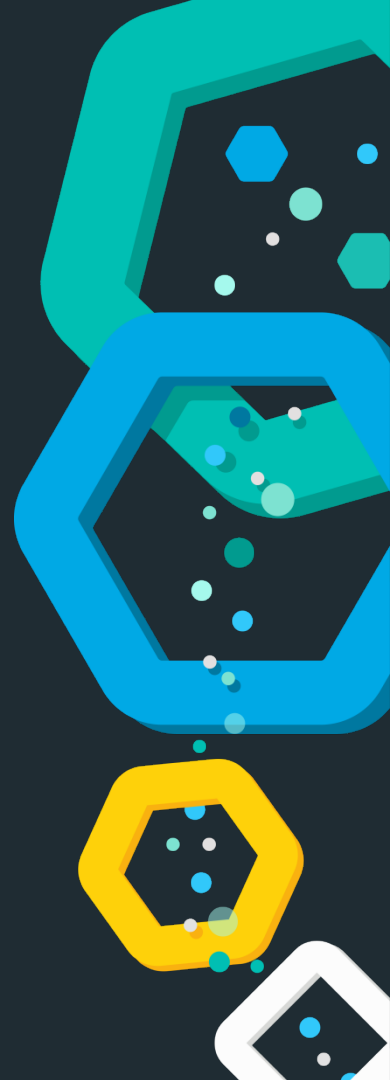


Elastic StackでKafkaをモニタリング！を始めてみるには？

2019/04/08

Community Engineer @Elastic
Jun Ohtani @johtani

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

*Kafka*を利用している人？

*Kafka*の運用をしている人？

*Kafka*の監視どうやってます？

監視してない

（ワイルド。。。）

*Zabbix*で監視

Confluent Control Center

*SaaS*サービス

Datadog?

その他

（何があるんだろう？）

Prometheus?

