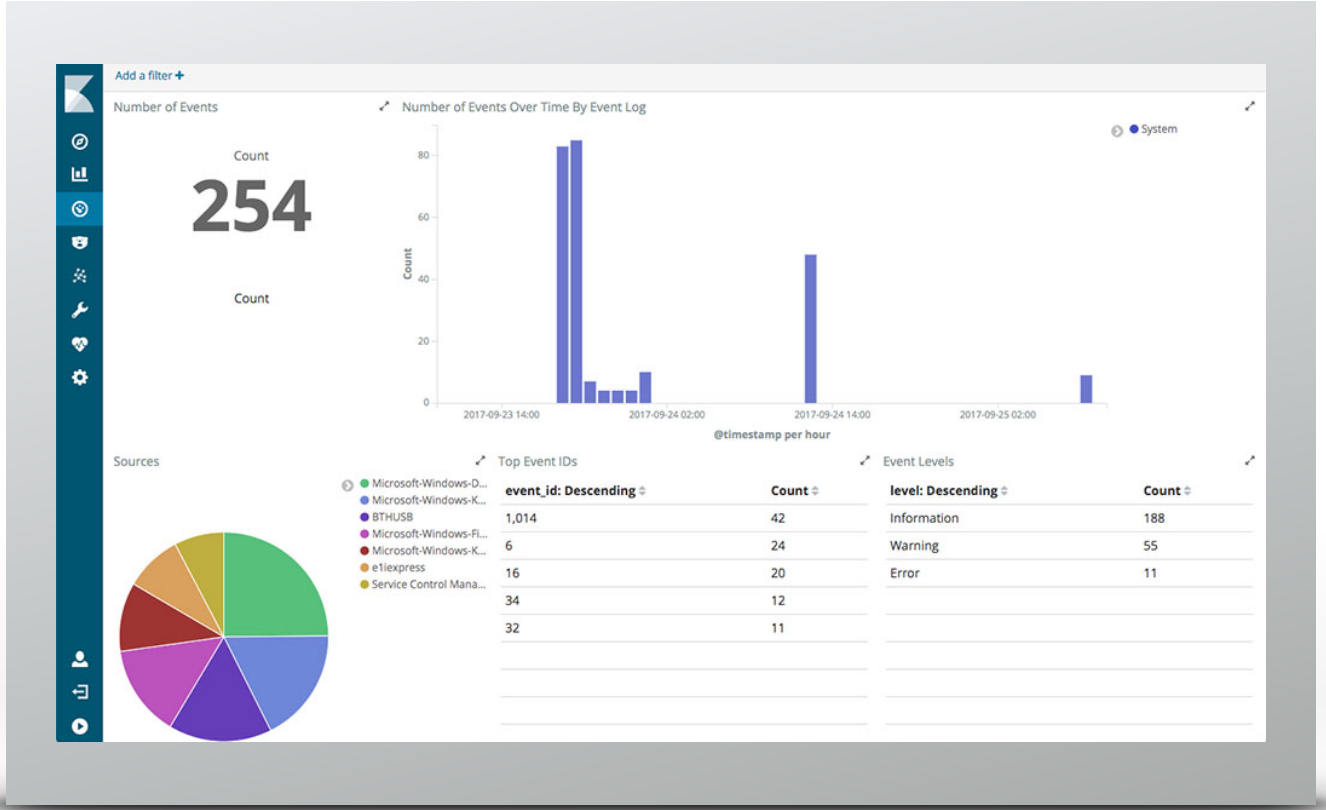
winlogbeat

Welcome to **1998**



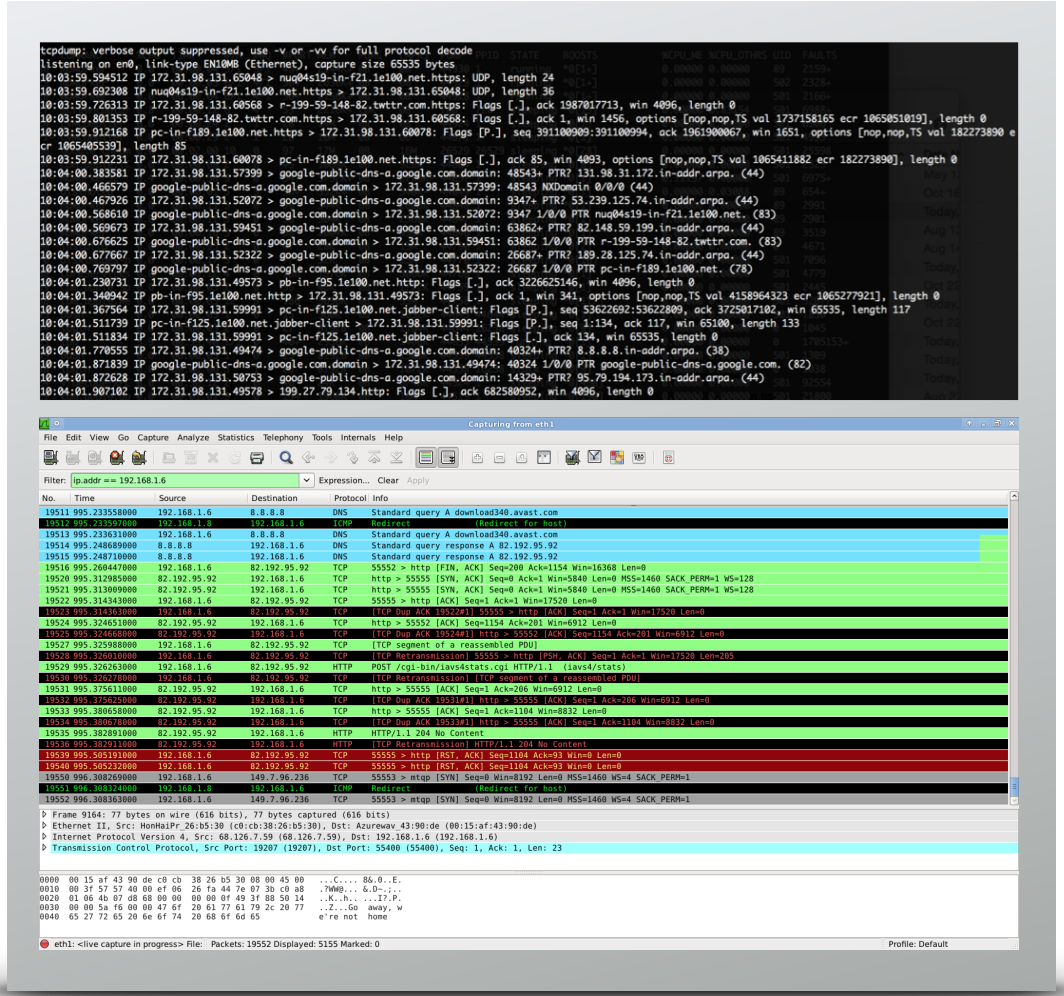
winlogbeat

Now



Packetbeat

Capture the **Packet**



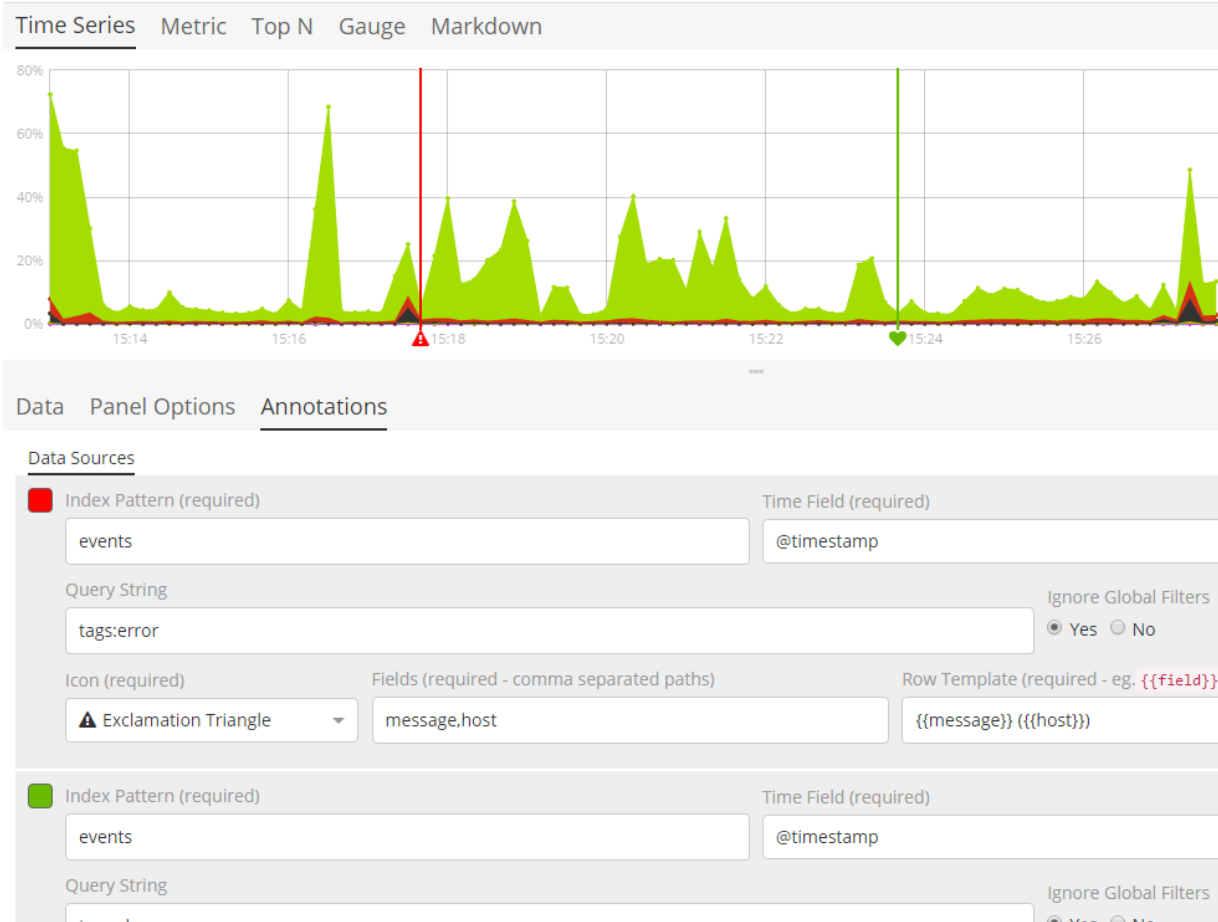
