



Elastic Stackで始める アプリケーション監視

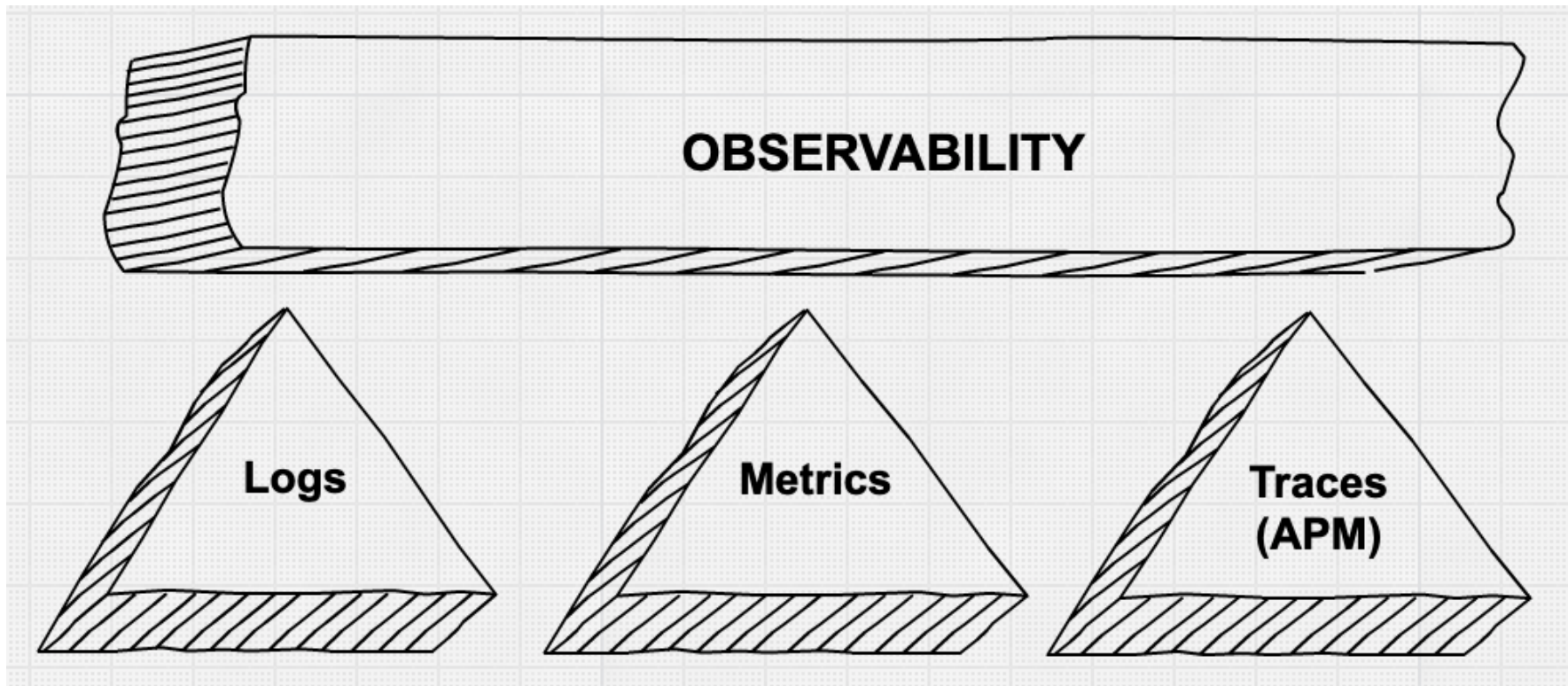
Jun Ohtani, Community Advocate
2019/10/04

