Elastic再入門

Jun Ohtani, Kosho Owa

2019/03/20 @Elastic

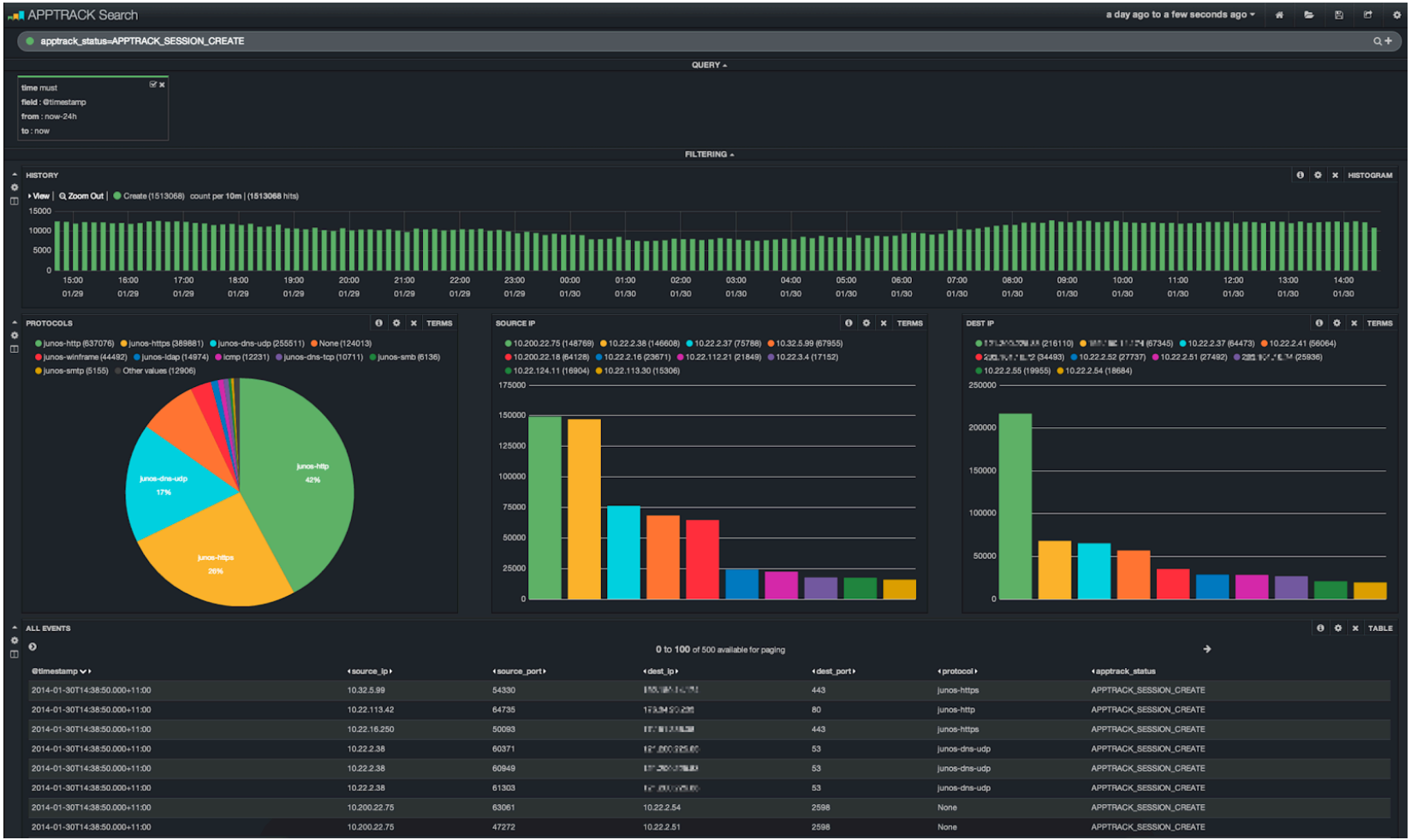
どのくらい再入門？

Elasticsearch (Es)
0.90系から触ってない人？

Kibana 3系

Es1.x系から触ってない人？

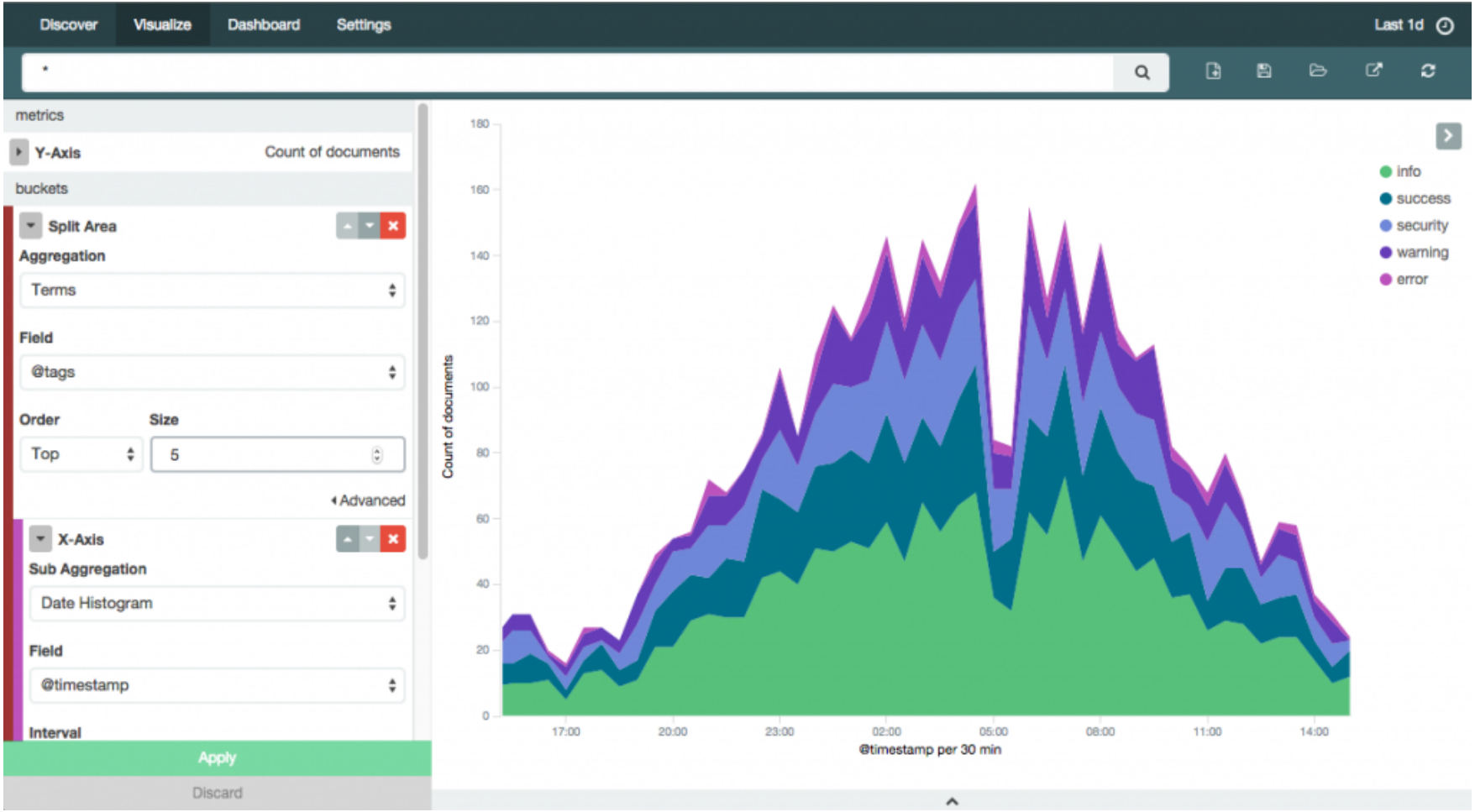
Kibana 3系


APPTRACK Search
a day ago to a few seconds ago
apptrack_status=APPTRACK_SESSION_CREATE
QUERY
time must
field : @timestamp
from : now-24h
to : now
FILTERING
HISTORY
HISTOGRAM
View | Zoom Out | Create (1513068) count per 10m | (1513068 hits)
15000
10000
5000
0
15:00 01/29
16:00 01/29
17:00 01/29
18:00 01/29
19:00 01/29
20:00 01/29
21:00 01/29
22:00 01/29
23:00 01/29
00:00 01/30
01:00 01/30
02:00 01/30
03:00 01/30
04:00 01/30
05:00 01/30
06:00 01/30
07:00 01/30
08:00 01/30
09:00 01/30
10:00 01/30
11:00 01/30
12:00 01/30
13:00 01/30
14:00 01/30
PROTOCOLS
TERMS
junos-http (637076)
junos-https (389881)
junos-dns-udp (255511)
None (124013)
junos-winframe (44492)
junos-ldap (14974)
icmp (12231)
junos-dns-tcp (10711)
junos-smb (6136)
junos-smtp (5155)
Other values (12906)
junos-http 42%
junos-dns-udp 17%
junos-https 26%
SOURCE IP
TERMS
10.200.22.75 (148769)
10.22.2.38 (146608)
10.22.2.37 (75788)
10.32.5.99 (67955)
10.200.22.18 (64128)
10.22.2.16 (23671)
10.22.112.21 (21849)
10.22.3.4 (17152)
10.22.124.11 (16904)
10.22.113.30 (15306)
175000
150000
125000
100000
75000
50000
25000
0
DEST IP
TERMS
(216110)
(67345)
10.22.2.37 (64473)
10.22.2.41 (56064)
(34493)
10.22.2.52 (27737)
10.22.2.51 (27492)
(25936)
10.22.2.55 (19955)
10.22.2.54 (18684)
250000
200000
150000
100000
50000
0
ALL EVENTS
TABLE
0 to 100 of 500 available for paging
@timestamp
source_ip
source_port
dest_ip
dest_port
protocol
apptrack_status
2014-01-30T14:38:50.000+11:00 10.32.5.99 54330 443 junos-https APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.22.113.42 64735 80 junos-http APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.22.16.250 50093 443 junos-https APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.22.2.38 60371 53 junos-dns-udp APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.22.2.38 60949 53 junos-dns-udp APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.22.2.38 61303 53 junos-dns-udp APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.200.22.75 63061 10.22.2.54 2598 None APPTRACK_SESSION_CREATE
2014-01-30T14:38:50.000+11:00 10.200.22.75 47272 10.22.2.51 2598 None APPTRACK_SESSION_CREATE