Capture the **Packet**

アプリケーションのリリースタイミング

- バグフィックスリリース
- 新機能リリース
- 新サービス開始
- サーバー増強

Time Series Visual Builder

Annotations on Visualization

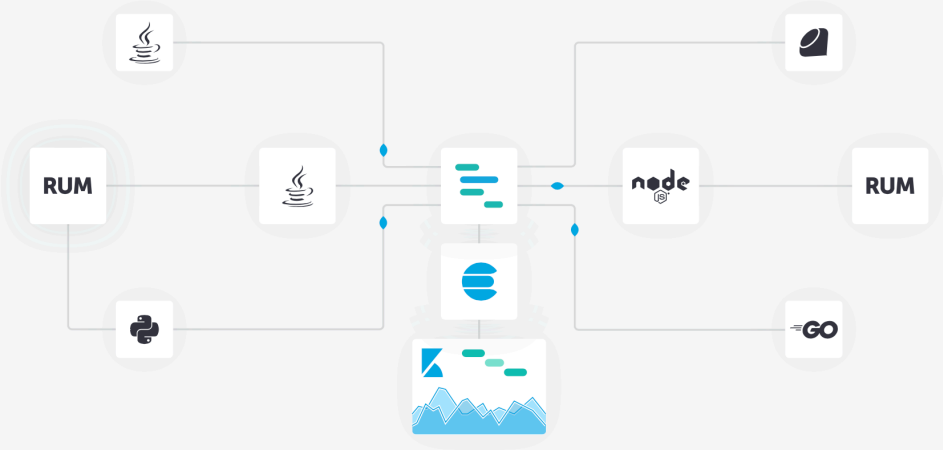