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>



Kibana、ログだけじゃないし
監視系の話もできないとなあ

O'REILLY
オライリー・ジャパン

入門 監視

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 健人 訳



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？





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

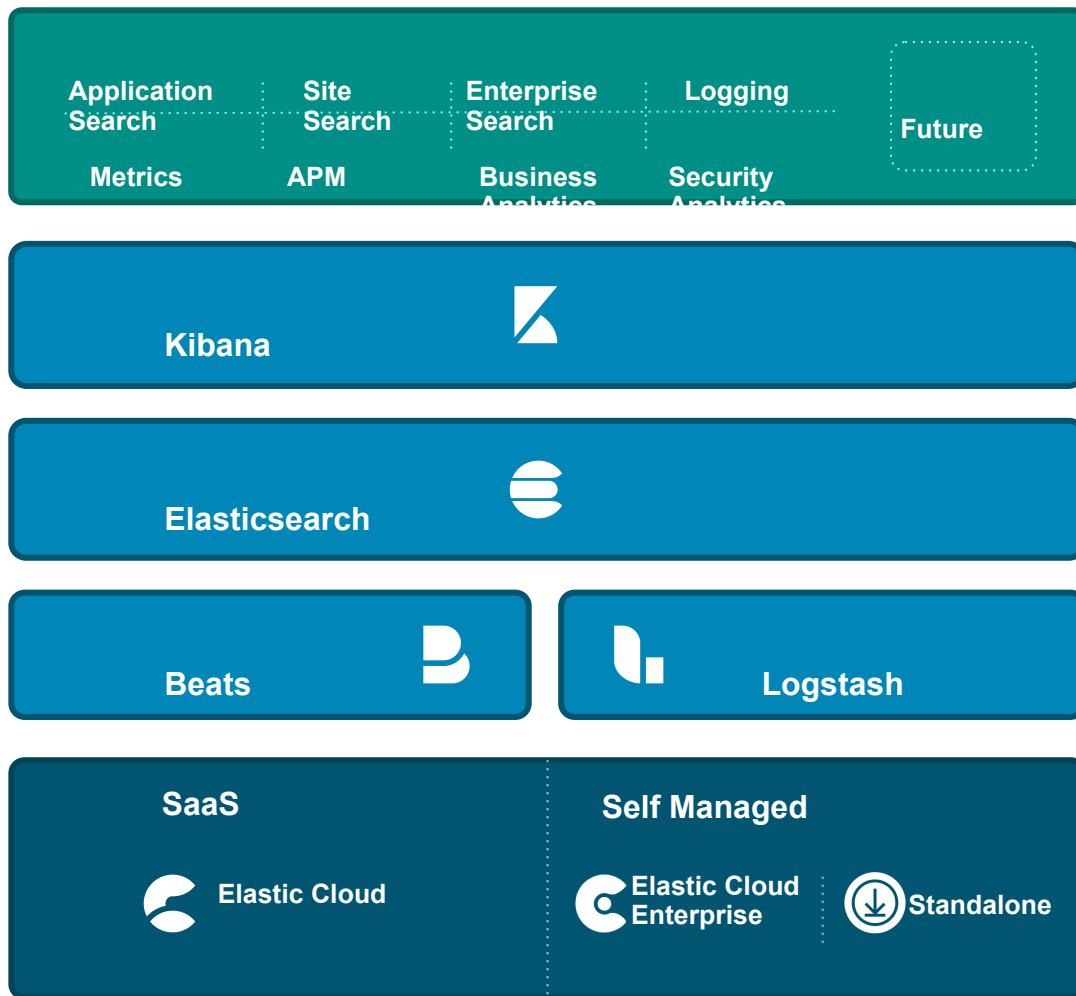
8:10 - 2015年10月8日

3,013件のリツイート 2,612件のいいね

21 3,013 2,612

Elastic Stackとは？

Elastic Stack



ソリューション

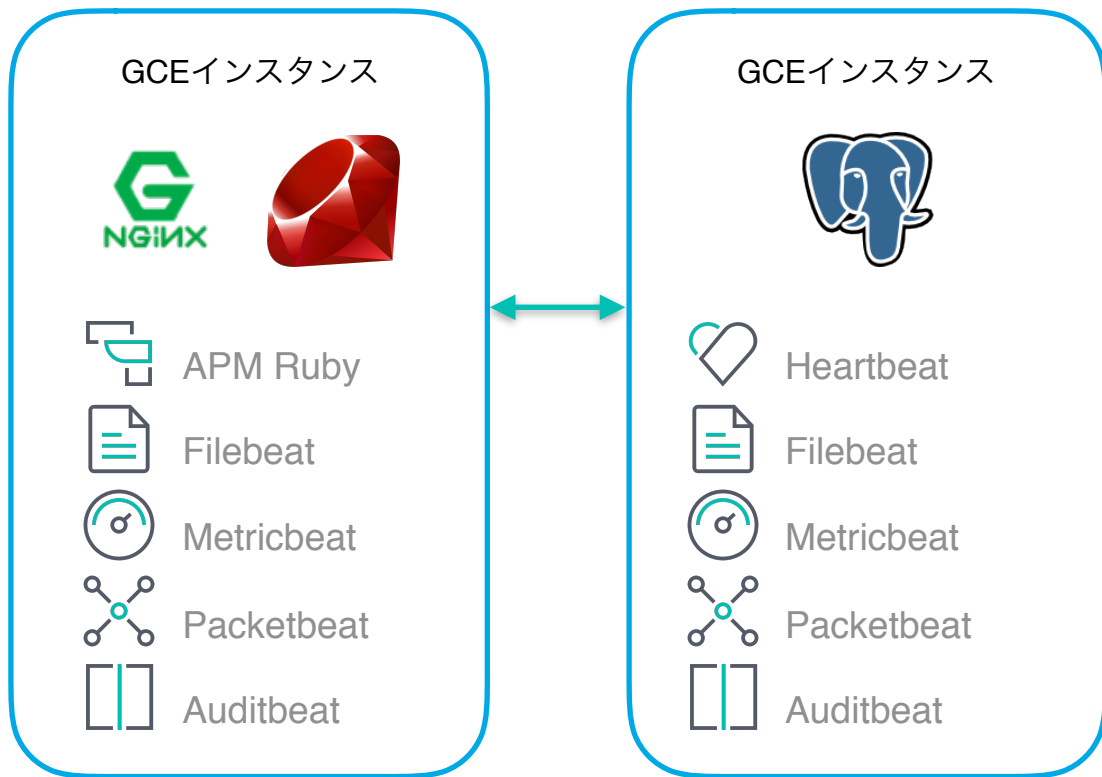
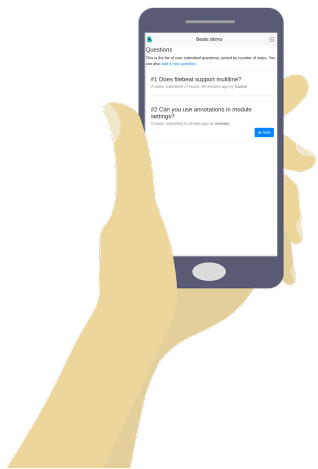
可視化、管理