elastic

Es2.x系から触ってない人？

Kibana 4系


Discover
Visualize
Dashboard
Settings
Last 1d
*
metrics
Y-Axis
Count of documents
buckets
Split Area
Aggregation
Terms
Field
@tags
Order
Size
Top
5
Advanced
X-Axis
Sub Aggregation
Date Histogram
Field
@timestamp
Interval
Apply
Discard
Count of documents
180
160
140
120
100
80
60
40
20
0
17:00
20:00
23:00
02:00
05:00
08:00
11:00
14:00
@timestamp per 30 min
info
success
security
warning
error

elastic

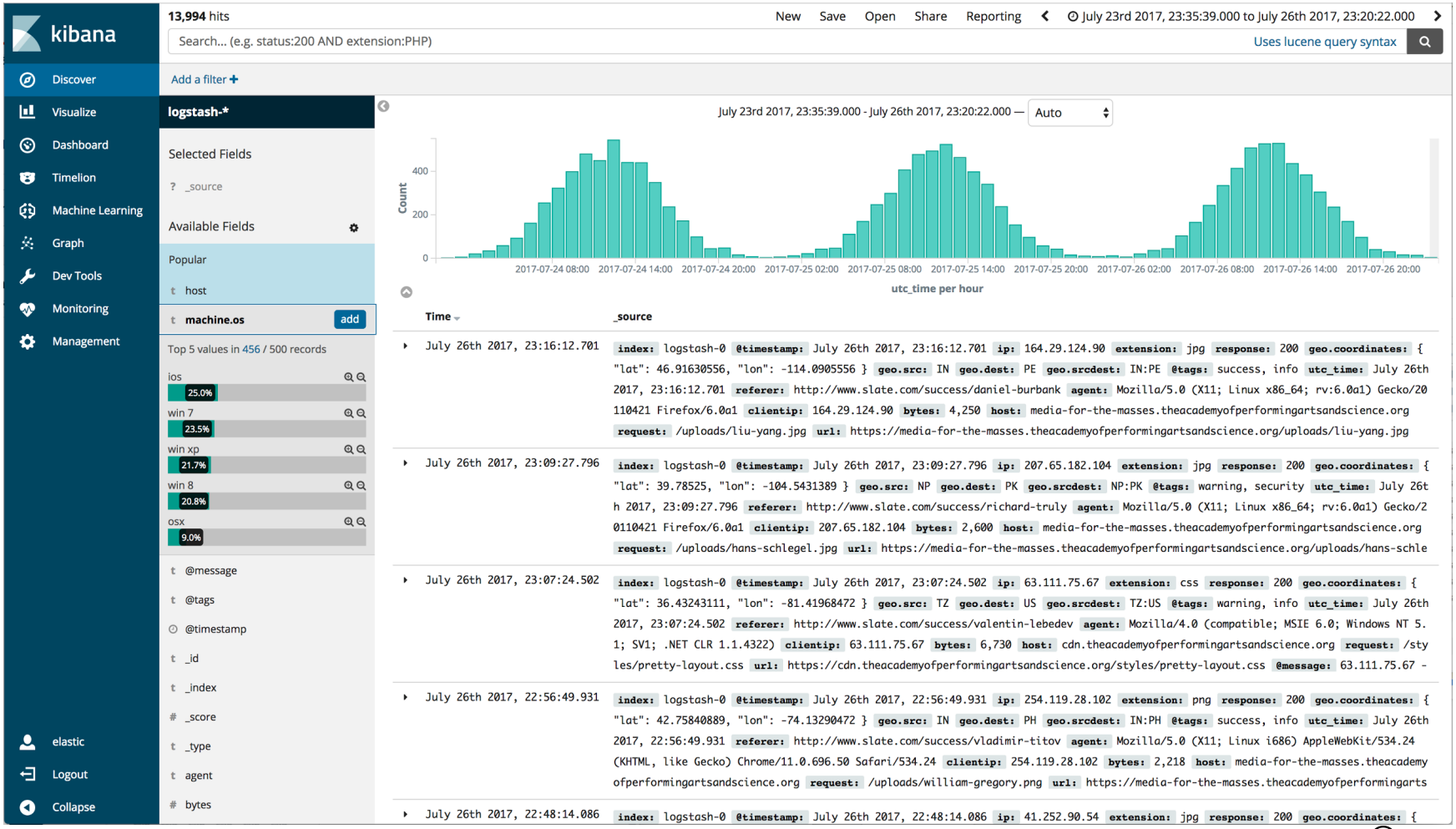
5.x系から触ってない人？

Kibana 5系


kibana
Elastic Stack - Apache Logs V4
New
Add
Save
Open
Share
Options
Reporting
April 2nd 2016, 16:20:52.026 to April 9th 2016, 23:22:52.856
*
Discover
Visualize
Dashboard
Timelion
Graph
Dev Tools
Monitoring
Management
Guest User
Logout
Collapse
Apache - Total Visitors
11,979,137
Count
Apache - Unique Visitors
128,088
Unique Visitors
Apache - Bytes and Count
United States
China
France
Germany
India
Count
200,000
70,000
40,000
20,000
7,000
4,000
2,000
700
400
200
2016-04-03 17:00
2016-04-04 17:00
2016-04-05 17:00
2016-04-06 17:00
2016-04-07 17:00
2016-04-08 17:00
@timestamp per hour
Apache - Country and Status
United States
China
France
Germany
India
200
304
301
404
416
206
412
Apache - Unique Visitors by City
City
Unique Visitors
Beijing 243,706
Woodbridge 134,791
Seattle 123,545
Seoul 111,663
Mumbai 109,801
Tokyo 106,182
New York 102,947
Bangalore 102,738
Apache - Country traffic by hour
United States
China
Germany
India
United Kingdom
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
Hour of Day
Apache - Top OS
Windows 95
Windows 2000
Windows NT
Windows 98
Windows 10
Windows 7
FreeBSD
Fedora
iOS
Mac OS X
Chrome OS
Windows XP
Kindle
Ubuntu
Linux
Other
Windows
OpenBSD
Windows 8.1
Android
Windows Phone
Solaris
Windows 8
BlackBerry OS
Windows Vista
Apache - Visitor Map
Calgary

elastic

6.2系から触ってない人？


kibana
13,994 hits
New Save Open Share Reporting
July 23rd 2017, 23:35:39.000 to July 26th 2017, 23:20:22.000
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Collapse
logstash-*
Selected Fields
? _source
Available Fields
Popular
t host
t machine.os add
Top 5 values in 456 / 500 records
ios 25.0%
win 7 23.5%
win xp 21.7%
win 8 20.8%
osx 9.0%
t @message
t @tags
@timestamp
t _id
t _index
_score
t _type
t agent
bytes
July 23rd 2017, 23:35:39.000 - July 26th 2017, 23:20:22.000 — Auto
Count
400
200
0
2017-07-24 08:00 2017-07-24 14:00 2017-07-24 20:00 2017-07-25 02:00 2017-07-25 08:00 2017-07-25 14:00 2017-07-25 20:00 2017-07-26 02:00 2017-07-26 08:00 2017-07-26 14:00 2017-07-26 20:00
utc_time per hour
Time
_source
July 26th 2017, 23:16:12.701 index: logstash-0 @timestamp: July 26th 2017, 23:16:12.701 ip: 164.29.124.90 extension: jpg response: 200 geo.coordinates: { "lat": 46.91630556, "lon": -114.0905556 } geo.src: IN geo.dest: PE geo.srcdest: IN:PE @tags: success, info utc_time: July 26th 2017, 23:16:12.701 referer: http://www.slate.com/success/daniel-burbank agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 clientip: 164.29.124.90 bytes: 4,250 host: media-for-the-masses.theacademyofperformingartsandscience.org request: /uploads/liu-yang.jpg url: https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/liu-yang.jpg
July 26th 2017, 23:09:27.796 index: logstash-0 @timestamp: July 26th 2017, 23:09:27.796 ip: 207.65.182.104 extension: jpg response: 200 geo.coordinates: { "lat": 39.78525, "lon": -104.5431389 } geo.src: NP geo.dest: PK geo.srcdest: NP:PK @tags: warning, security utc_time: July 26th 2017, 23:09:27.796 referer: http://www.slate.com/success/richard-truly agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 clientip: 207.65.182.104 bytes: 2,600 host: media-for-the-masses.theacademyofperformingartsandscience.org request: /uploads/hans-schlegel.jpg url: https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/hans-schle
July 26th 2017, 23:07:24.502 index: logstash-0 @timestamp: July 26th 2017, 23:07:24.502 ip: 63.111.75.67 extension: css response: 200 geo.coordinates: { "lat": 36.43243111, "lon": -81.41968472 } geo.src: TZ geo.dest: US geo.srcdest: TZ:US @tags: warning, info utc_time: July 26th 2017, 23:07:24.502 referer: http://www.slate.com/success/valentin-lebedev agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) clientip: 63.111.75.67 bytes: 6,730 host: cdn.theacademyofperformingartsandscience.org request: /styles/pretty-layout.css url: https://cdn.theacademyofperformingartsandscience.org/styles/pretty-layout.css @message: 63.111.75.67 -
July 26th 2017, 22:56:49.931 index: logstash-0 @timestamp: July 26th 2017, 22:56:49.931 ip: 254.119.28.102 extension: png response: 200 geo.coordinates: { "lat": 42.75840889, "lon": -74.13290472 } geo.src: IN geo.dest: PH geo.srcdest: IN:PH @tags: success, info utc_time: July 26th 2017, 22:56:49.931 referer: http://www.slate.com/success/vladimir-titov agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 clientip: 254.119.28.102 bytes: 2,218 host: media-for-the-masses.theacademyofperformingartsandscience.org request: /uploads/william-gregory.png url: https://media-for-the-masses.theacademyofperformingarts
July 26th 2017, 22:48:14.086 index: logstash-0 @timestamp: July 26th 2017, 22:48:14.086 ip: 41.252.90.54 extension: jpg response: 200 geo.coordinates: {