分散トレーシング

- マイクロサービス
- 1つのリクエストに対して複数のプロセスが関係
- アプリケーションパフォーマンスモニタリングの1つ

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

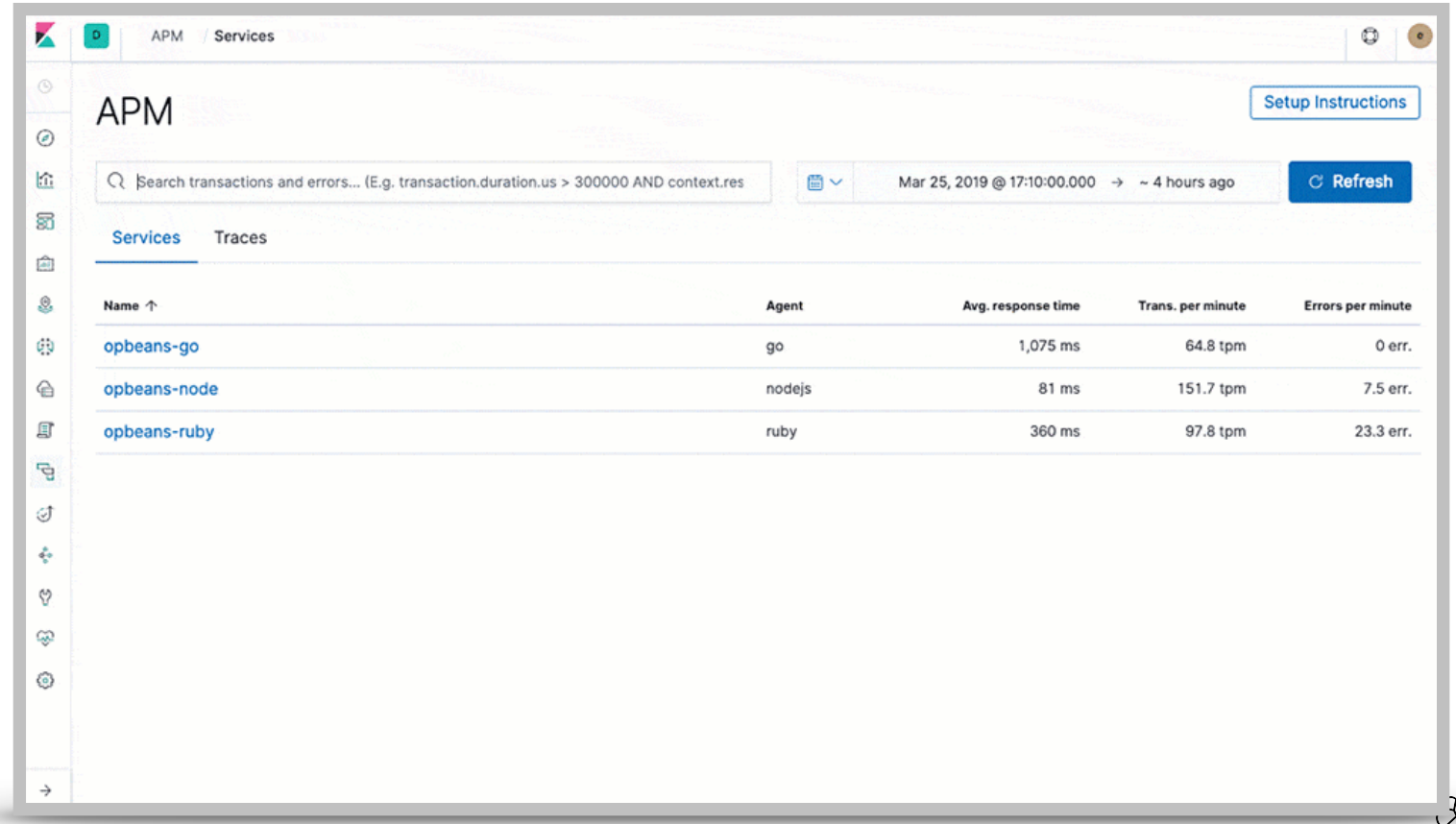
検索 + APM

サポート言語

