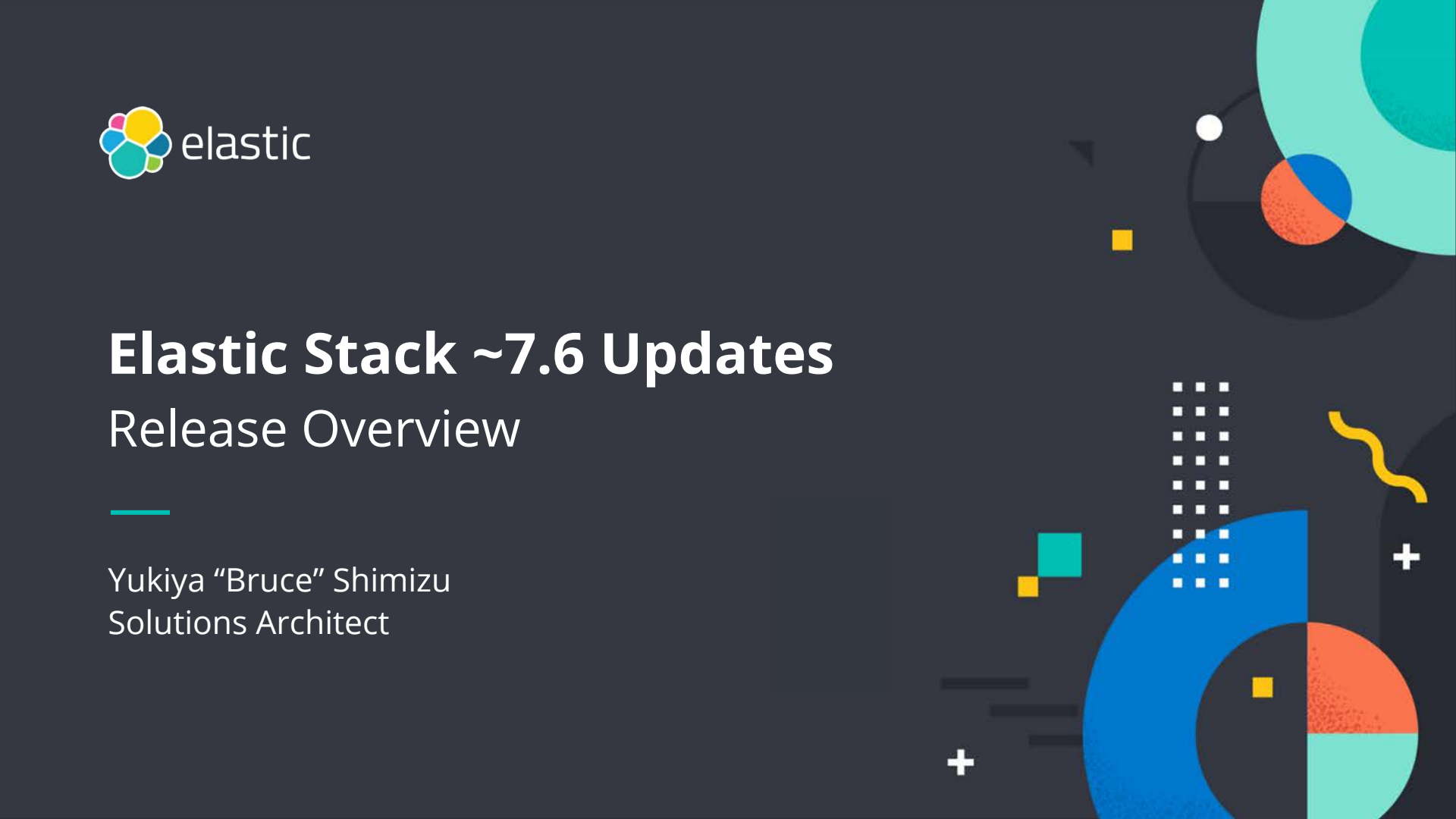
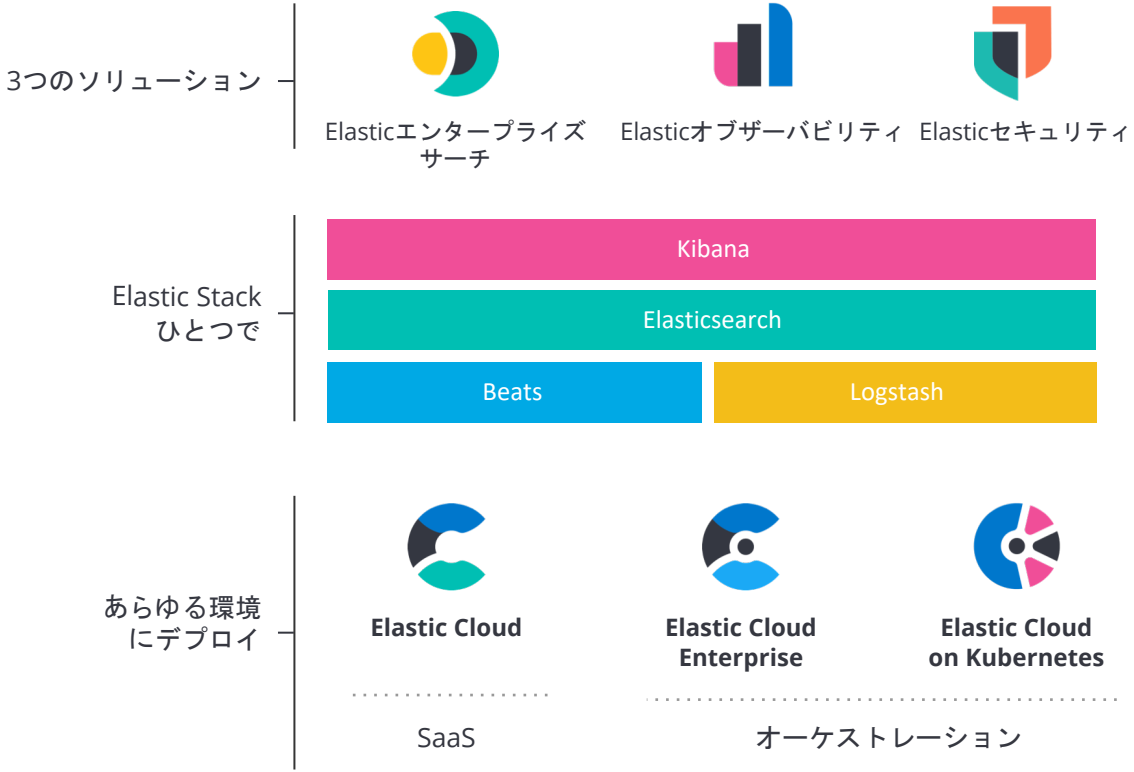