elastic

Elastic Stackとは？

Elastic Stack

Kibana

可視化、管理

Elasticsearch

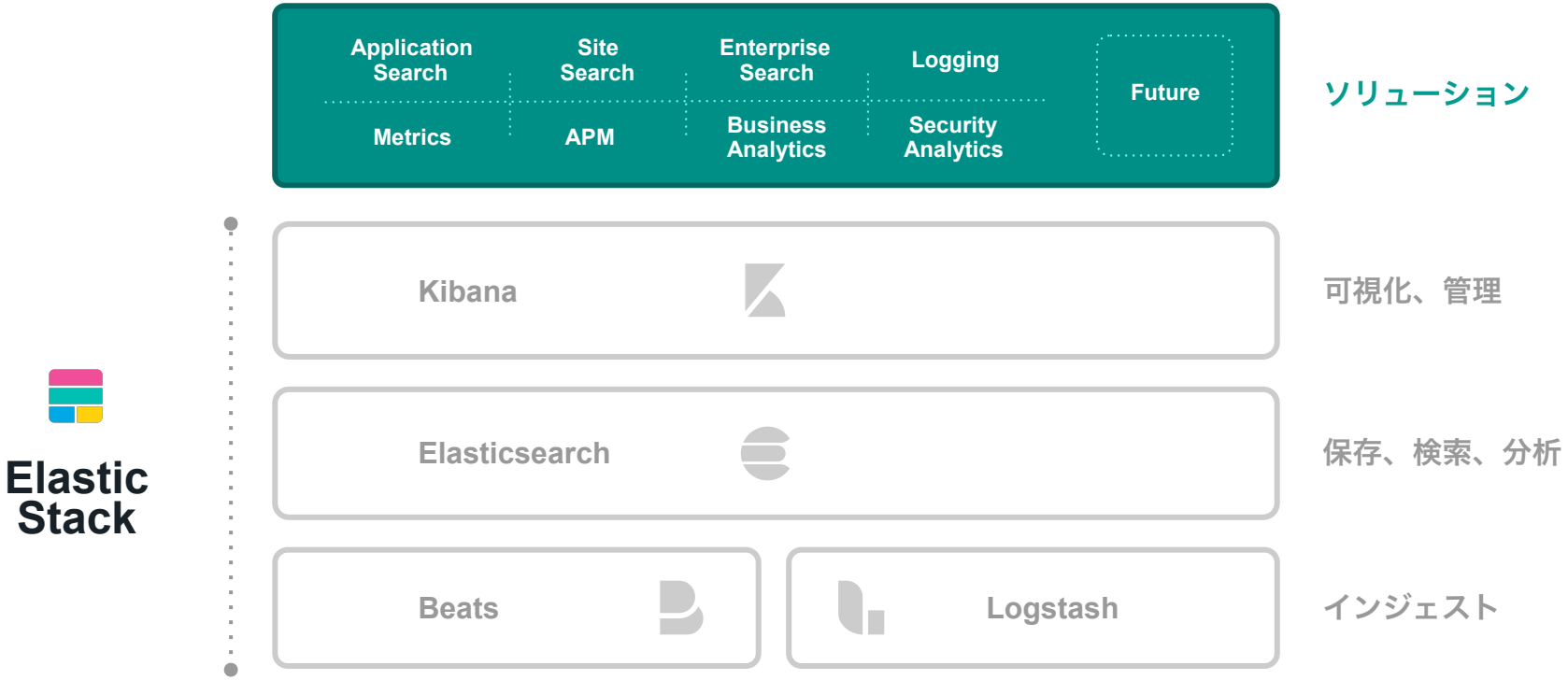
保存、検索、分析

Beats

Logstash

インジェスト

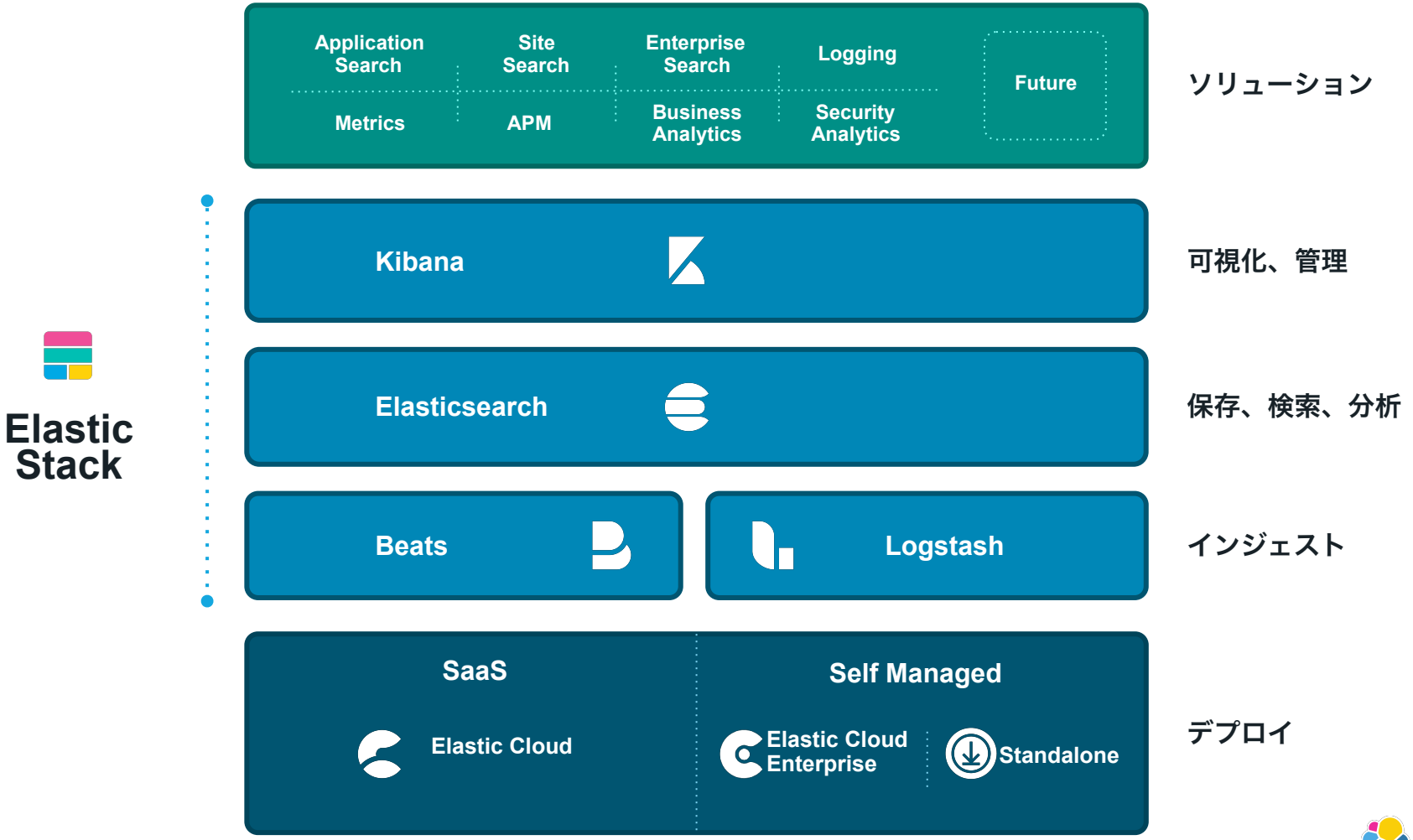
elastic


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 Stack

Elastic Stack

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

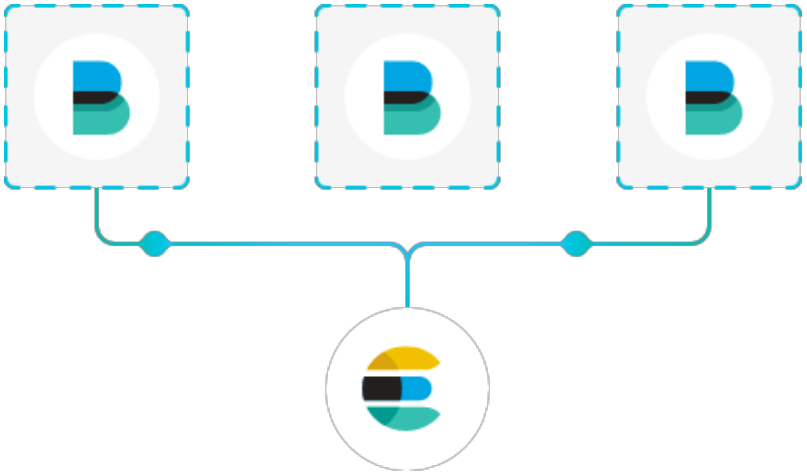
elastic


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 Stack
SaaS
Self Managed
Elastic Cloud
Elastic Cloud Enterprise
Standalone
デプロイ