- Node.js
- Python
- Ruby
- Go
- Java
- .NET

- RUM - Real User Monitoring JavaScript Agent

Elastic APM



elastic

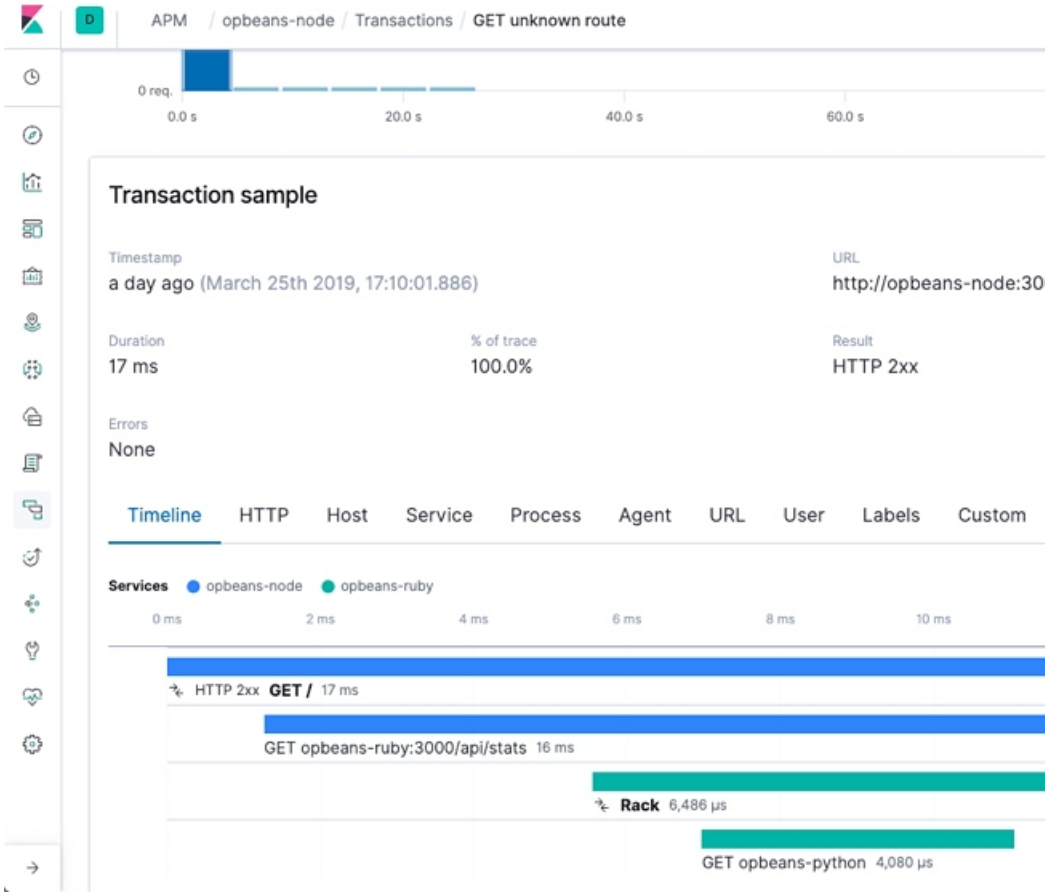
Distributed Tracing

Beta I Basic (free)