アジェンダ

- Elastic Stackとは？
- Kafkaのモニタリングを軽く試してみるには？
- さらに色々試してみるには？

Elastic Stackとは？

Elastic Stack

Kibana

可視化、管理

Elasticsearch

保存、検索、分析

Beats

Logstash

インジェスト

elastic

Elastic Stack

Application Search | Site Search | Enterprise Search | Logging | Future

Metrics | APM | Business Analytics | Security Analytics

ソリューション

Kibana

可視化、管理

Elasticsearch

保存、検索、分析

Beats | Logstash

インジェスト

elastic

Elastic Stack

App Search | Site Search | Enterprise Search | Logging | Future

Metrics | APM | Business Analytics | Security Analytics

ソリューション

Kibana

可視化、管理

Elasticsearch

保存、検索、分析

Beats | Logstash

インジェスト

SaaS

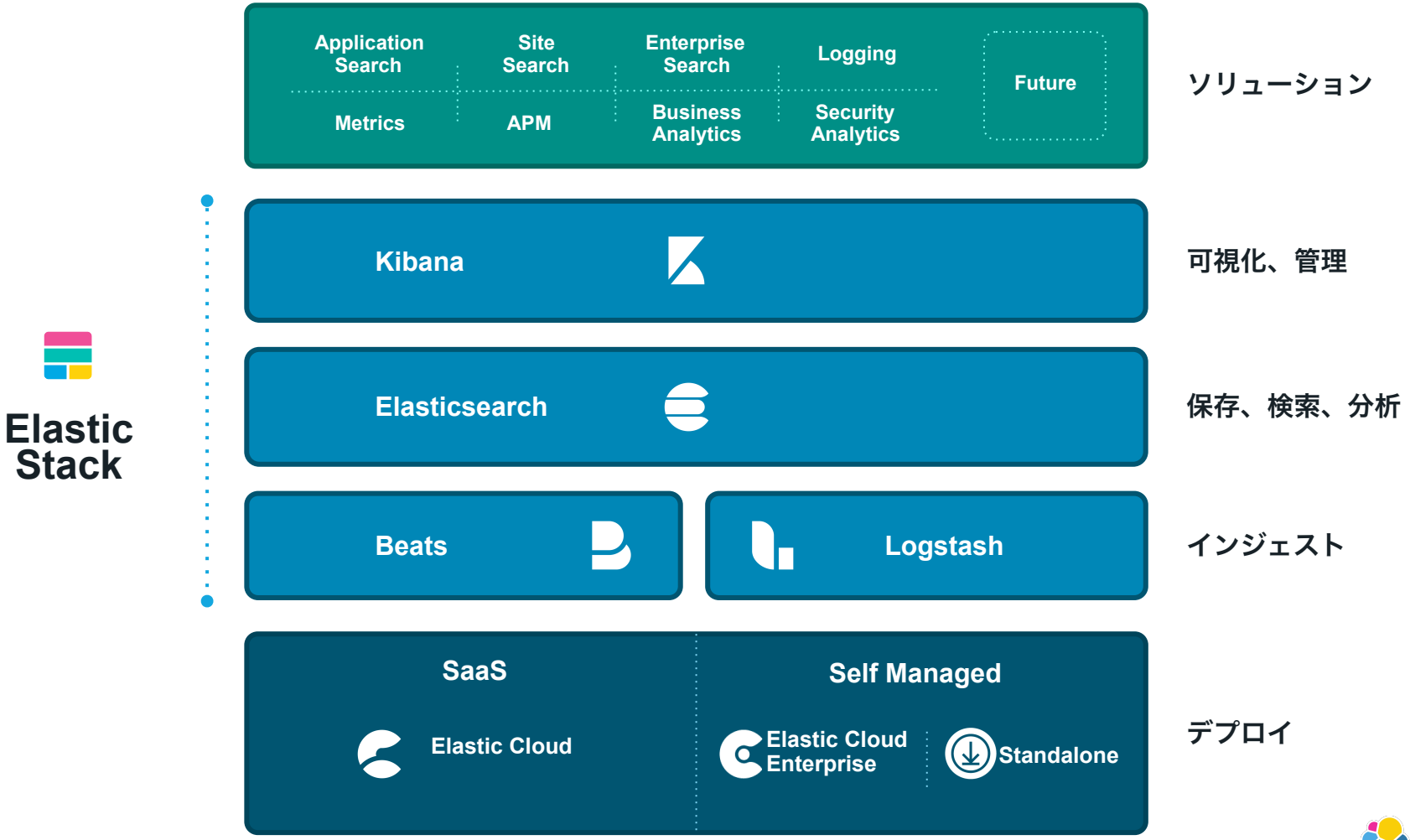
Elastic Cloud

Self Managed

Elastic Cloud Enterprise | Standalone

デプロイ

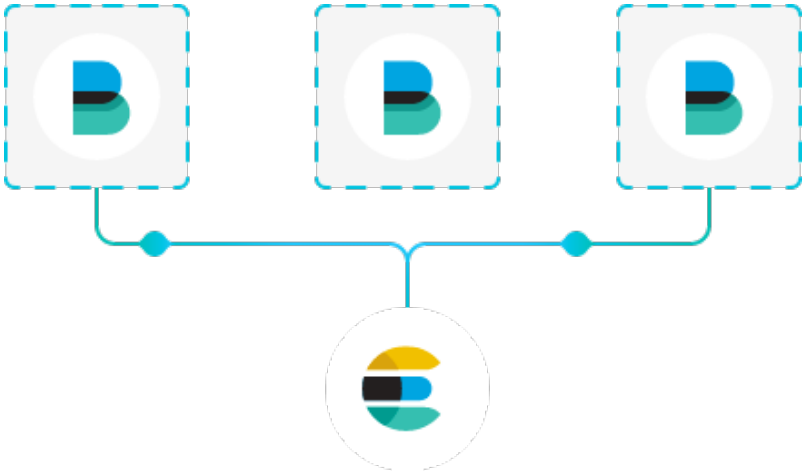
elastic


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

beats

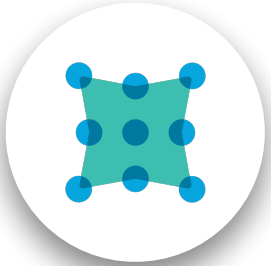
Beats

軽量データシッパー



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