保存、検索、分析

インジェスト

デプロイ

デモサイト



デモサイト



<https://www.johtani.dev>

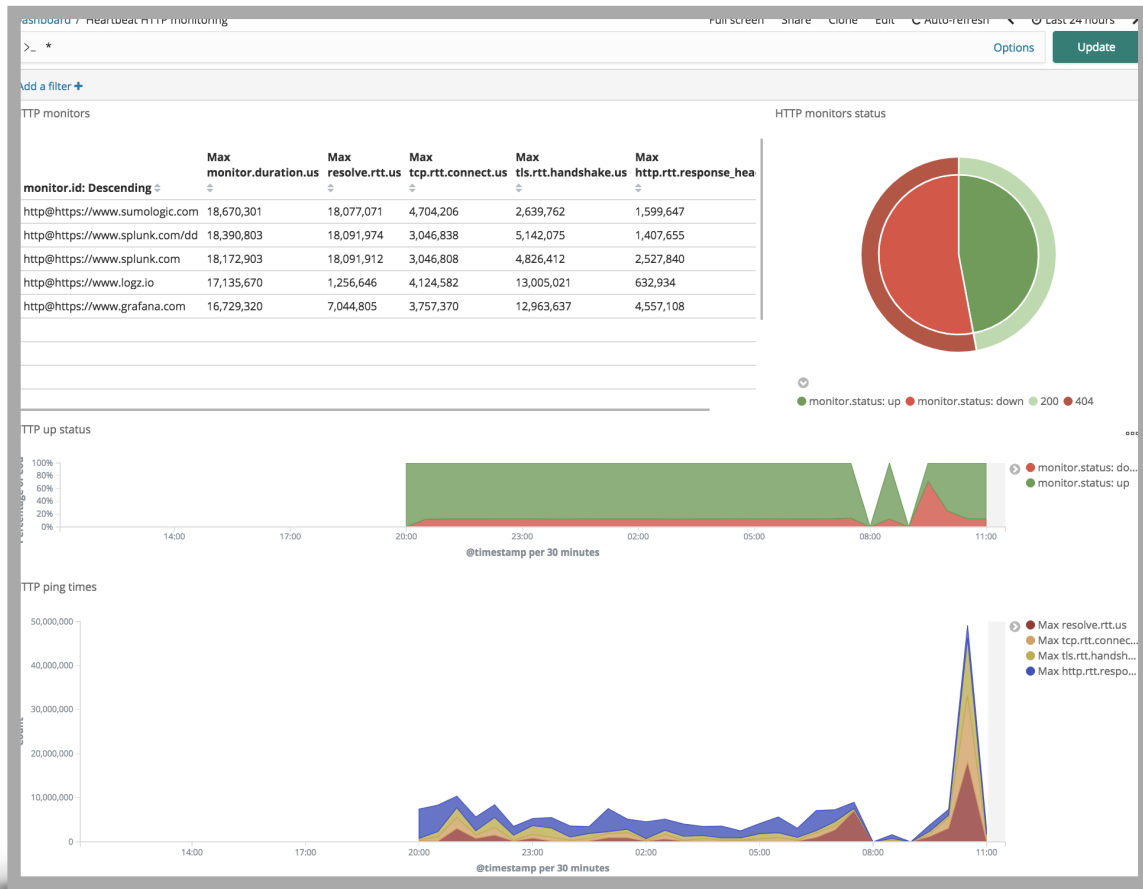
アプリケーションの 監視ポイント

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

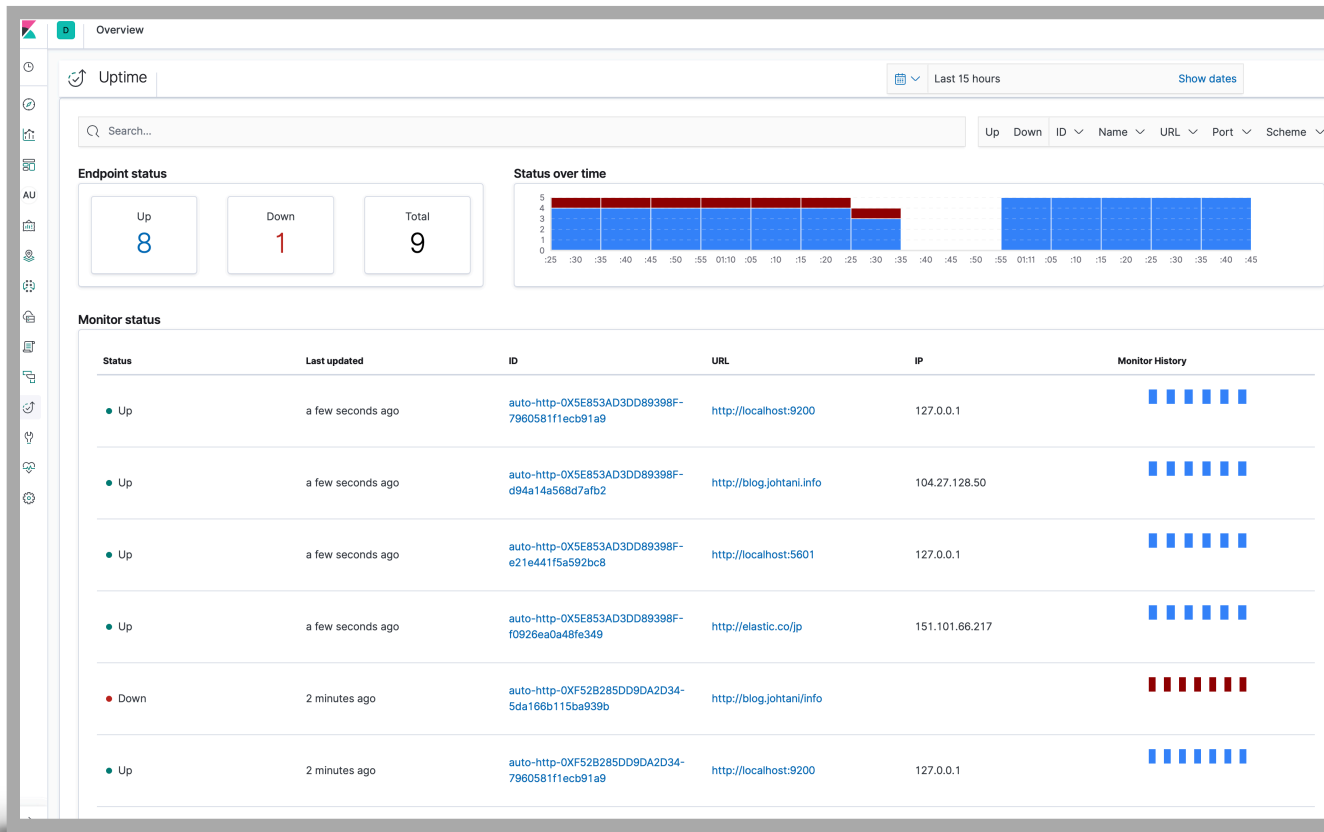
Heartbeat

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](#)

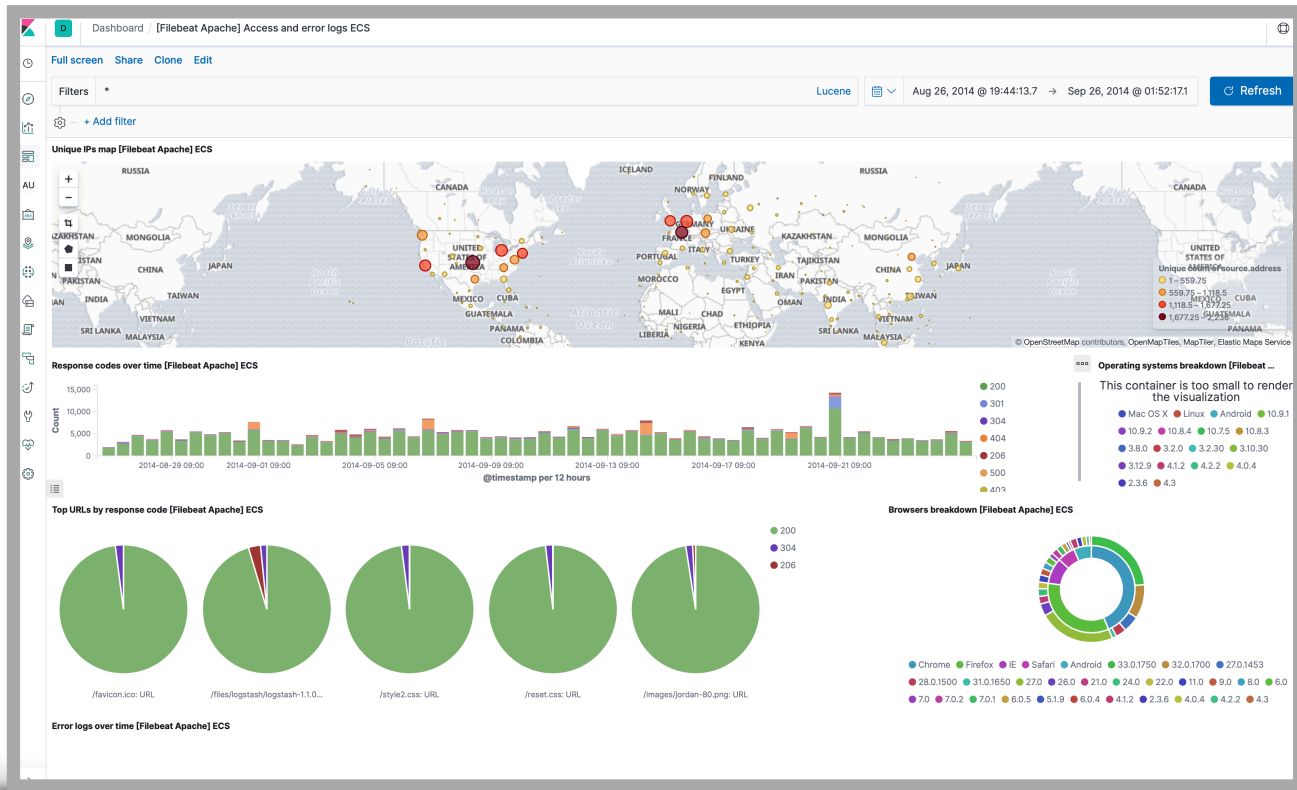
[vSphere module](#)

[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](#)