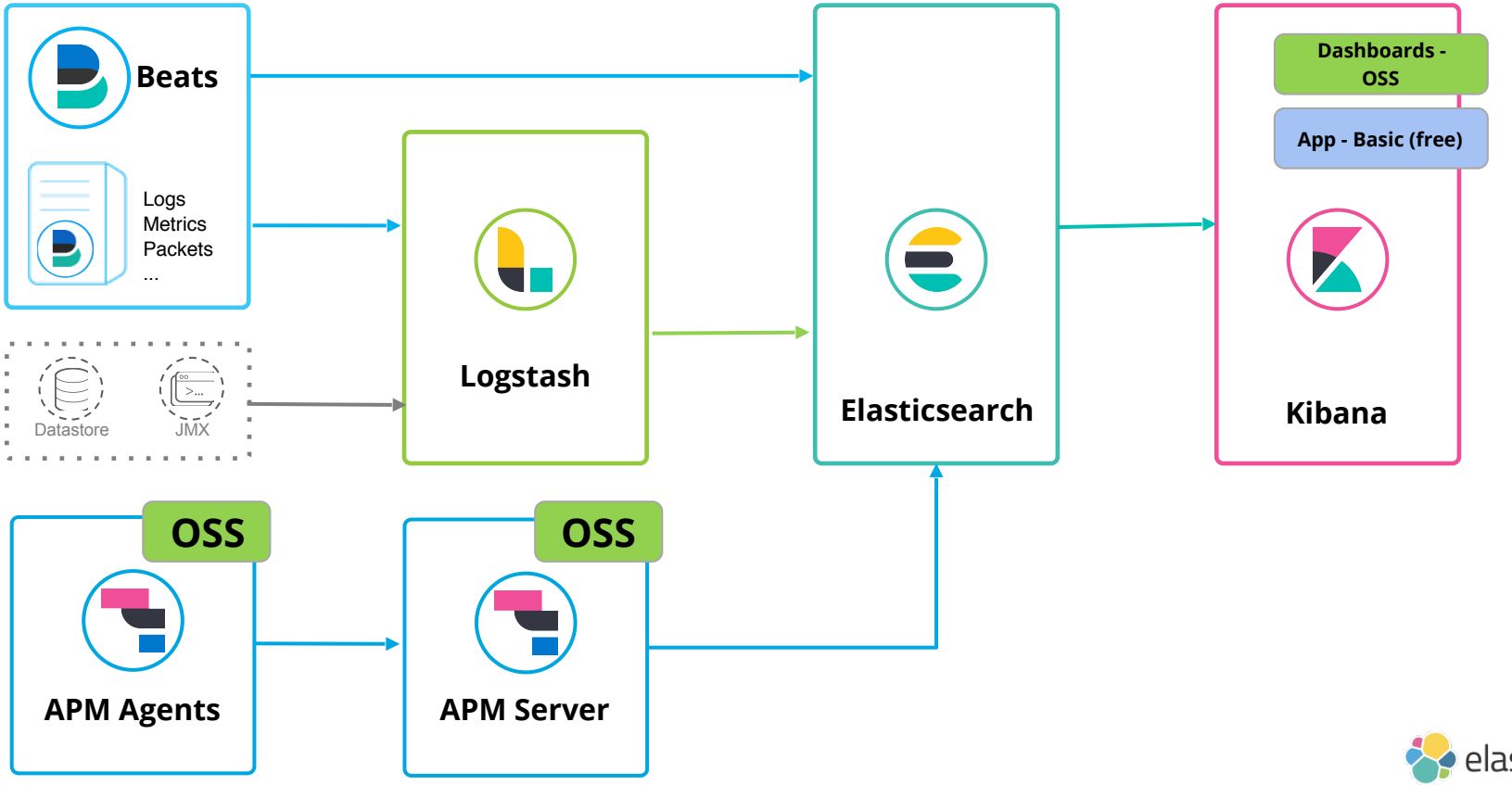
全ての計測されたサービスを見るための
統合されたビュー

サブコンテキスト内のトレースに遷移

OpenTracing 互換



Deployment



elastic

APM Ruby Agent

Framework Support

- Ruby on Rails >= 4.x
- Sinatra and Rack compatible frameworks

APM Ruby Agent with Rails

How to use with Rails

- Add elastic-apm gem in Gemfile

```
gem 'elastic-apm'
```

- Create elastic_apm.yml file under config dir

```
server_url: http://localhost:8200
secret_token: ''
```

- See reference for other configurations
https://www.elastic.co/guide/en/apm/agent/ruby/current/configuration.html

そのほかの便利な機能

- Infra UI
- Logs UI
- Machine Learning
- Alerting

Infrastructure Solution

Beta I Basic (free)