beats

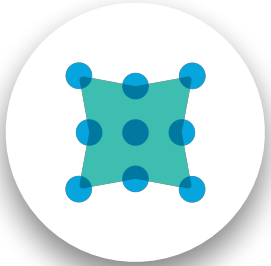
Beats

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

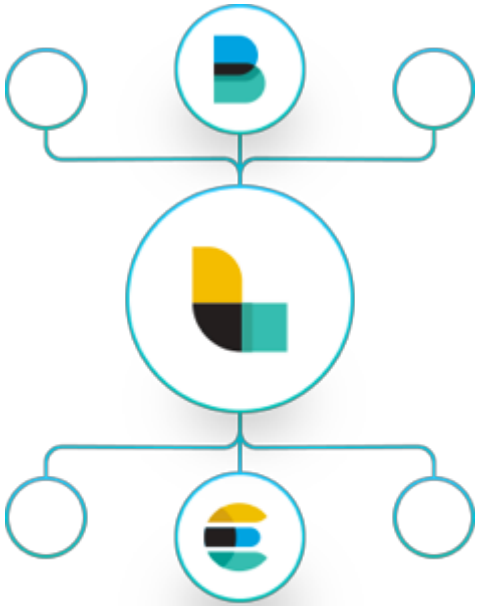
+40 community Beats

elastic

logstash

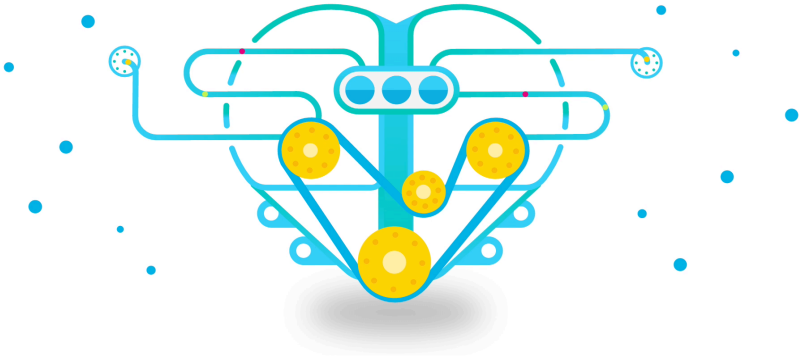
Logstash

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

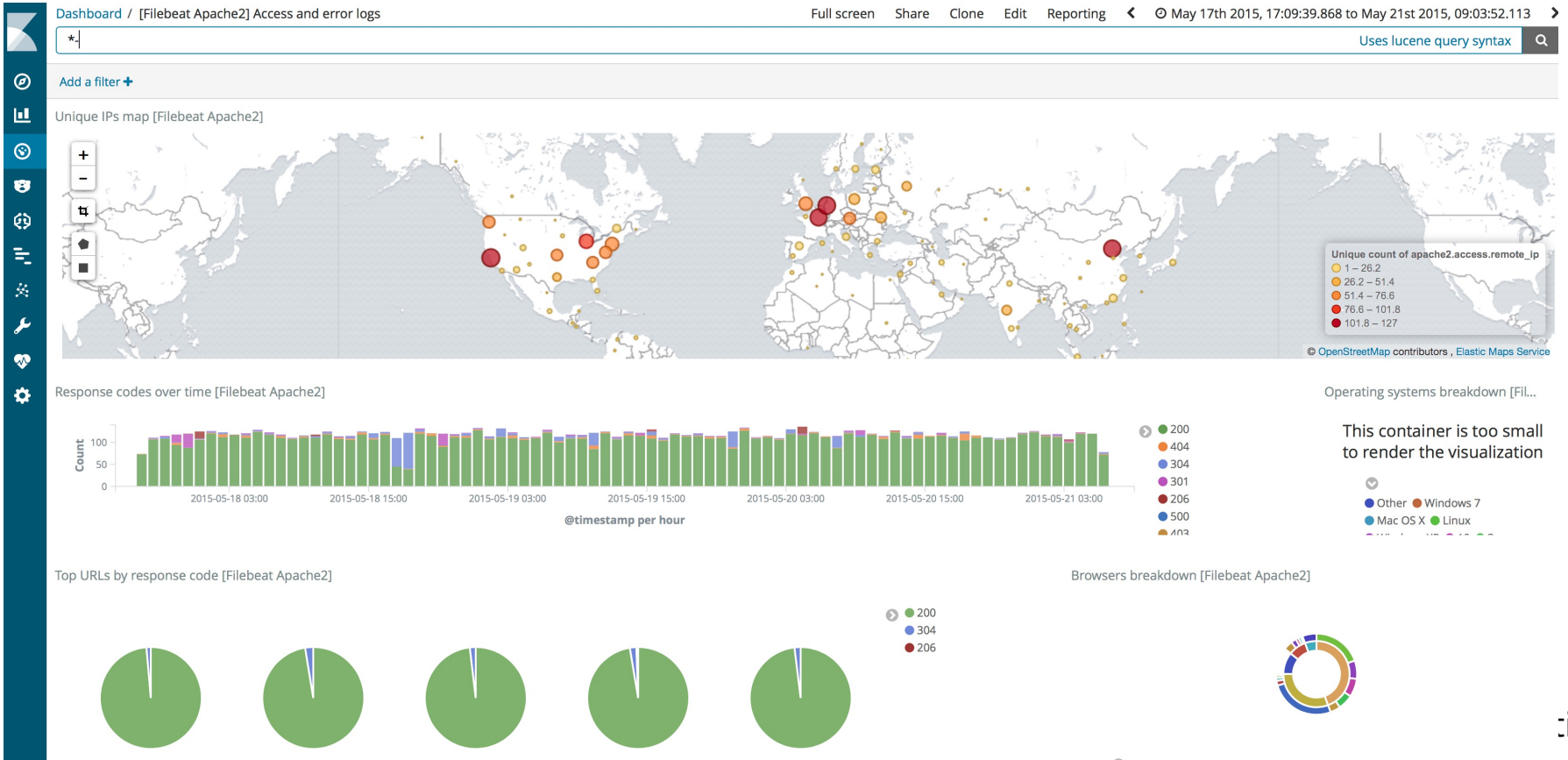
kibana

Kibana

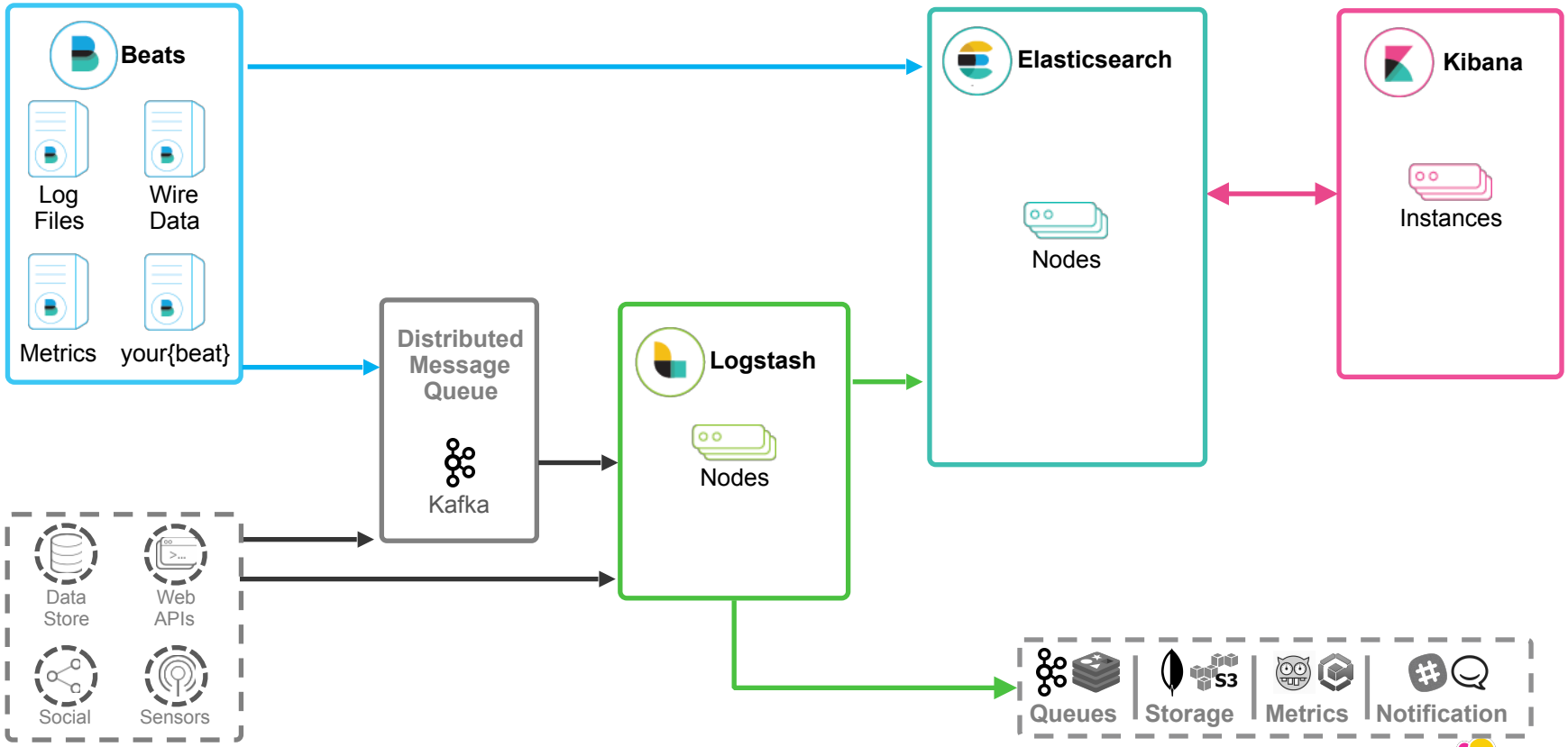
Window into the Elastic Stack

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

Reporting
ine Learni
ger Canva
lonitoring CSV

X-PACK

PAID

FREE

OPEN

PRODUCT.ZIP

OPT IN

DEFAULT

Ingestions

Distributed

Engine

Data Collection

Dashboard

Visualizations

Agents

Edge Collection

estions

Enrichment

Dashboard

ction

Distributed

Search Engine

Data Collection

OSS

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

メールアドレス トライアル

送信することにより、Elastic Cloud標準利用規約に同意し、Elasticより各種通知のメールを受け取ることを了承したものとみなされます。個人情報はElasticのプライバシーポリシーに基づいて取り扱われます。