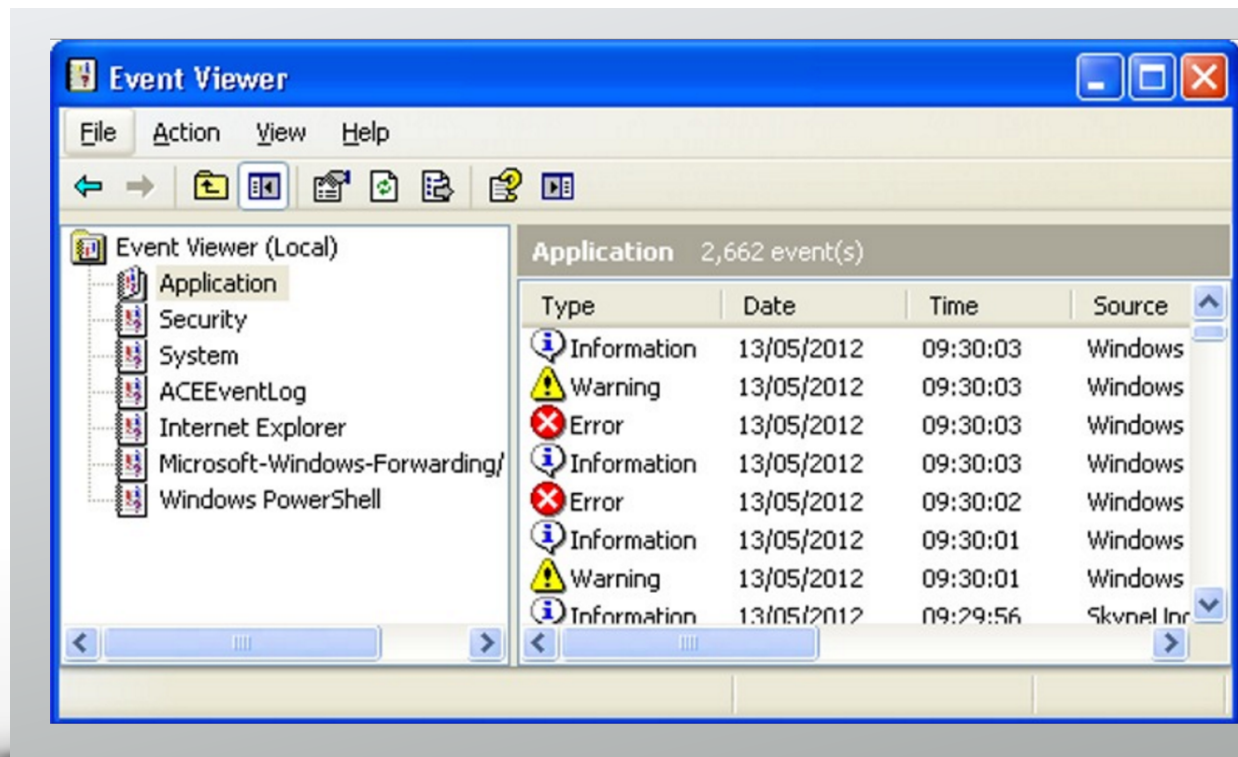
[System module](#)

[Traefik module](#)

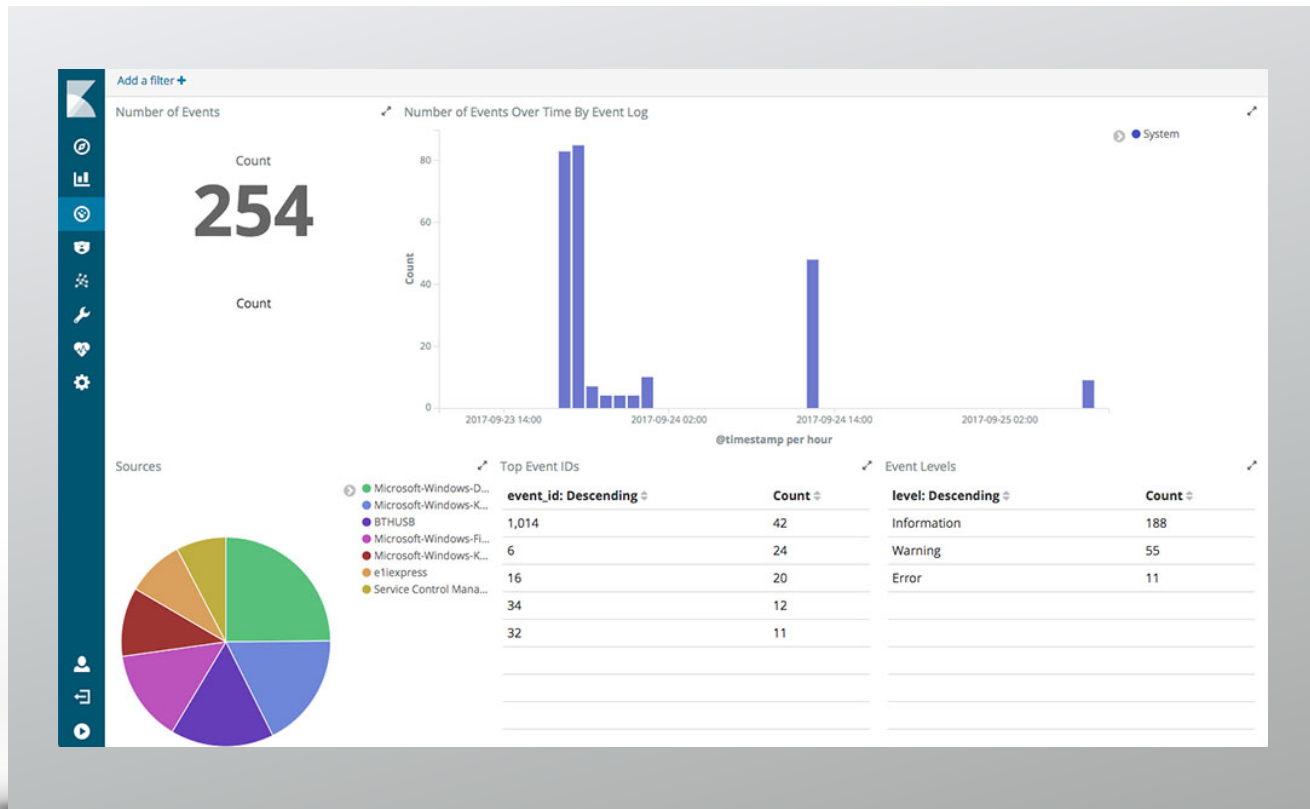
[Zeek \(Bro\) Module](#)