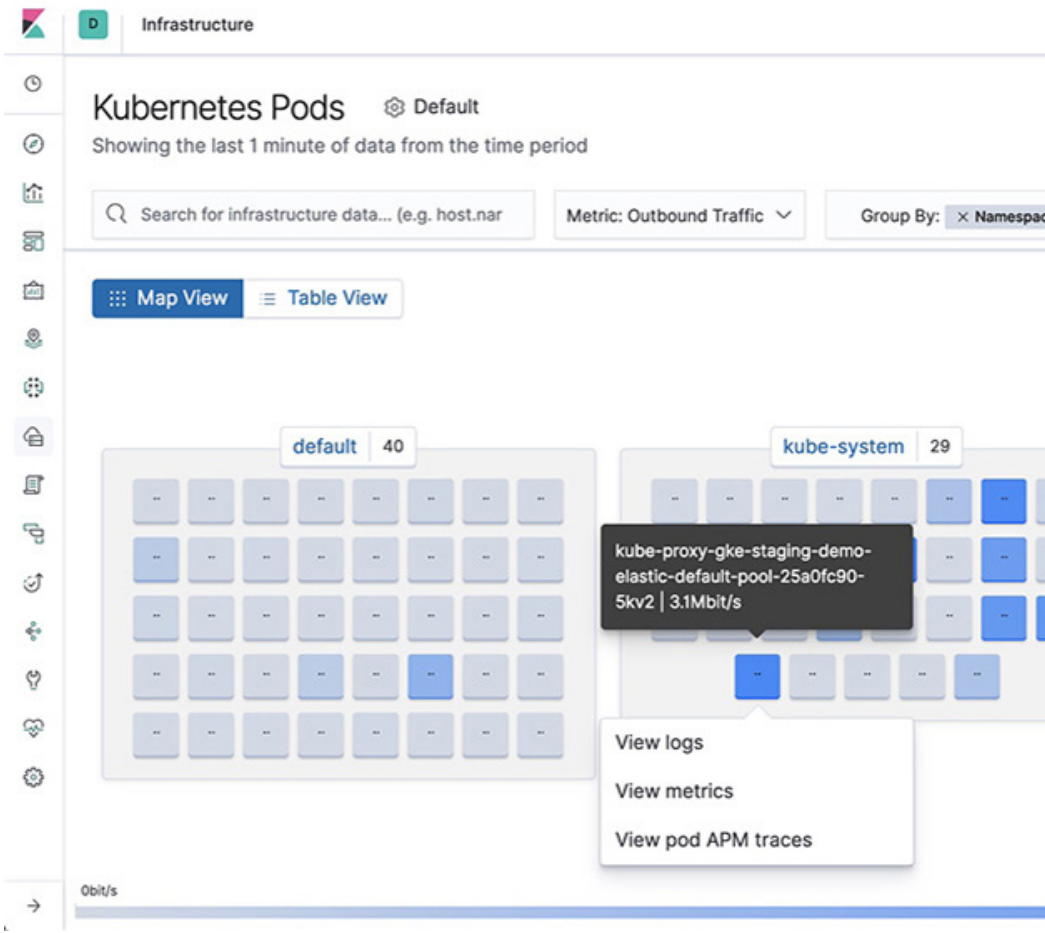
インフラオペレーター向けに特化

1000を超えるインフラの構成を俯瞰

Kubernetes、Docker のネイティブサポート

メトリック、ログ、APM ビューへのドリル・ダウン

アドホックおよび構造化検索



Logs Solution

Beta I Basic (free)

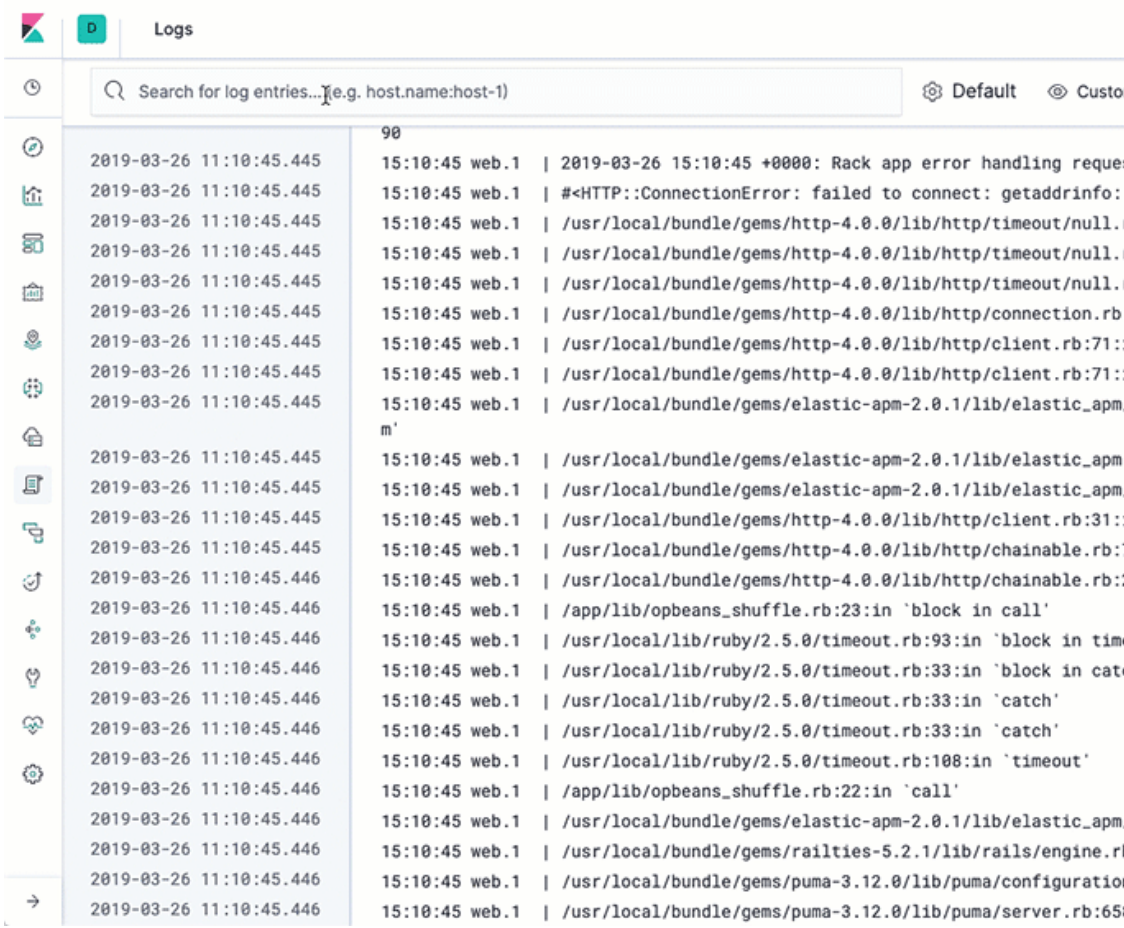
ライブでログのトラブルシューティングを助ける軽量なログビューアー

コンソールのような表示

(tail -fのような)ライブ・ログ・ストリーミング

履歴ログの無限スクロール

アドホックおよび構造化検索



アラート

通知を受け取る。何も逃さない。

CPU消費量が予想外に増えている。アプリケーションの応答時間が異常に長くなっている。Elasticsearchのインデックス効率が急落した... こうした場合に、オプションのアラート機能で誰よりも早く状況を把握することができます。