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

メールアドレス トライアル

送信することにより、Elastic Cloud標準利用規約に同意し、Elasticより各種通知のメールを受け取ることを了承したものとみなされます。個人情報はElasticのプライバシーポリシーに基づいて取り扱われます。

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

メールアドレス トライアル

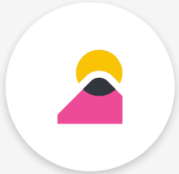
送信することにより、Elastic Cloud標準利用規約に同意し、Elasticより各種通知のメールを受け取ることを了承したものとみなされます。個人情報はElasticのプライバシーポリシーに基づいて取り扱われます。

Solutions

Elasticのソリューション

ログファイルの収集や、ブロックすべきIPアドレスの特定、数百万のドキュメントの高速な検索まで。
Elastic Stackの数多くの活用法から、一部をご紹介します。

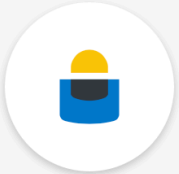
ログ分析



メトリック

APM

サイト内検索



セキュリティ分析

アプリ検索

Business Analytics

Enterprise Search

最新情報をお届けします。

メールアドレス

送信

Infrastructure UI

Infrastructure Solution

Beta | Basic (free)

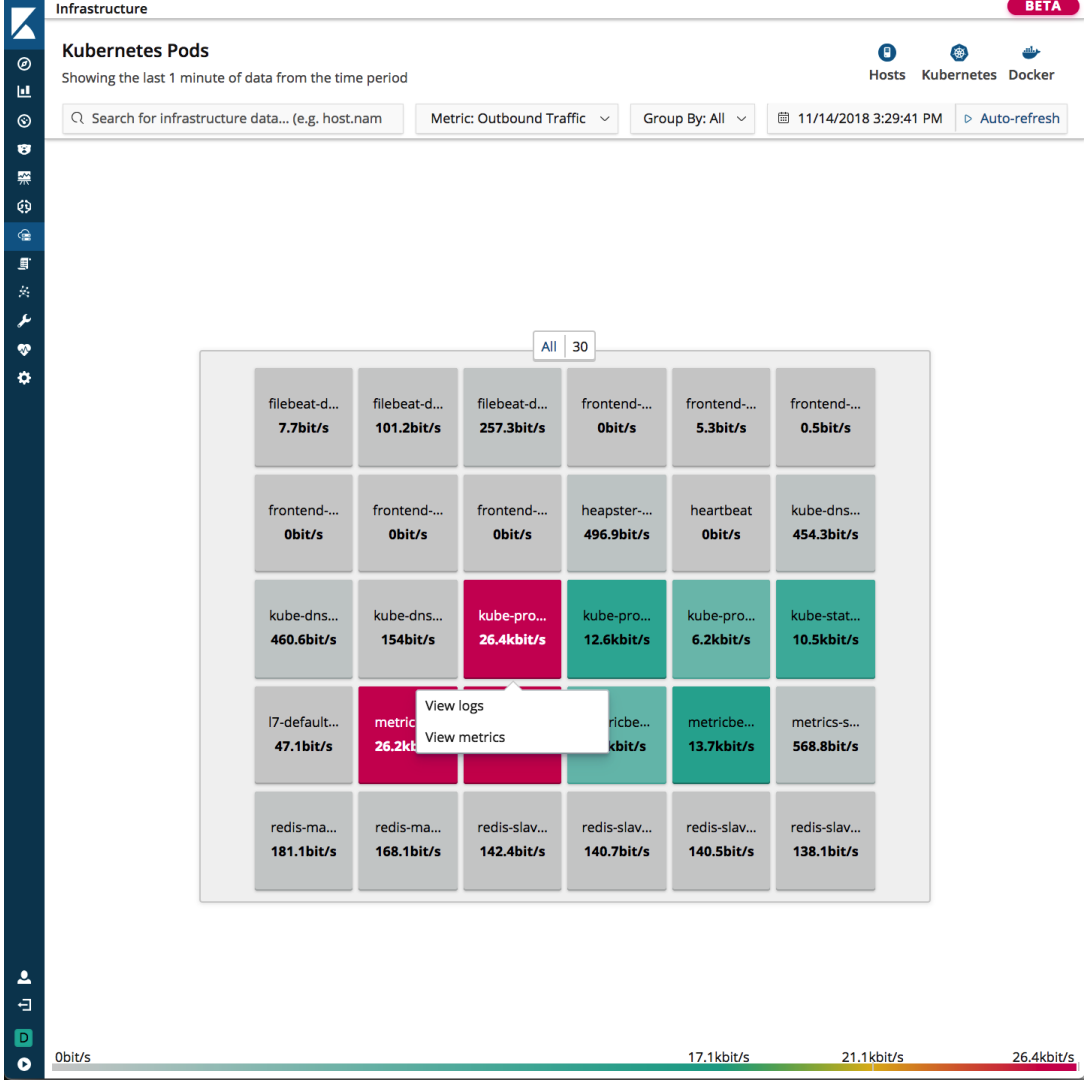
インフラオペレーター向けに特化

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 UI

Logs Solution

Beta | Basic (free)

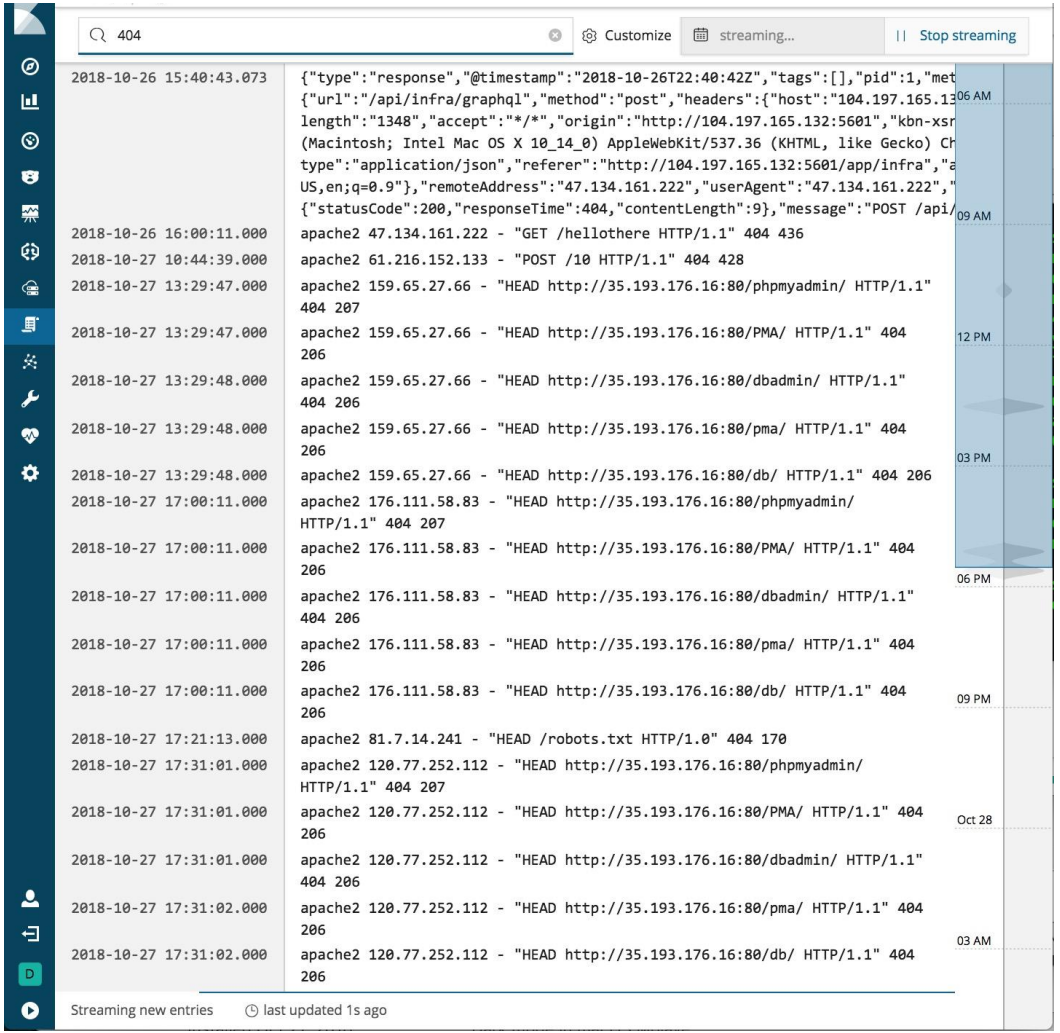
ライブでログのトラブルシューティングを助ける軽量なログビューアー

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



APM

Java & Go Agents GA

OSS

Javaサポート:

Java 7-11

テクノロジー/フレームワーク:

Servlet API, Spring Web MVC, Spring Boot, Tomcat, WildFly, Jetty, Websphere, JDBCなど

Goのサポート:

Go 1.8+

テクノロジー/フレームワーク:

httprouter, Echo, Gin, gorilla/mux, database/sql, GORM, gocql, gRPC

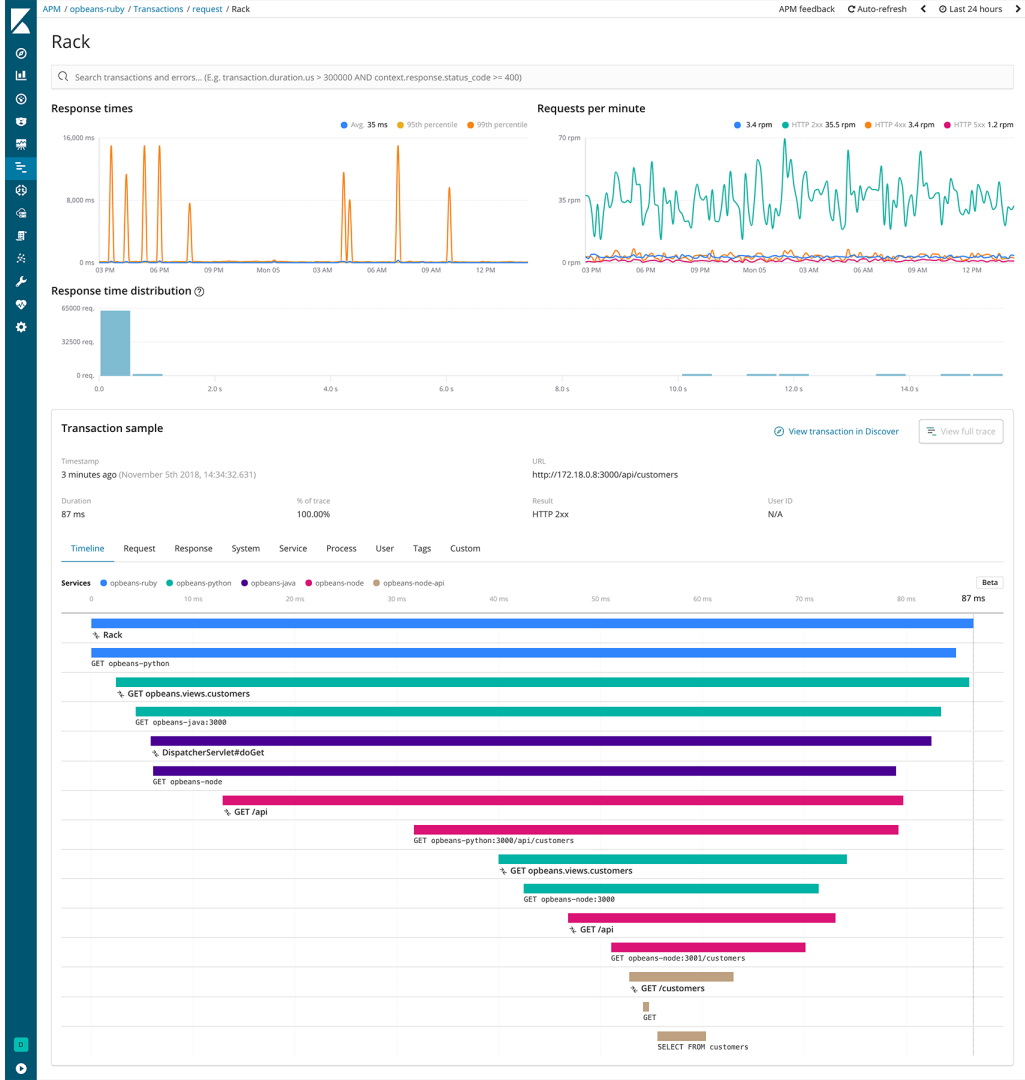
Distributed Tracing

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



機能をピックアップ

elastic 製品 Cloud サービス 導入事例 リソース ダウンロード お問い合わせ JP

X-Pack 今すぐはじめる

Elasticsearch SQL

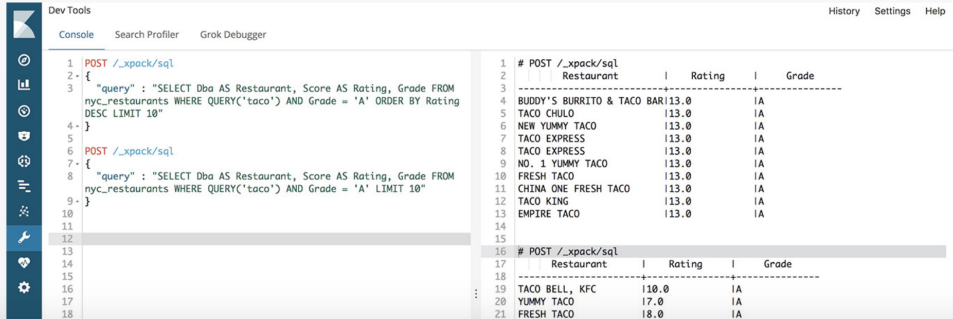
Elasticsearch has the speed, power, and flexibility your data needs — and it speaks SQL.

NEW Elasticsearch SQL is now here, making scalable search and relevance more accessible to SQL developers everywhere.

Read More

Scalable Search with Scoring... and SQL

Elasticsearch is a full text search engine with all the goodies you'd expect, like relevance scoring, stemming, synonyms, and more. And since it's a distributed document store — with horizontal scalability — it can handle billions of rows of data without skipping a beat. With Elasticsearch SQL, you can access that full text search, blazing speed, and effortless scalability with a familiar query syntax.



Rollups API (6.3 - Experimental)

容量が。。。

- 定期的に統計データを集約して保存するElasticsearchのJobを登録
- 主な利点は容量の削減
- データが少なくなるため
  - Queryがより高速に
  - 少ないノードでデータを管理
  - Snapshotがより小さく
  - データの保持期間がより長く
- 1つのクエリでロールアップしたデータとしてないデータを問い合わせ

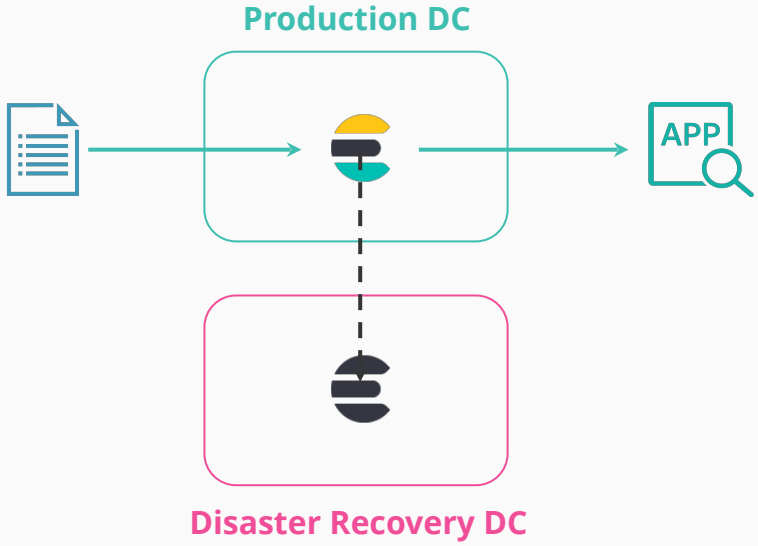
X-Pack feature (Basic, free)