winlogbeat

Welcome
to **1998**



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 1987817713, 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 10658051819], length 0
10:03:59.912168 IP pc-in-f189.1e100.net.https > 172.31.98.131.60078: Flags [P..], seq 391100900:391100994, ack 1961900067, win 1651, options [nop,nop,TS val 182273890 ecr 1065485533], 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)
10:04:00.568618 IP google-public-dns-a.google.com.domain > 172.31.98.131.52072: 9347 1/0/0 PTR nuq04s19-in-f21.1e100.net. (83)
10:04:00.569572 IP 172.31.98.131.59451 > google-public-dns-a.google.com.domain: 6362: PTR: 82.148.59.109.in-addr.arpa. (44)
10:04:00.676626 IP google-public-dns-a.google.com.domain > 172.31.98.131.59451: 6362 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
10:04:01.348942 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
10:04:01.367564 IP 172.31.98.131.59991 > pc-in-f125.1e100.net.jobber-client: Flags [P..], seq 53622692:53622809, ack 3725017102, win 65535, length 117
10:04:01.511834 IP pc-in-f125.1e100.net.jobber-client > 172.31.98.131.59991: Flags [P..], seq 1:134, ack 117, win 65100, length 133
10:04:01.511834 IP 172.31.98.131.59991 > pc-in-f125.1e100.net.jobber-client: Flags [..], ack 134, win 65535, length 0
10:04:01.778555 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 > 199.27.19.134.http: Flags [..], ack 682580952, win 4096, length 0
```

Packetbeat

Capture the
Packet

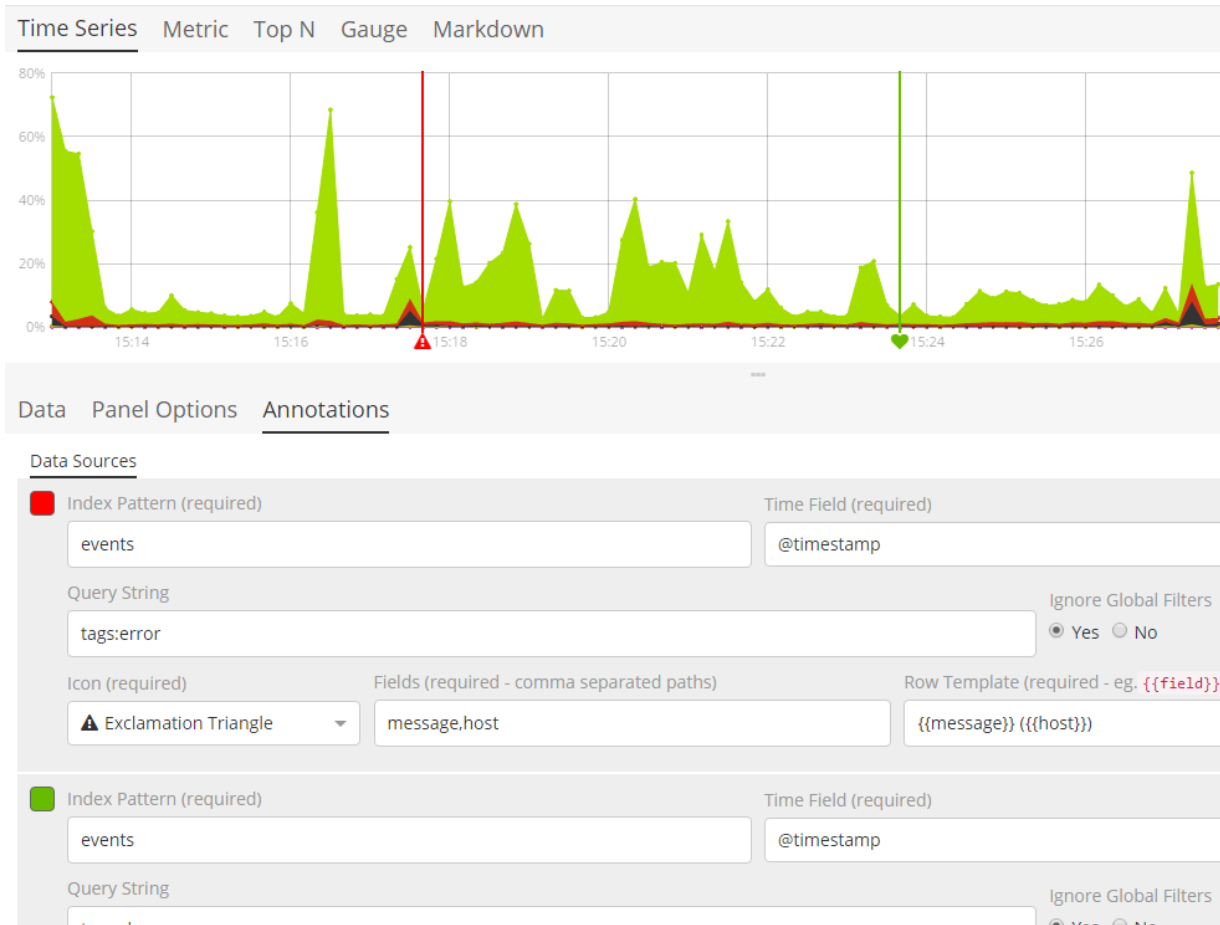


アプリケーションのリリースタイミング

- 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

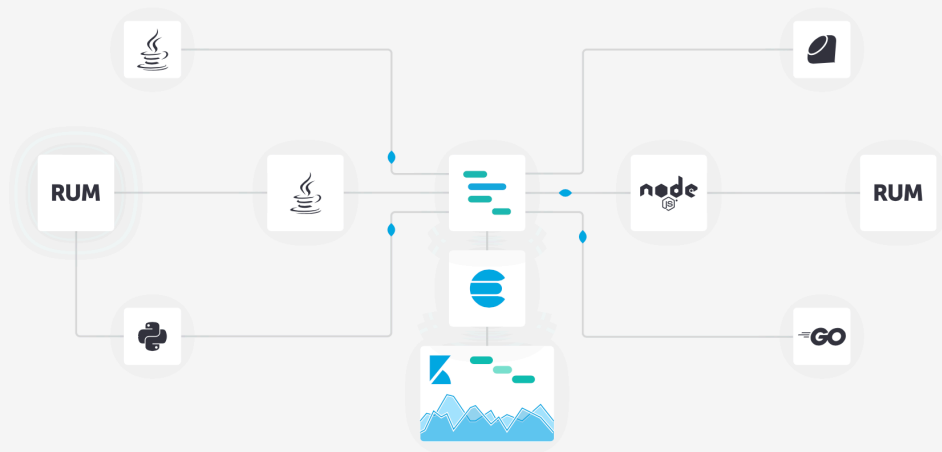


オープンソースのアプリケーション パフォーマンス監視 (APM)

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。