The Beats family



Packetbeat

Network data

Metricbeat

Metrics

Winlogbeat

Windows Event Logs

Auditbeat

Audit data

Filebeat

Log files

Heartbeat

Uptime monitoring

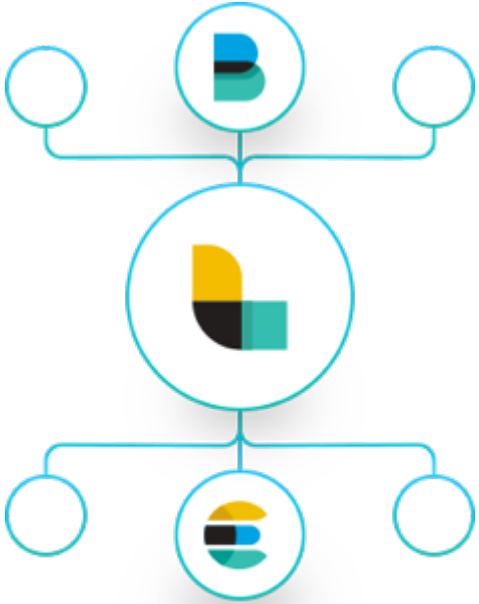
+40 community Beats

elastic

logstash

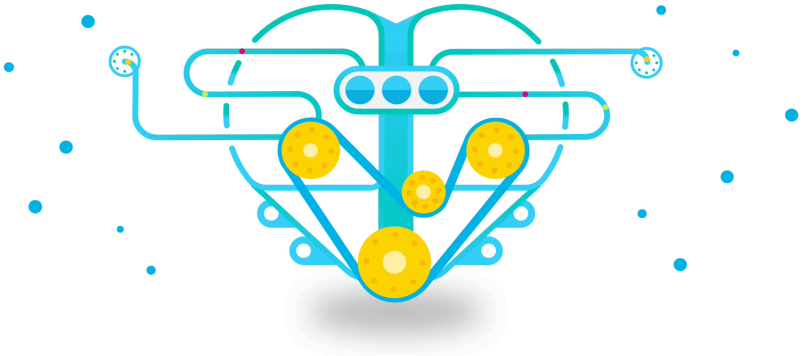
Logstash

データ加工パイプライン



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

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

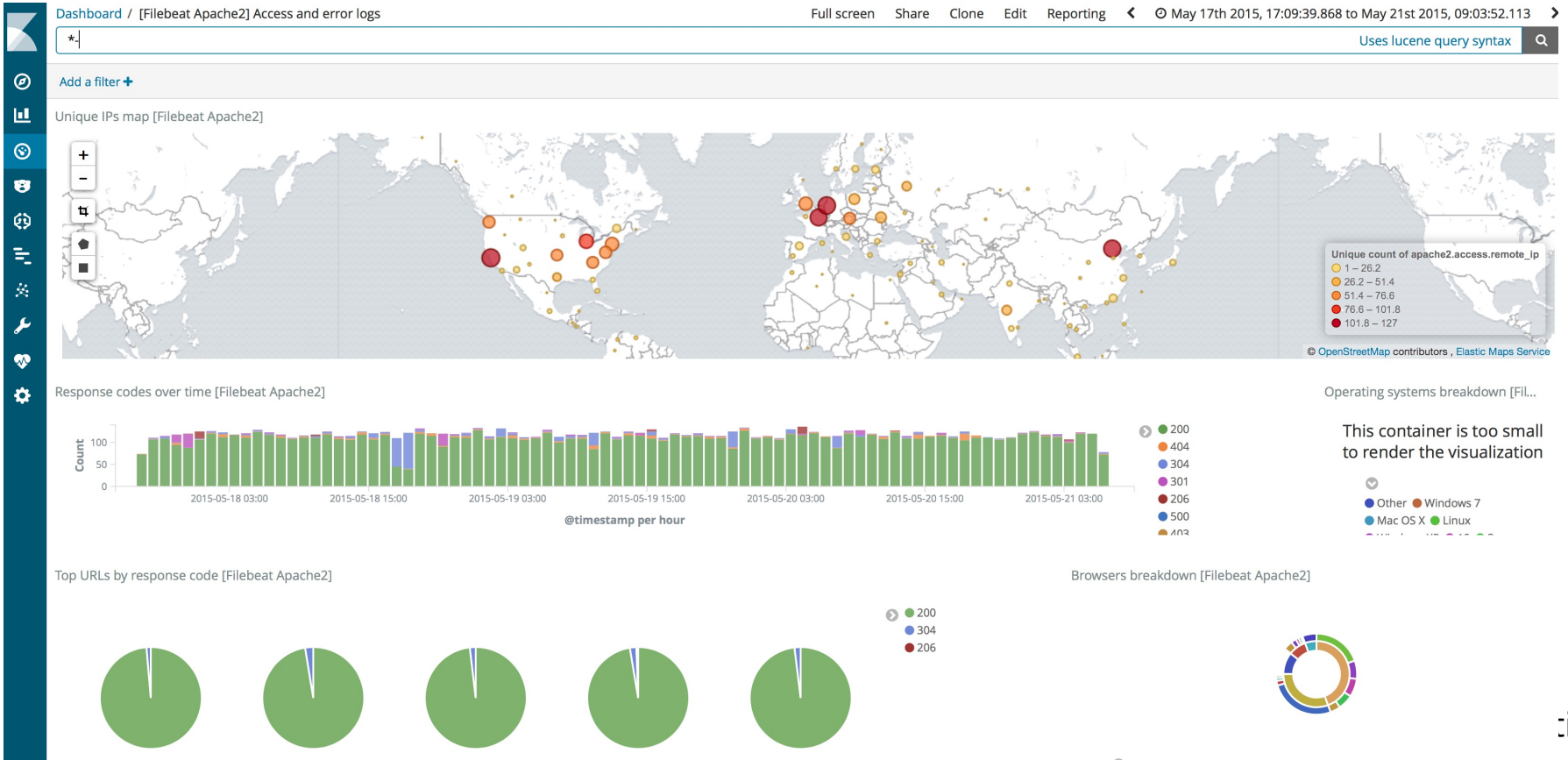
kibana