Elasticのアラート機能でデータの変化を通知する。ビデオを見る

NEW UIに統合されたツールでAPMデータのアラートを受信できるようになりました。

データの変化を検知する

Elasticsearchのクエリ機能をフルパワーで活用するアラート機能なら、データの重要な変化を見逃しません。

つまり、Elasticsearchでクエリできるものは何でもアラートすることが可能です。たとえば、次のような場合に通知します。

同じユーザーが1時間以内に3つの異なる場所からログインした。 セキュリティ侵害の疑いを想定してプロアクティブに対応できます。

機械学習

もう見逃さない

データセットはますます複雑化し、急速に増えています。単純なルール定義や、ダッシュボードを見るだけで、インフラのトラブルや侵入者、ビジネスの課題を特定することは困難です。Elasticの機械学習では、トレンドや周期性などからデータの振る舞いを自動的に、リアルタイムにモデル化し、すばやく問題を特定して原因分析をサポートします。さらに誤検出を防ぎます。

異常検知を自動化しよう。ビデオをみる

NEW カスタムルールを追加してドメイン知識を活用できるようになりました。

データの常識を覆す

Elastic Stackは、「先週の1秒あたりのリクエスト数は？」といった質問にすばやく答え、リアルタイムに結果を視覚化することが得意です。では「いつもと何か違うことが起きてる？」とか、「この原因は何？」といった質問はどうでしょう？

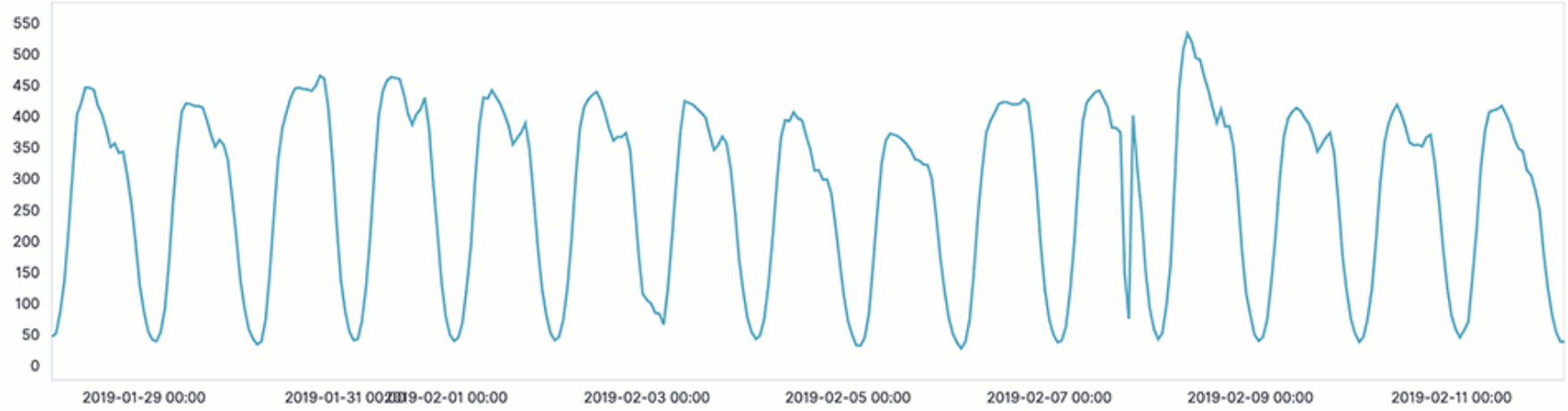
Elasticの機械学習はこうした質問に答えることができ、幅広いユースケースやデータに対応します。あなたのクリエイティブな発想で、新しい使い方を見つけてください。