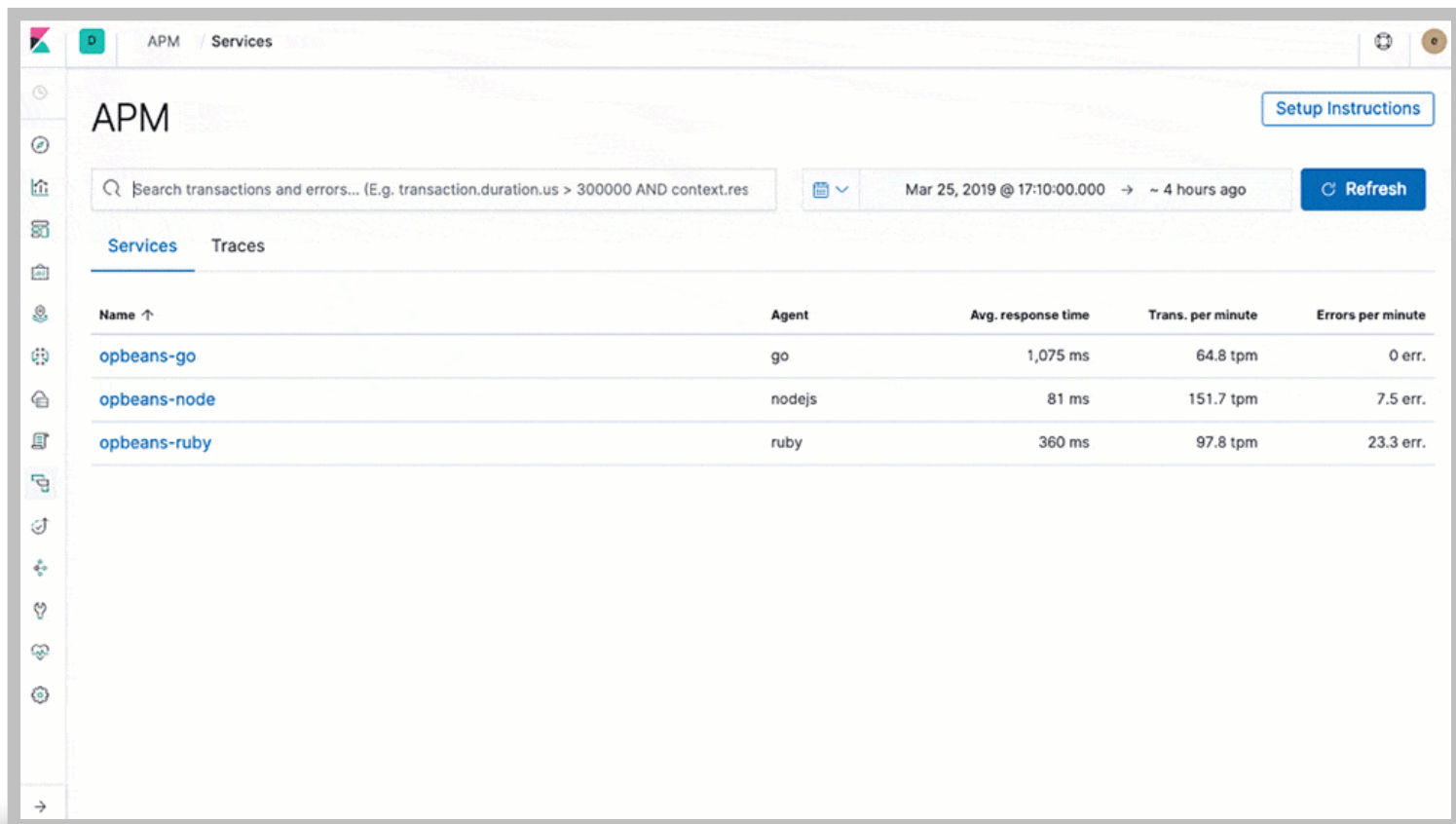
ElasticのAPMで、パフォーマンスメトリックの可視化が簡単に。 | [今すぐトライ](#)

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](#)

サポート言語

- Node.js
 - Python
 - Ruby
 - Go
 - Java
 - .NET
-
- RUM - Real User Monitoring JavaScript Agent

Elastic APM



The screenshot displays the Elastic APM interface for the 'Services' section. At the top, there is a search bar with the placeholder text 'Search transactions and errors... (E.g. transaction.duration.us > 300000 AND context.res)'. To the right of the search bar, the current time and range are shown as 'Mar 25, 2019 @ 17:10:00.000 → ~ 4 hours ago', along with a 'Refresh' button. Below the search bar, there are two tabs: 'Services' (which is selected) and 'Traces'. A 'Setup Instructions' button is located in the top right corner. The main content area features 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.

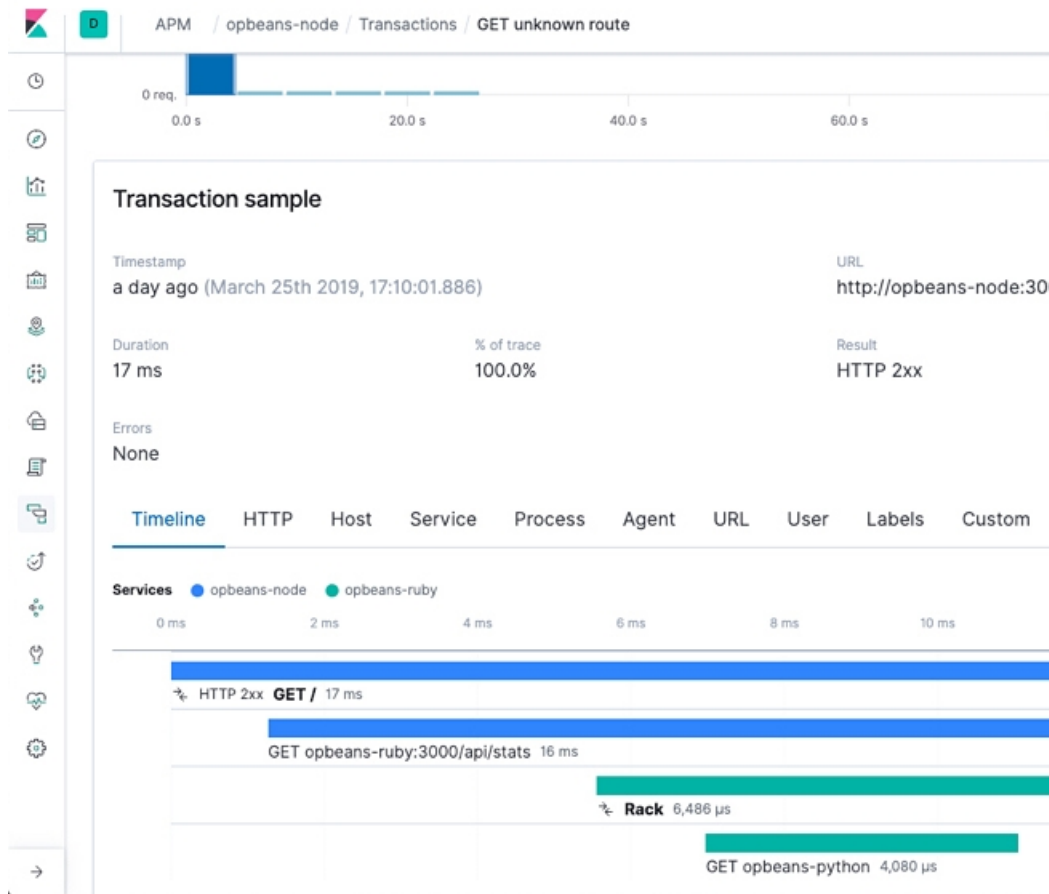
Distributed Tracing

Beta | Basic (free)

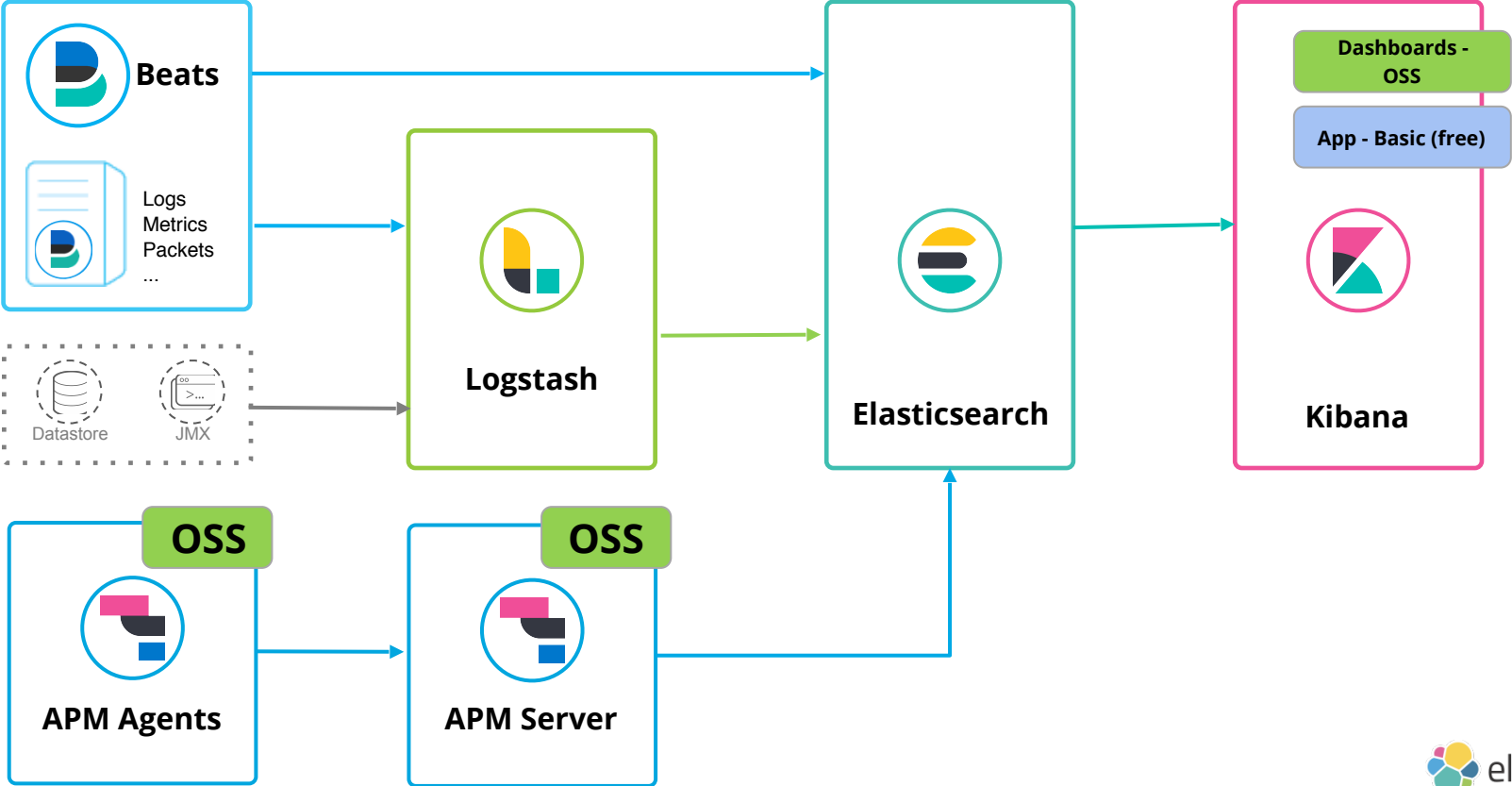
全ての計測されたサービスを見るための
統合されたビュー

サブコンテキスト内のトレースに遷移

OpenTracing 互換



Deployment



APM Ruby Agent

Framework Support

- Ruby on Rails $\geq 4.x$
- 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>

その他の便利な機能

- Infra UI
- Logs UI
- Machine Learning
- Alerting

Infrastructure Solution

Beta | Basic (free)

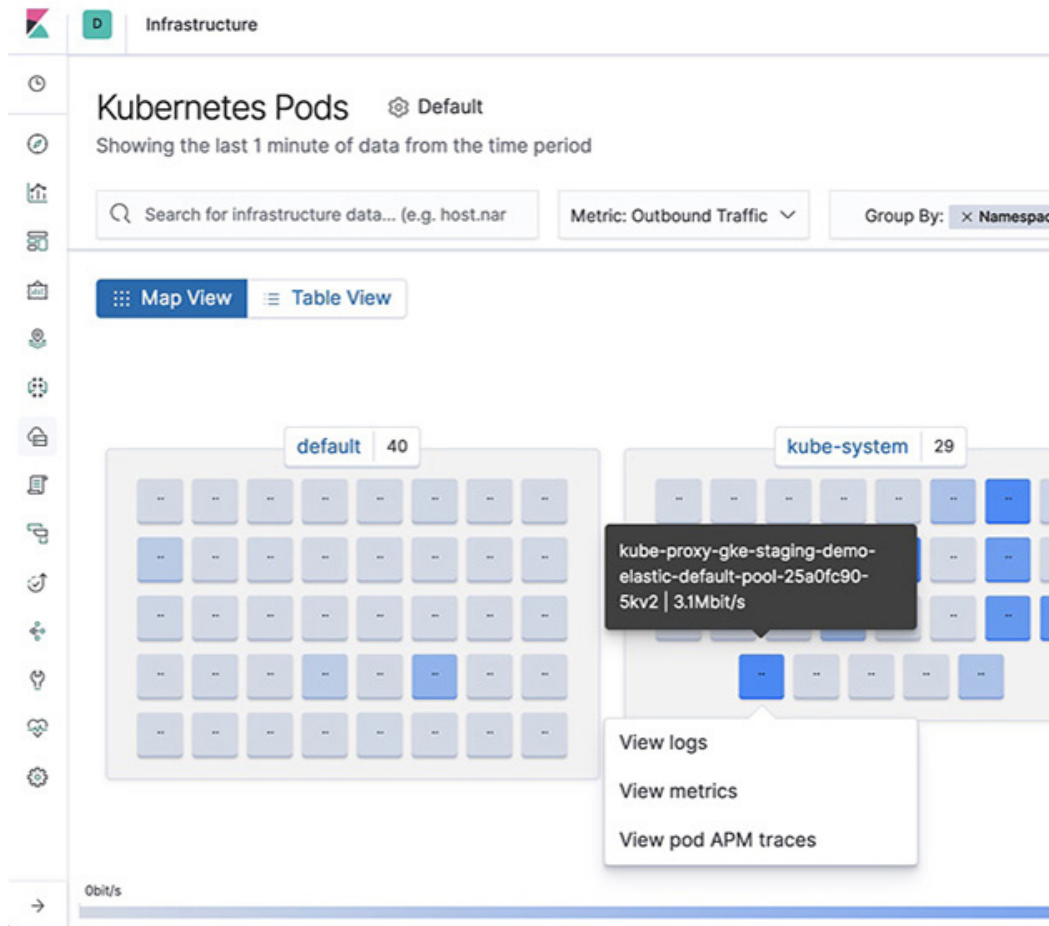
インフラオペレーター向けに特化

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 | Basic (free)

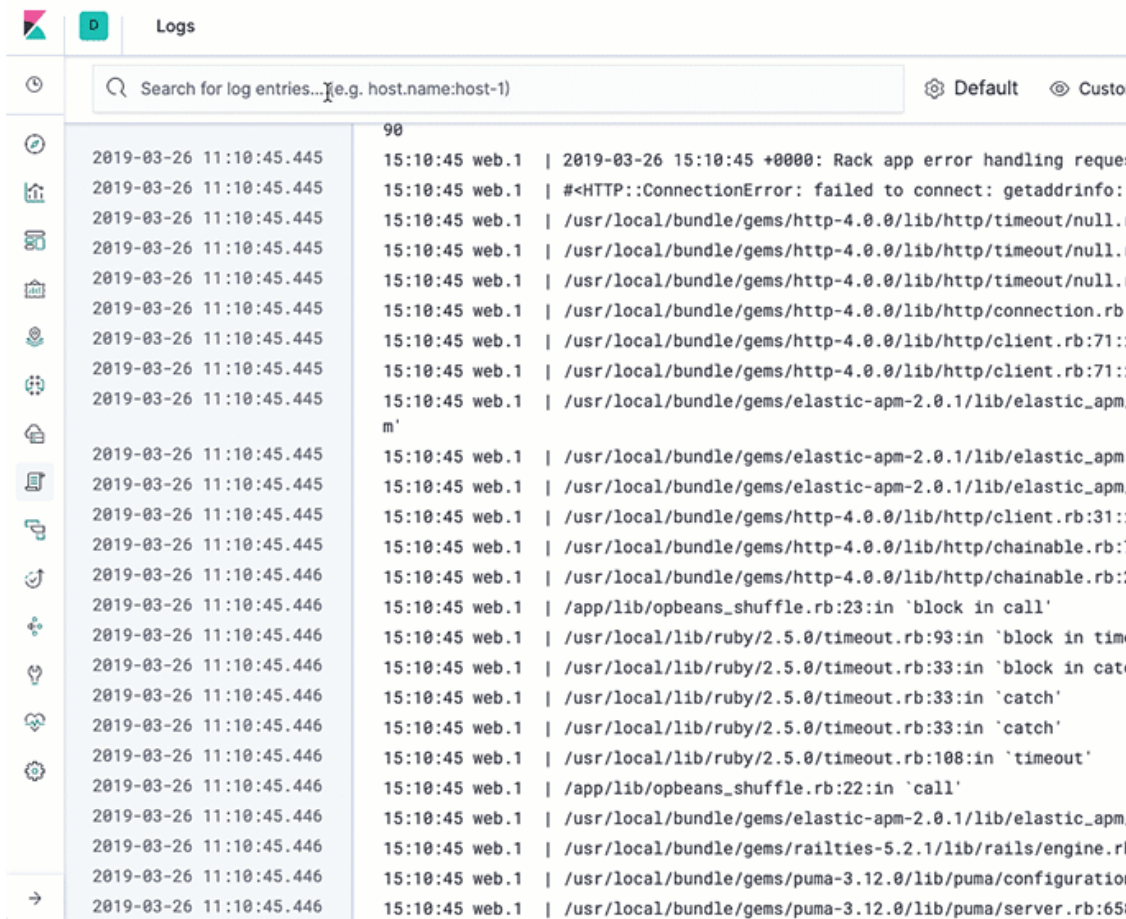
ライブでログのトラブルシューティング
を助ける軽量なログビューアー

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

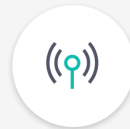
履歴ログの無限スクロール

アドホックおよび構造化検索