Kibana

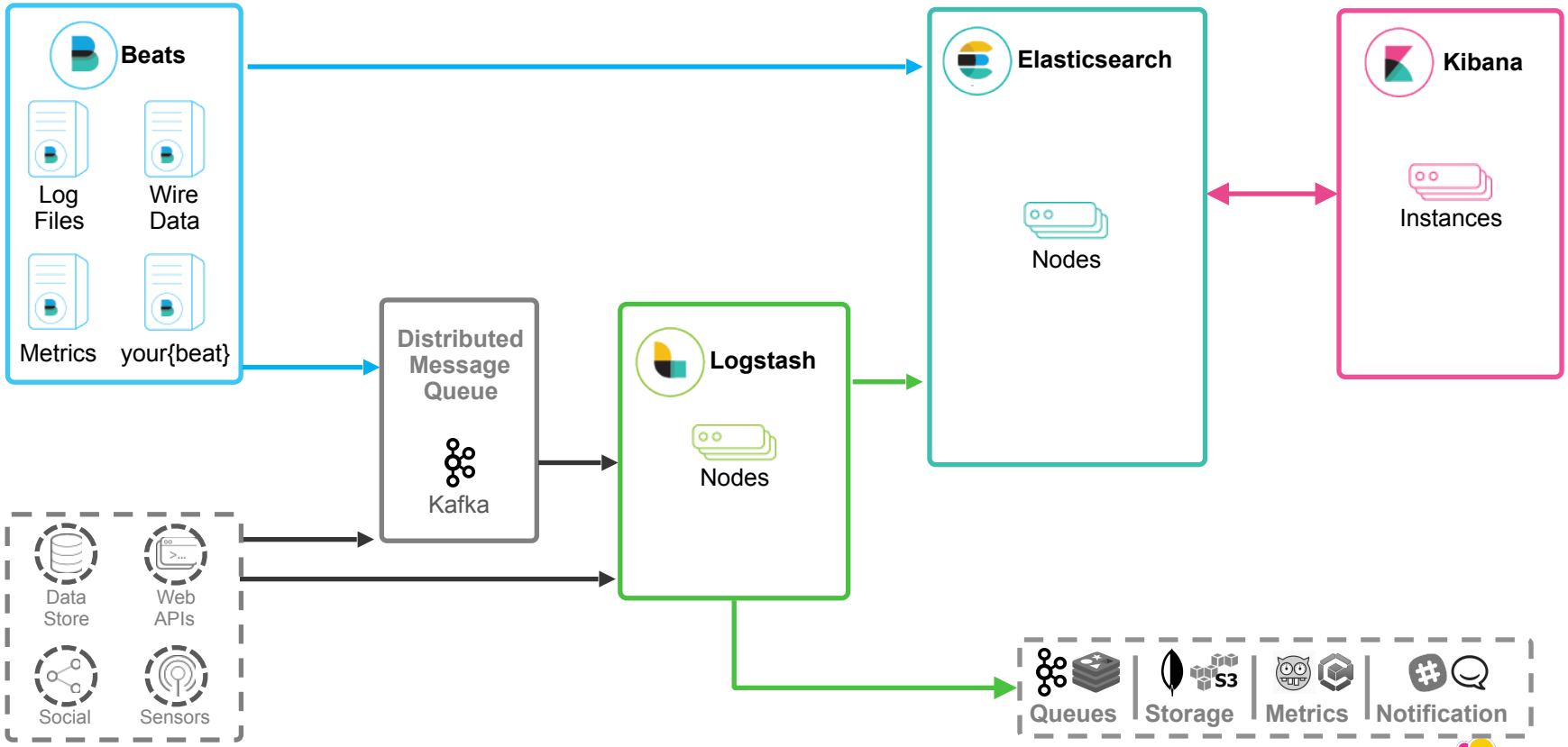
Window into the Elastic Stack

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

Kibana 6


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

Elastic Stackの構成



elastic

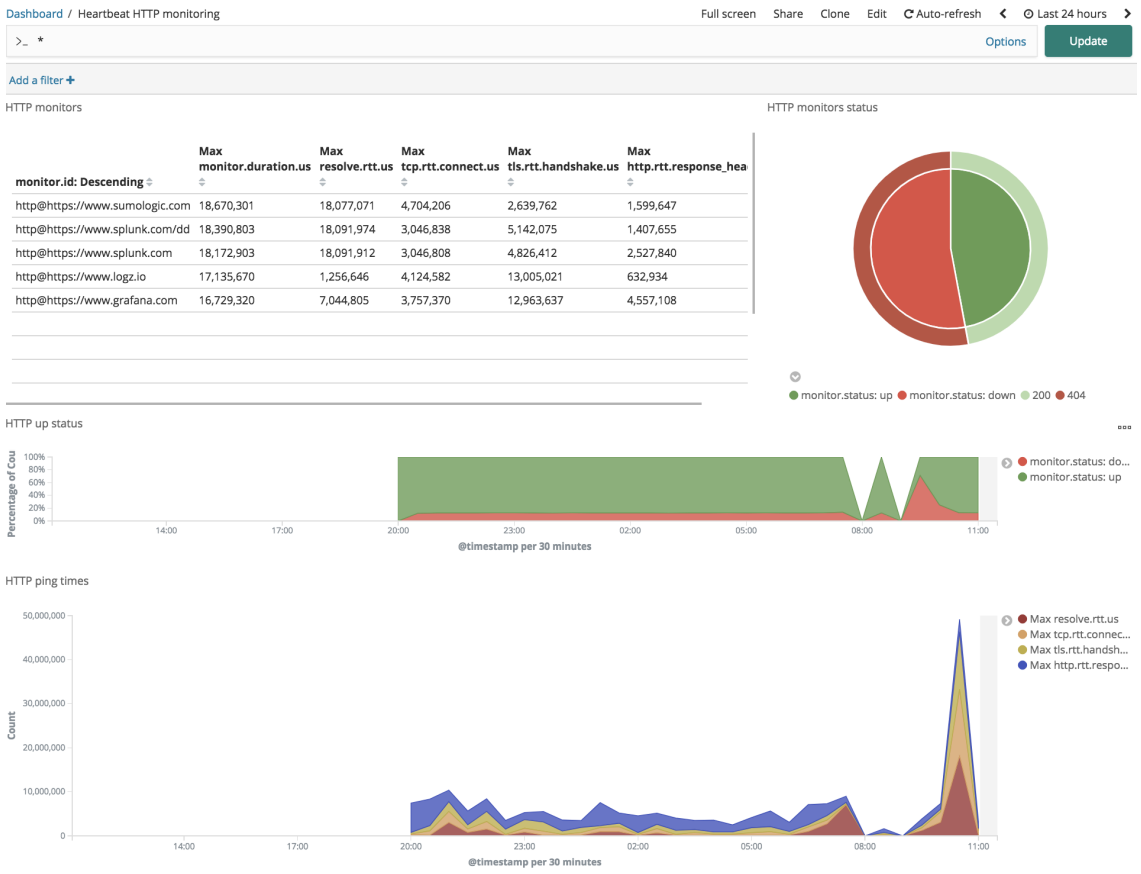
Kafkaのモニタリング with Beats

監視ポイント？

- 外形監視 → Heartbeat
- メトリック（メトリクス） → Metricbeat
  - サーバー、アプリケーション
- ログ → Filebeat

Heartbeat

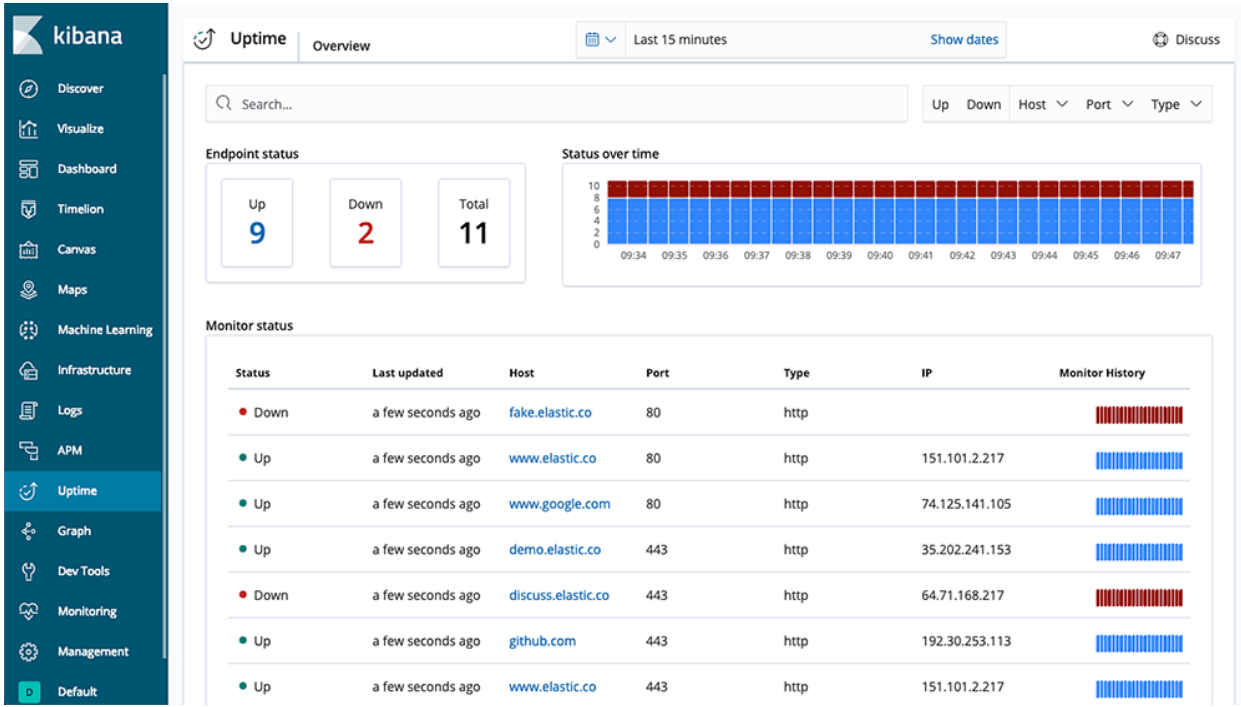
Lightweight Shipper for Uptime Monitoring