Cross-Cluster Replication

Beta | Platinum

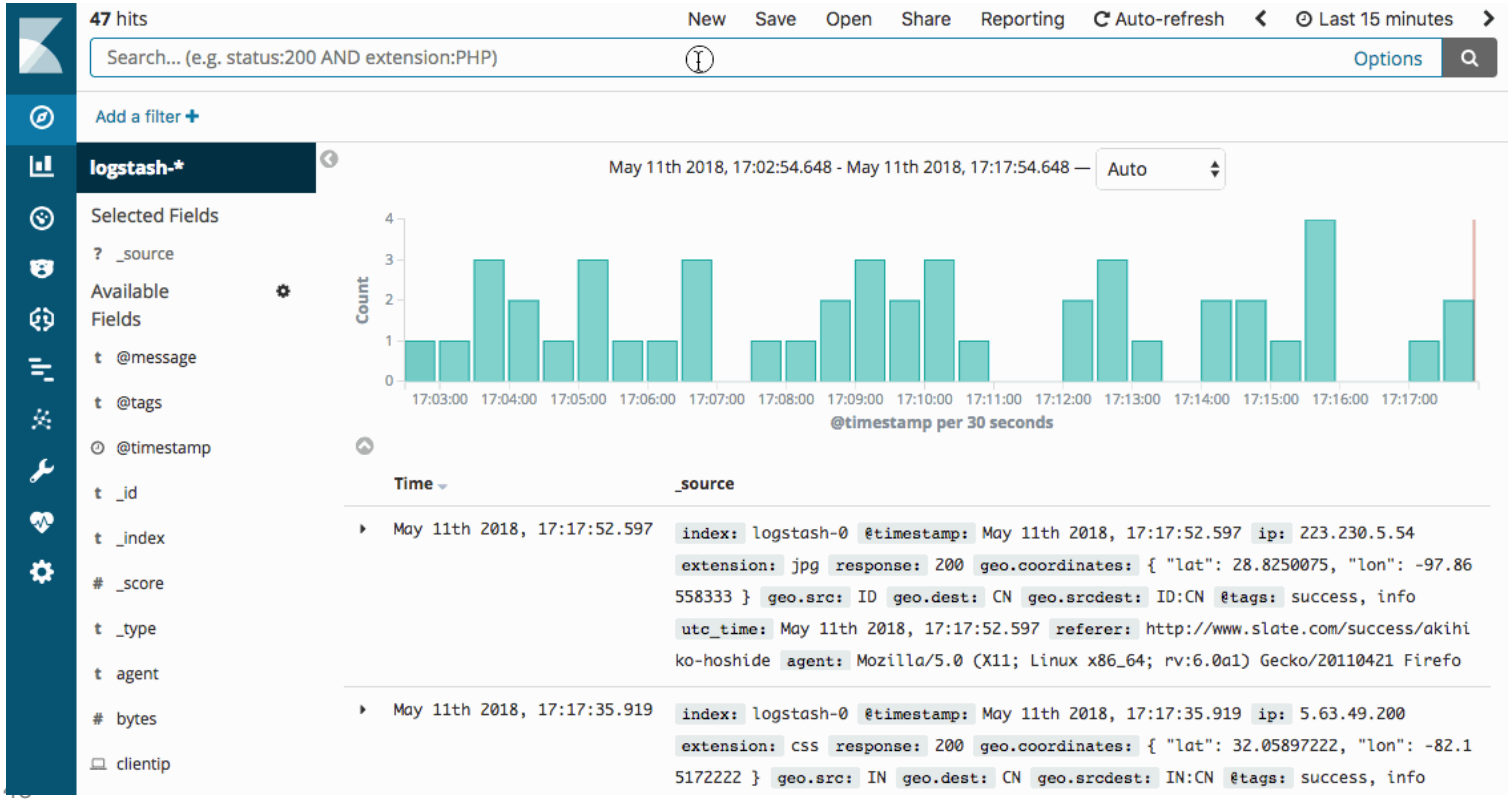
Elasticsearch クラスター間でインデックスを複製

これまでの回避策では、運用上のオーバーヘッド、複数のテクノロジーの採用、システムの複雑さなどがあった



Leader Follower

Kibana Query Languageで自動補完

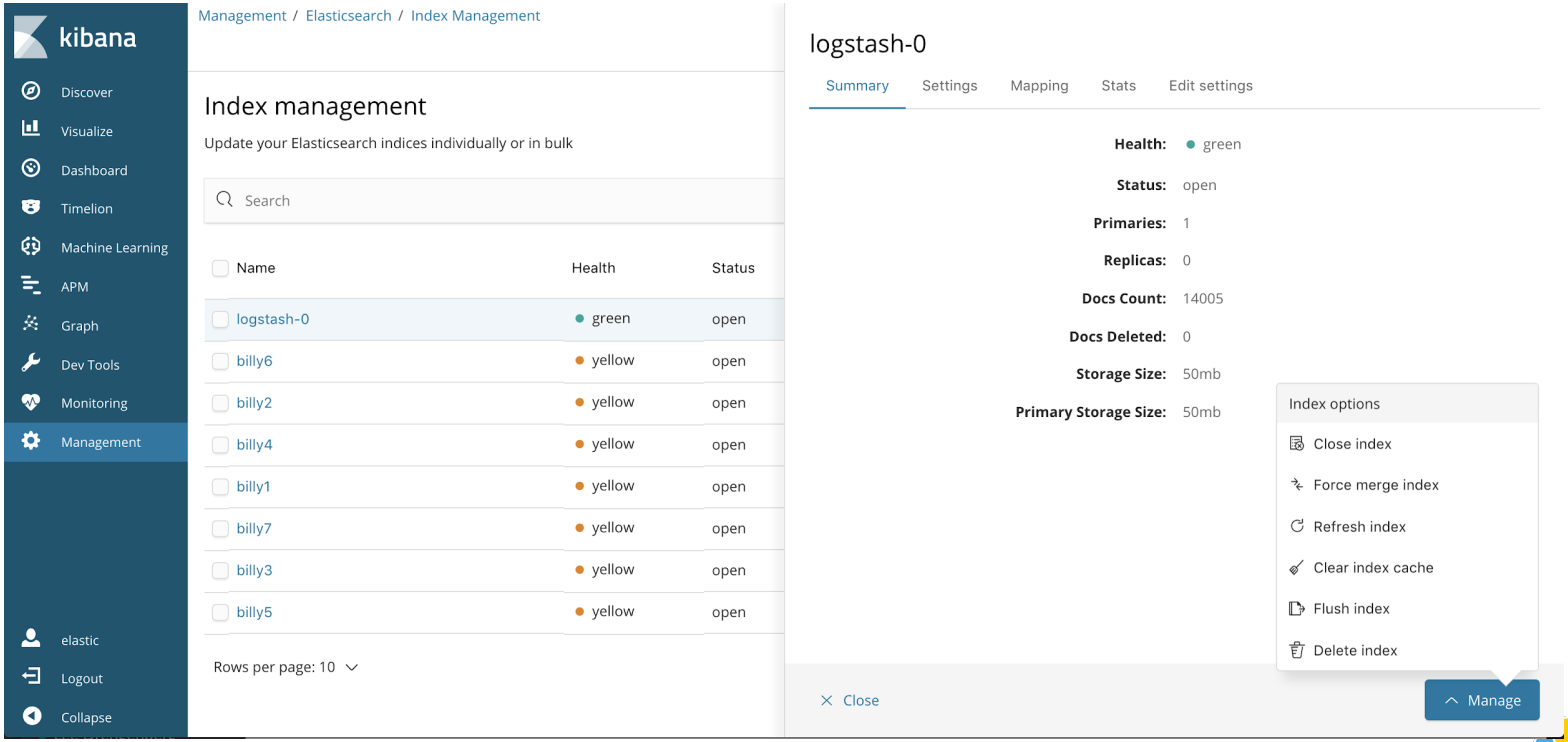


elastic

X-Pack feature (Basic, free)

Index Management UI

UIでIndex管理



elastic

Canvas: Create live pixel-perfect presentations

Beta | Basic (free)

Spaces

Basic (free) / Gold

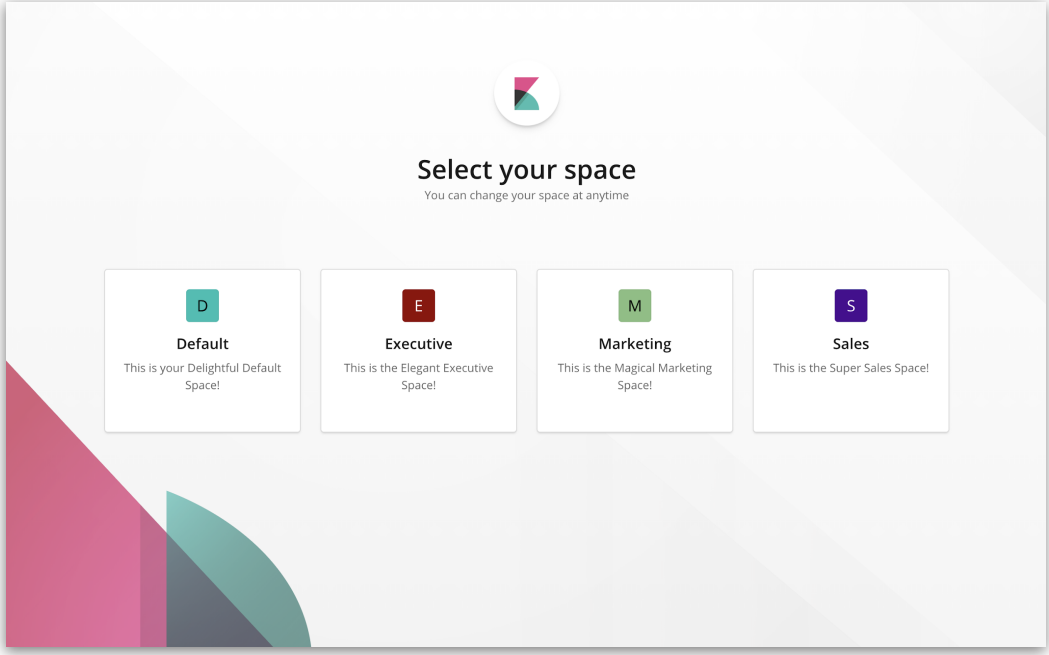
ビジュアル、ダッシュボードなどを、独立した**スペース**に分けて整理

ロールベースのアクセス制御を使用して空間へのユーザーアクセスを制御する

マルチテナントの簡素化

ユースケース:

- 組織
- 段階的フェーズ (開発、ステージ、プロダクションなど)
- セキュリティ (アクセスの制限)



Beats Central Management

Beta | Gold

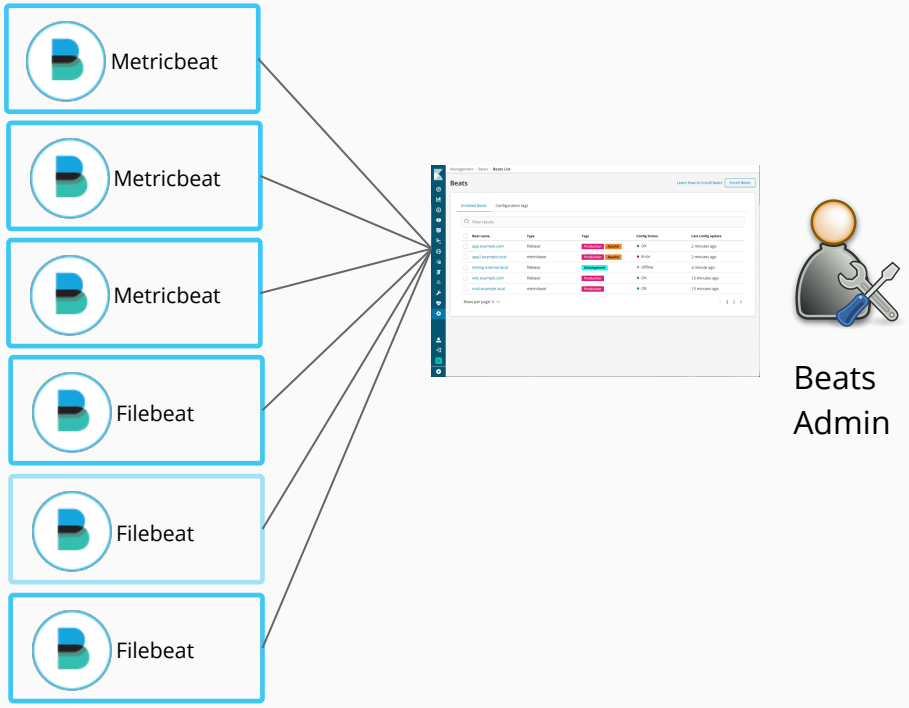
Beats 群を一元管理

- Beats の登録と解除
- 設定の追加、変更、削除

UI および API 経由で管理

現在のサポート対象:

- Filebeat (入力、モジュール)
- Metricbeat (モジュール)