The screenshot displays the 'Logs' interface. At the top, there is a search bar with the placeholder text 'Search for log entries... [e.g. host.name:host-1]'. Below the search bar, a vertical sidebar on the left contains various icons for navigation and settings. The main area shows a list of log entries, each with a timestamp (e.g., '2019-03-26 11:10:45.445') and a log message. The log messages include error handling requests, connection errors, and application-specific logs from services like 'elastic-apm' and 'puma'.

Timestamp	Log Message
2019-03-26 11:10:45.445	15:10:45 web.1 2019-03-26 15:10:45 +0000: Rack app error handling request
2019-03-26 11:10:45.445	15:10:45 web.1 #<HTTP::ConnectionError: failed to connect: getaddrinfo: nodename nor servname provided, or not known
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/timeout/null.rb:10:in `block in connect'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/timeout/null.rb:10:in `connect'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/connection.rb:10:in `connect'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/client.rb:71:in `connect'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/client.rb:71:in `connect'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/elastic-apm-2.0.1/lib/elastic_apm/middleware.rb:10:in `block in call'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/elastic-apm-2.0.1/lib/elastic_apm/middleware.rb:10:in `call'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/client.rb:31:in `connect'
2019-03-26 11:10:45.445	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/chainable.rb:10:in `connect'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/bundle/gems/http-4.0.0/lib/http/chainable.rb:10:in `connect'