elastic

Uptime UI

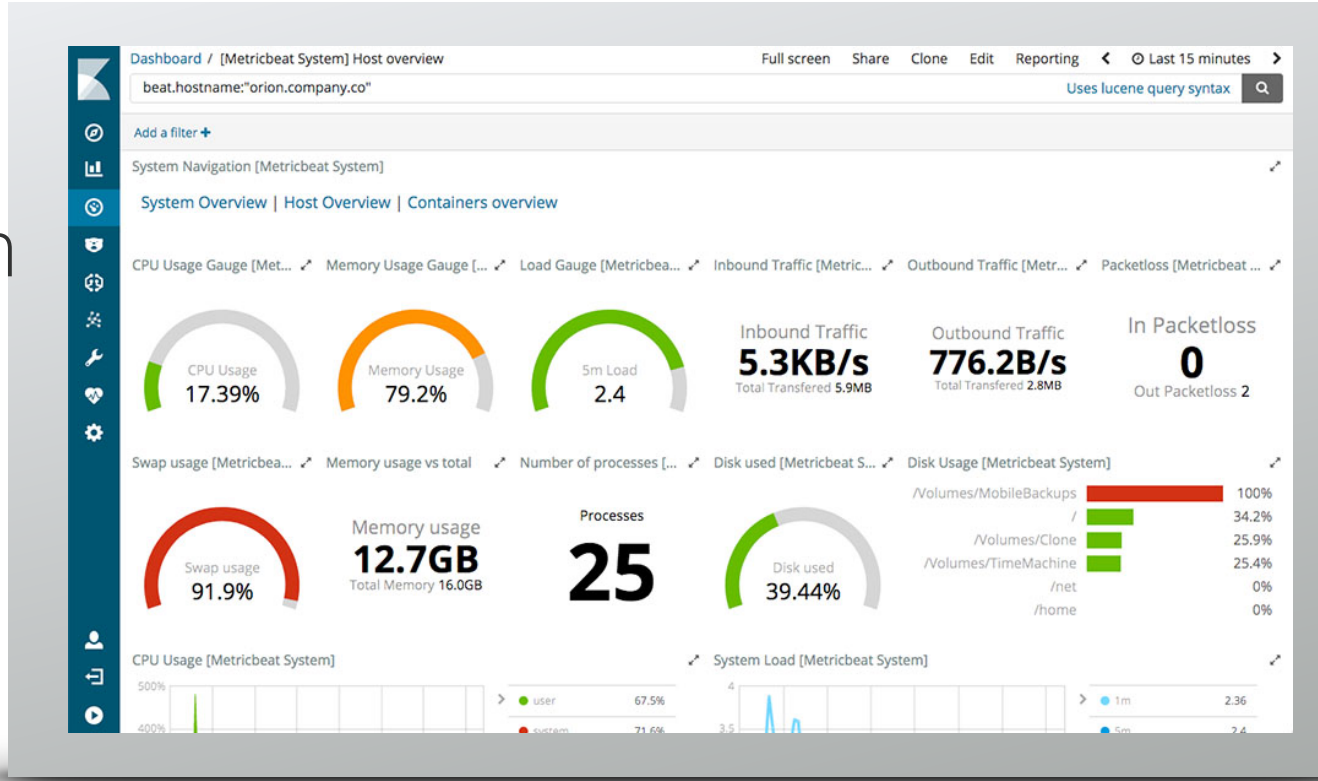
Dedicated Uptime Monitoring UI for Kibana



elastic

Metricbeat

Collect system and application **metrics**



elastic

Metricbeat

lots of **modules**


System


Apache


Docker

NGINX


HAProxy


Kafka


MongoDB

MySQL


PostgreSQL


Prometheus


Jolokia


Add your own

elastic

Metricbeat モジュール

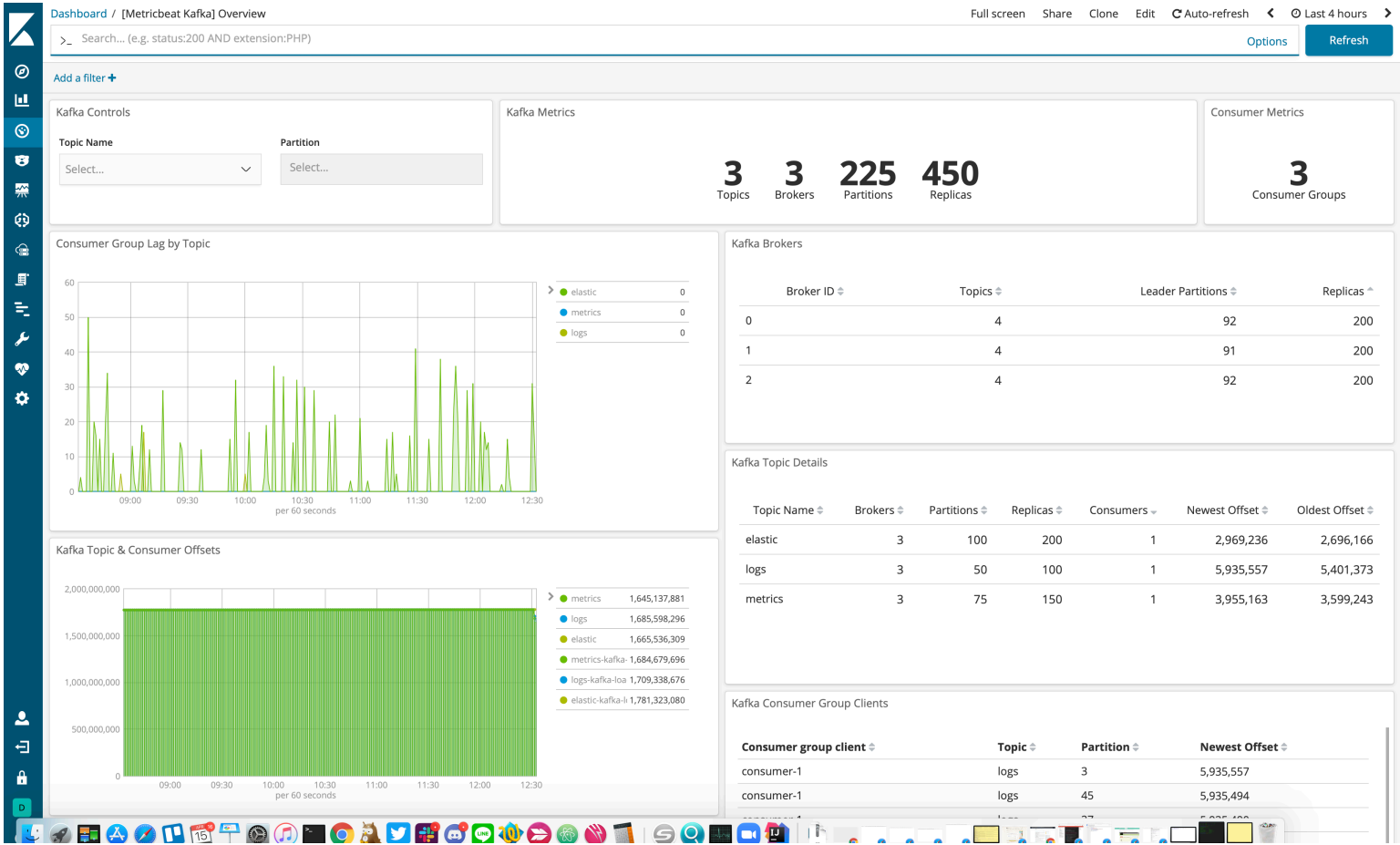
Aerospike module
Apache module
Ceph module
Couchbase module
Docker module
Dropwizard module
Elasticsearch module
Etcd module
Golang module
Graphite module
HAProxy module
HTTP module
Jolokia module
Kafka module
Kibana module
Kubernetes module
kvm module
Logstash module
Memcached module
MongoDB module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