ログとメトリック：アプリケーションに対する急激なリクエストの減少を特定して、原因となっているサーバーを突き止

Aggregation: Mean

Field: #orders_per_min

Bucket span: 15m Estimate bucket span



Name: order_per_minute

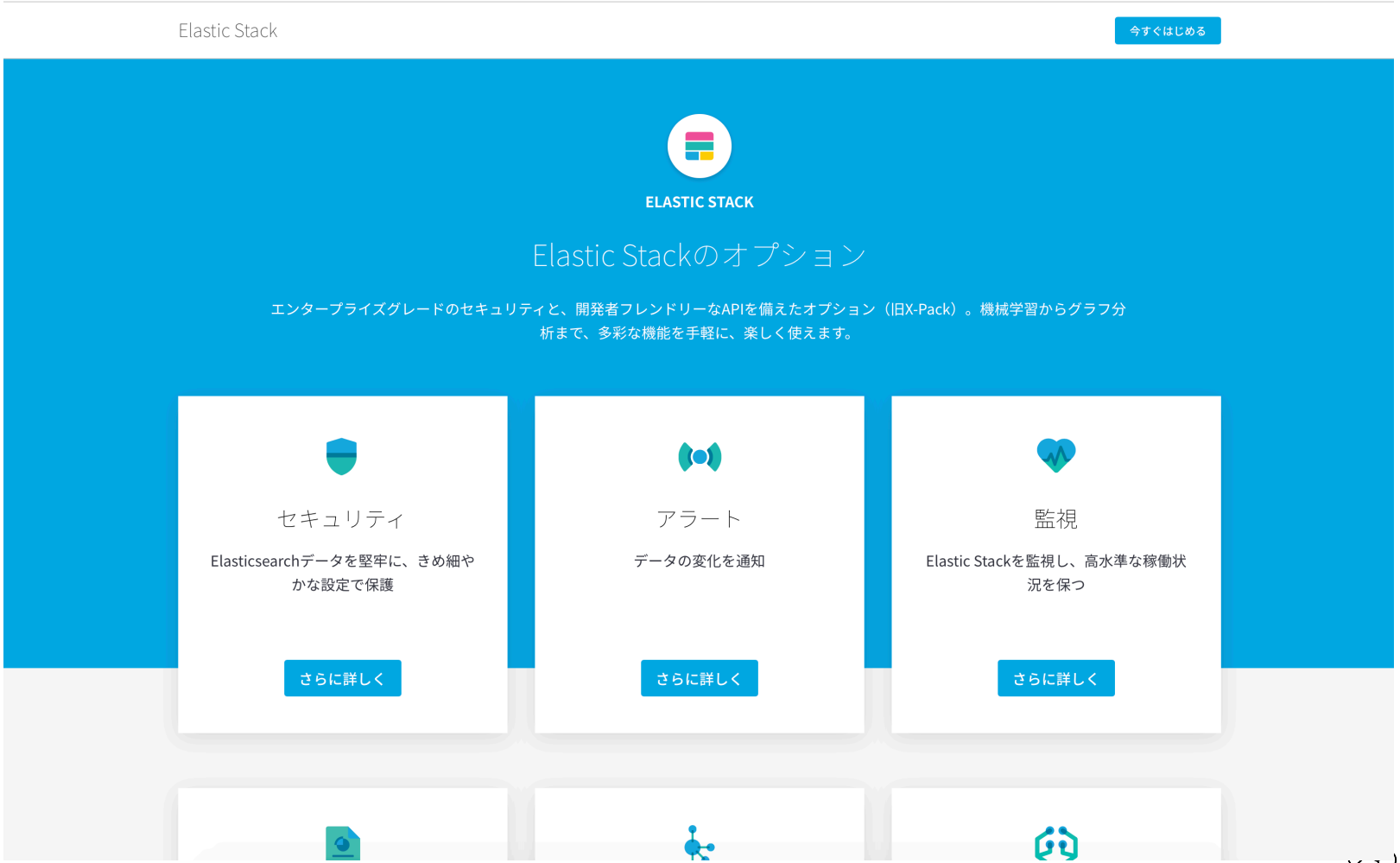
Description: Avg. orders per minutes

Job Groups: Job Group

Advanced

Move to advanced job configuration

さらに活用するには？


Elastic Stack
今すぐはじめる
ELASTIC STACK
Elastic Stackのオプション
エンタープライズグレードのセキュリティと、開発者フレンドリーなAPIを備えたオプション（旧X-Pack）。機械学習からグラフ分析まで、多彩な機能を手軽に、楽しく使えます。
セキュリティ
Elasticsearchデータを堅牢に、きめ細やかな設定で保護
さらに詳しく
アラート
データの変化を通知
さらに詳しく
監視
Elastic Stackを監視し、高水準な稼働状況を保つ
さらに詳しく

elastic

Elasticsearch Service　App Search　Site Search

ELASTIC CLOUD

Elasticsearchのパワーを利用したSaaS製品群

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

Elasticsearch Service

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

製品概要

今すぐトライ

Elastic App Search Service

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

製品概要

今すぐトライ

Elastic Site Search Service

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

製品概要

今すぐトライ

lastic

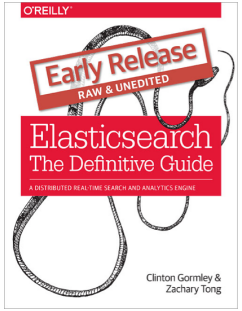
参考サイト

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

参考文献

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

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



elastic

参考文献

- 入門 監視
  ーモダンなモニタリングのためのデザインパターン
  Mike Julian　著、松浦 隼人　訳

  https://www.oreilly.co.jp/books/9784873118642/

elastic

Elastic Stackのセキュリティ：データを安全に保つためのベストプラクティス

Kosho Owa, Solution Architect, Elastic

2019年10月31日（木） 12:00PM | ウェビナー

elastic

Thank you!

- **Sample:** https://github.com/johtani/monitoring-ruby-app
- **Web** : https://www.elastic.co/jp/
- **Forums** : https://discuss.elastic.co/
- **Twitter** : @johtani