2019-03-26 11:10:45.446	15:10:45 web.1 /app/lib/opbeans_shuffle.rb:23:in `block in call'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/lib/ruby/2.5.0/timeout.rb:93:in `block in timeout'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/lib/ruby/2.5.0/timeout.rb:33:in `block in catch'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/lib/ruby/2.5.0/timeout.rb:33:in `catch'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/lib/ruby/2.5.0/timeout.rb:33:in `catch'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/lib/ruby/2.5.0/timeout.rb:108:in `timeout'
2019-03-26 11:10:45.446	15:10:45 web.1 /app/lib/opbeans_shuffle.rb:22:in `call'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/bundle/gems/elastic-apm-2.0.1/lib/elastic_apm/middleware.rb:10:in `block in call'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/bundle/gems/railties-5.2.1/lib/rails/engine.rb:10:in `call'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/bundle/gems/puma-3.12.0/lib/puma/configuration.rb:10:in `call'
2019-03-26 11:10:45.446	15:10:45 web.1 /usr/local/bundle/gems/puma-3.12.0/lib/puma/server.rb:65:in `call'



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、新しい使い方を教えてください。



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



D

Aggregation [ⓘ]

Mean

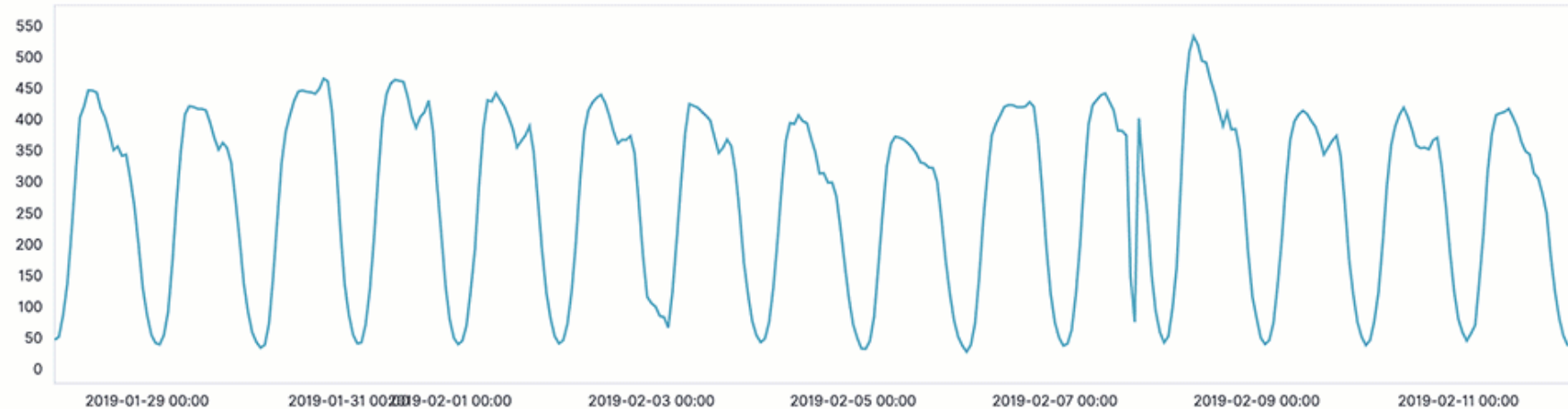
Field [ⓘ]

#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

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 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

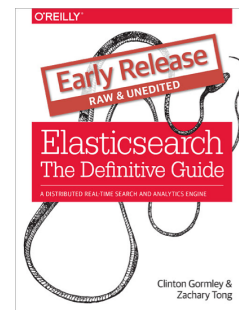
今すぐトライ

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



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 Stackのセキュリティ

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





Thank you!

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