Metricbeat モジュール

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

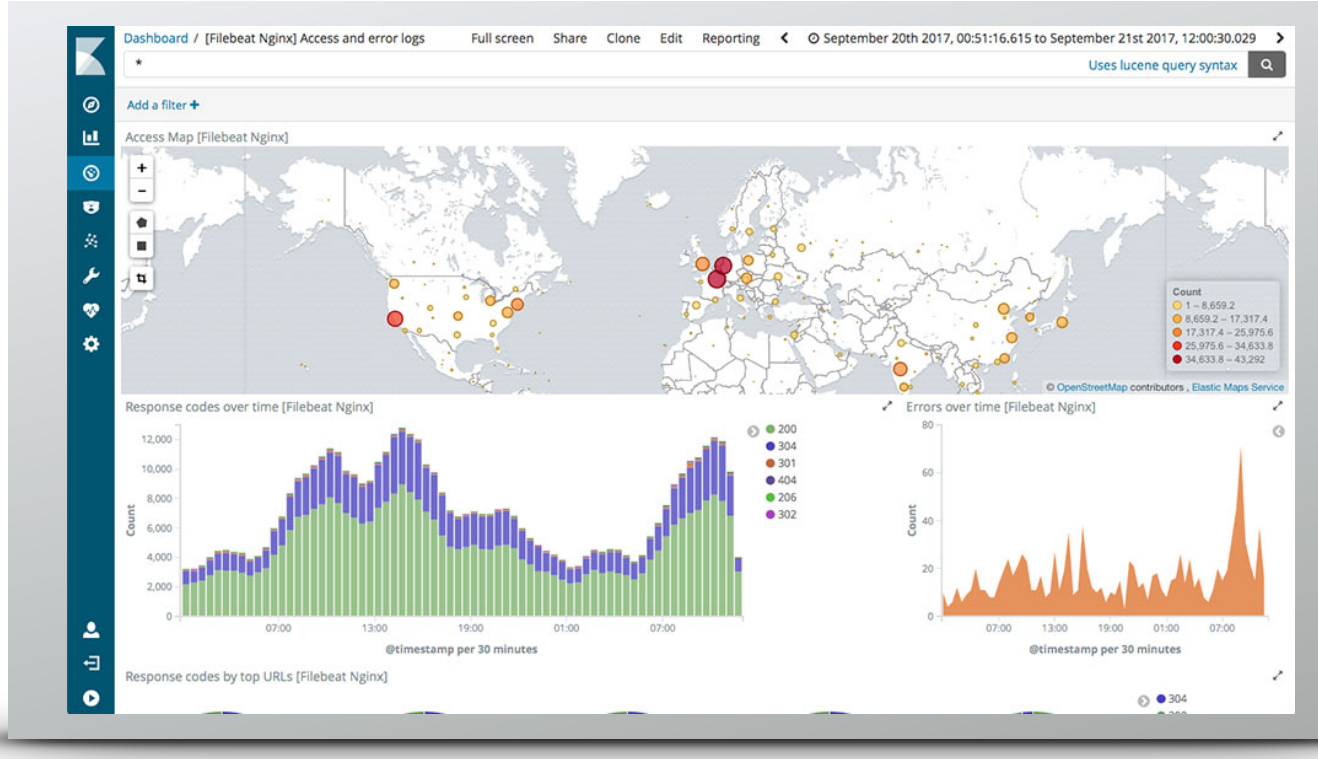
elastic

デモ画面 - Metricbeat Kafka module



Filebeat

tail log from
file



elastic

many **modules**

Apache

Nginx

Auditd

MySQL

Filebeat modules - v6.4.2

Apache2 module

Auditd module

Icinga module

IIS module

Kafka module

Logstash module

MongoDB module

MySQL module

Nginx module

Osquery module

PostgreSQL module

Redis module

System module

Traefik module

Filebeat modules - v6.4.2

Apache2 module

Auditd module

Icinga module

IIS module

Kafka module

Logstash module

MongoDB module

MySQL module

Nginx module

Osquery module

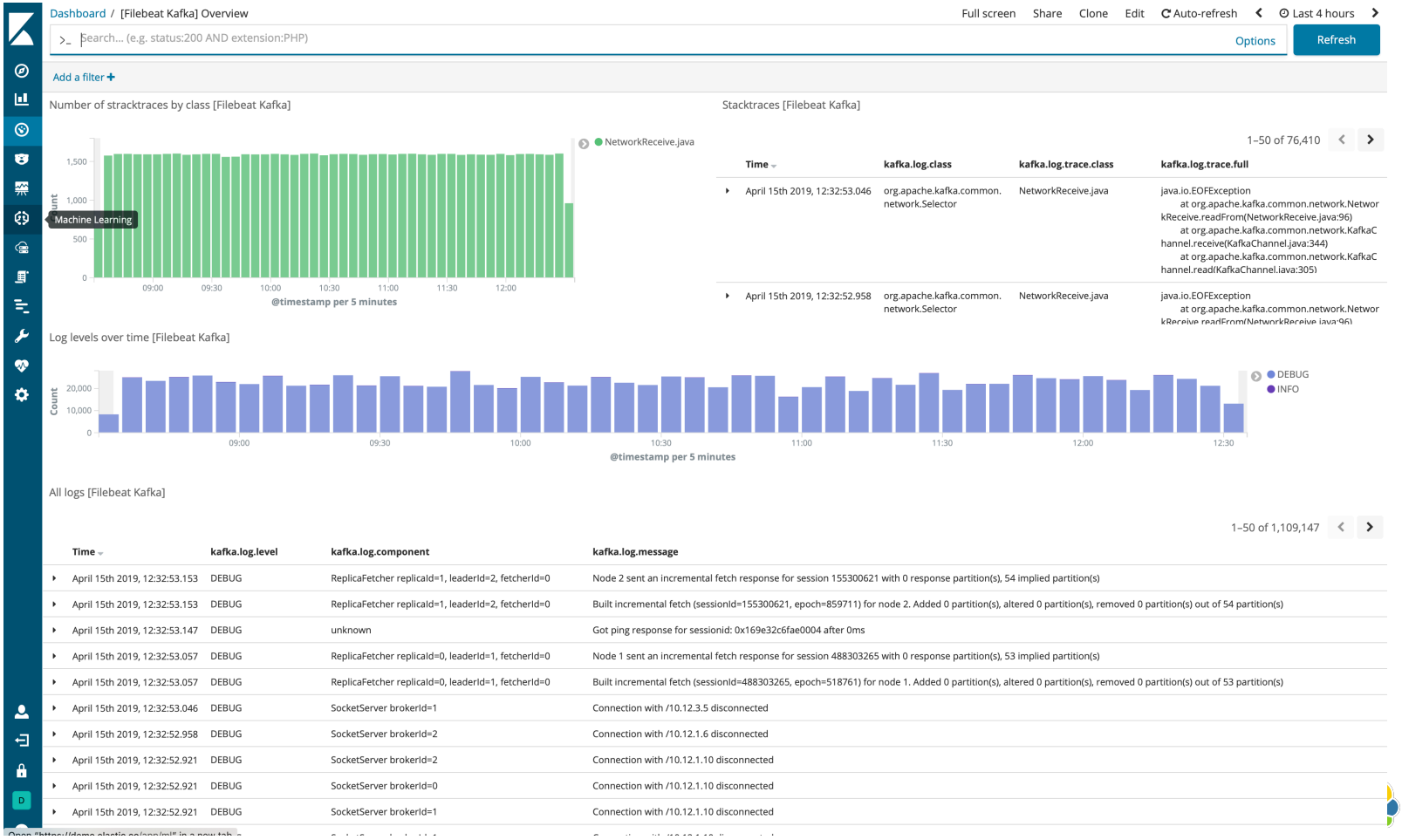
PostgreSQL module

Redis module

System module

Traefik module

デモ画面 - Filebeat Kafka module



elastic

さらに活用するには？

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

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

Chart interval: 1h

Use full server-* data

New job from index pattern server-*

Aggregation

Sum

Field

total

Bucket span

30m

Estimate bucket span

Sparse data

Name

sum-total

Description

Job description

Advanced

Create Job

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

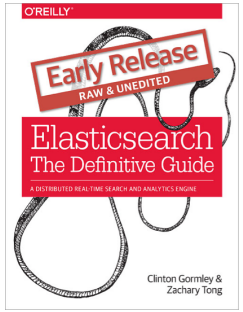
今すぐトライ

lastic

参考文献

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

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



elastic

参考サイト

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

elastic

Thank you!

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