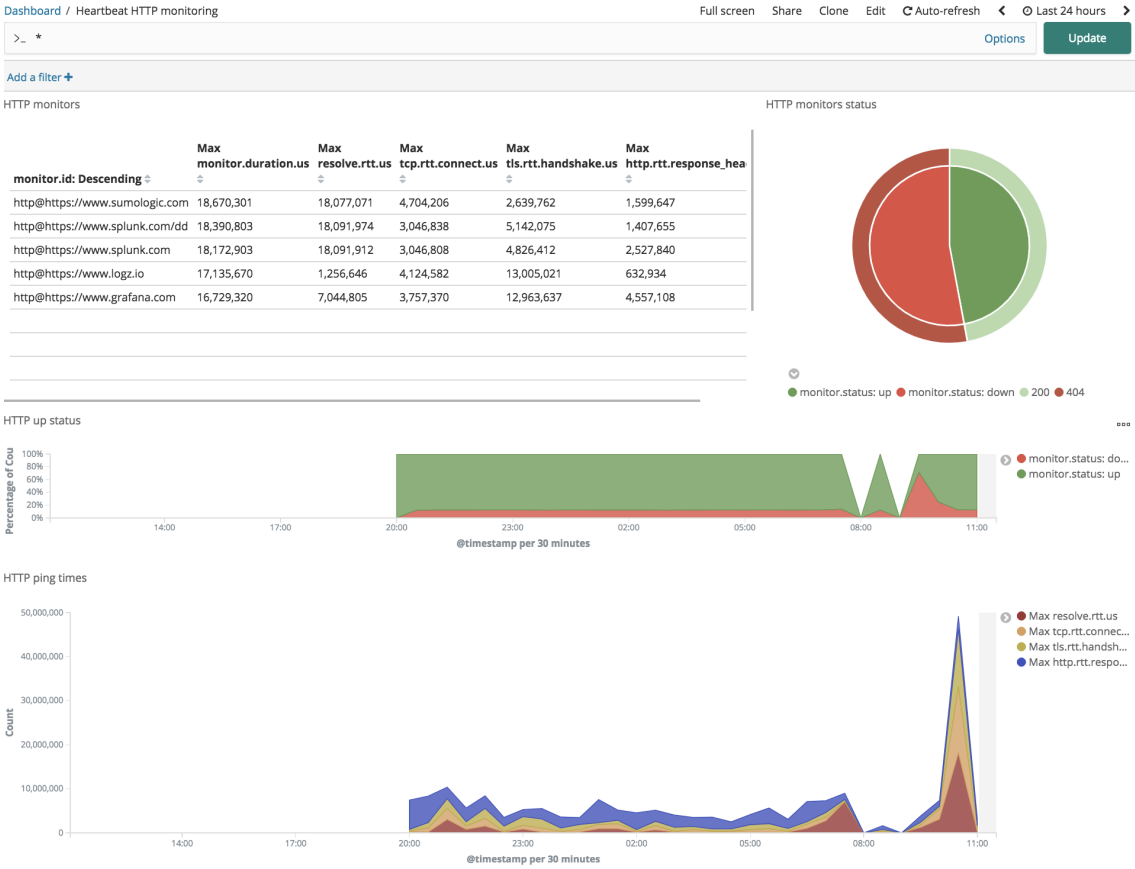
Heartbeat GA

OSS

新しい設定のリロード機能により、Heartbeat モニターを簡単に作成、更新、削除できるように

Docker & Kubernetes の自動検出

KibanaのAdd Dataにチュートリアル



Demo

Data Visualizer for Files

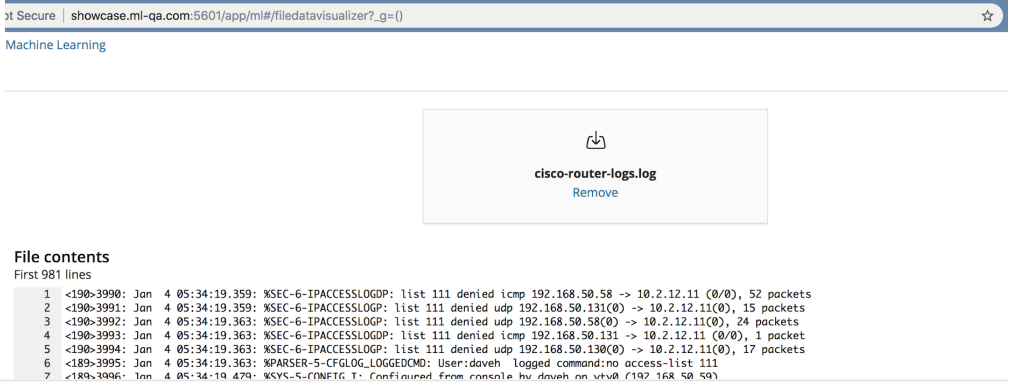
Experimental | Basic (free)

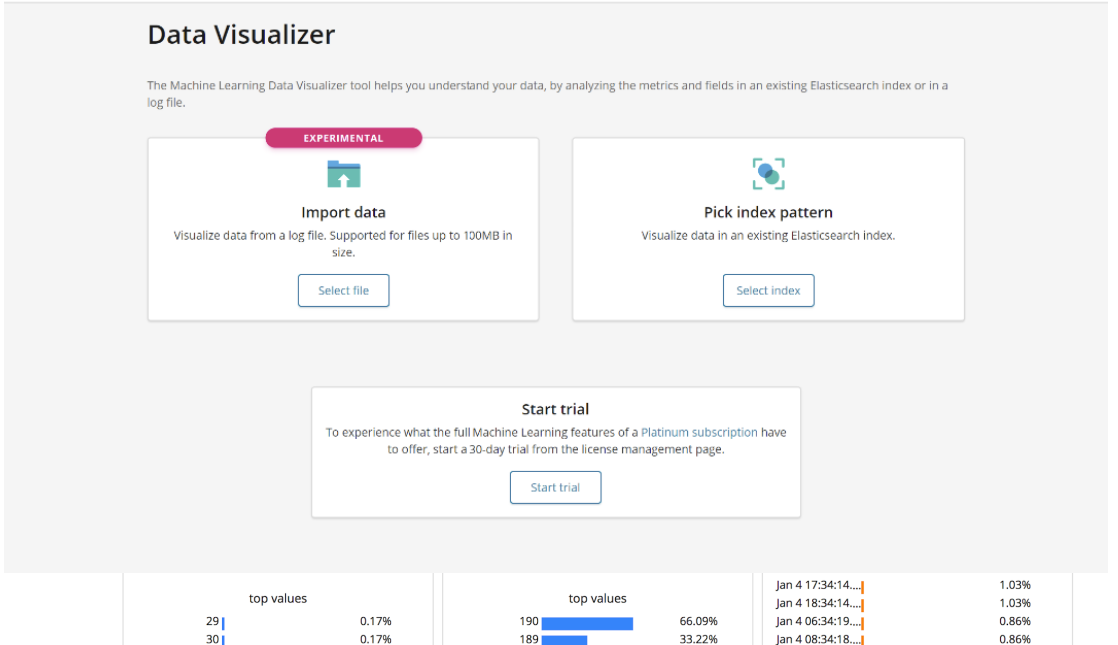
機械学習を最大限に活用するには、データを理解する必要がある

データビジュアライザーで、ファイル (最大 100 mb) をアップロード

フィールドの識別とインデックスパターンの作成に ファイル構造APIを使用できるように

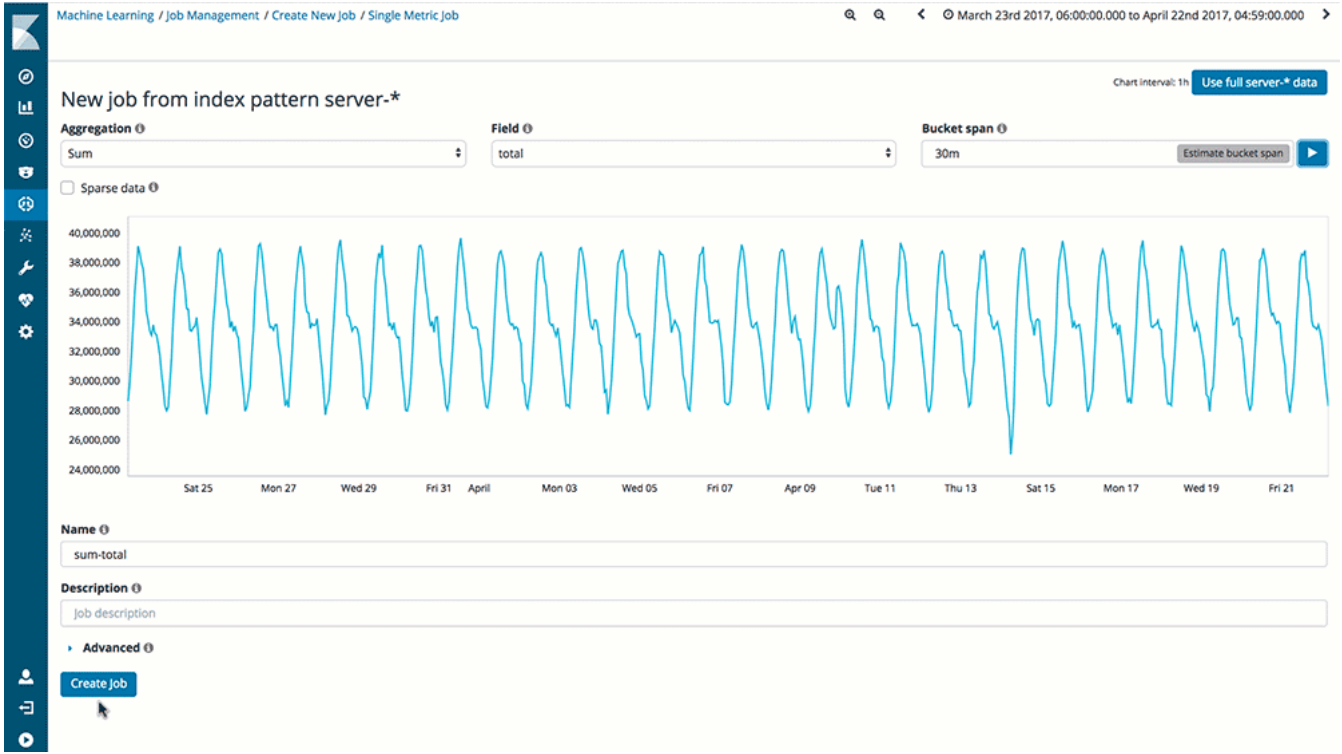
CSV、区切りテキスト、または JSON ファイルに対応





Machine Learning

Machine Learning -
https://www.elastic.co/jp/products/stack/machine-learning



elastic