Elastic Stack ~7.6 Updates

Release Overview

Yukiya “Bruce” Shimizu
Solutions Architect

Elastic テクノロジー



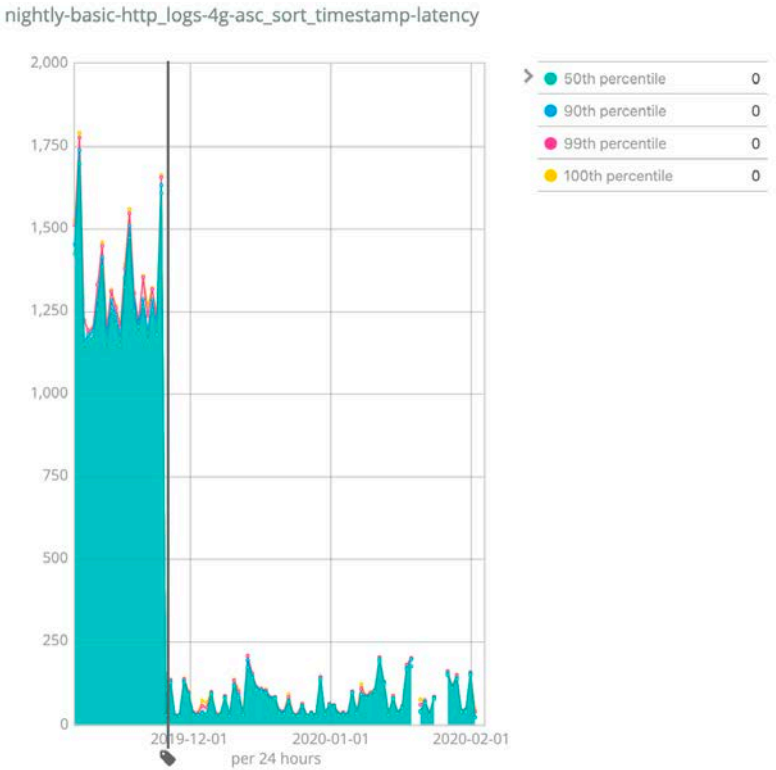
elastic

Elasticsearch

パフォーマンス最適化

DateとNumeric Data Typeのフィールドでソートが35倍高速化

- **Block-Max-WAND (7.0~)**
- 同様のアルゴリズムをDateやNumericフィールドのソートに適用
- 大量のTime Seriesデータのソート処理などに有益



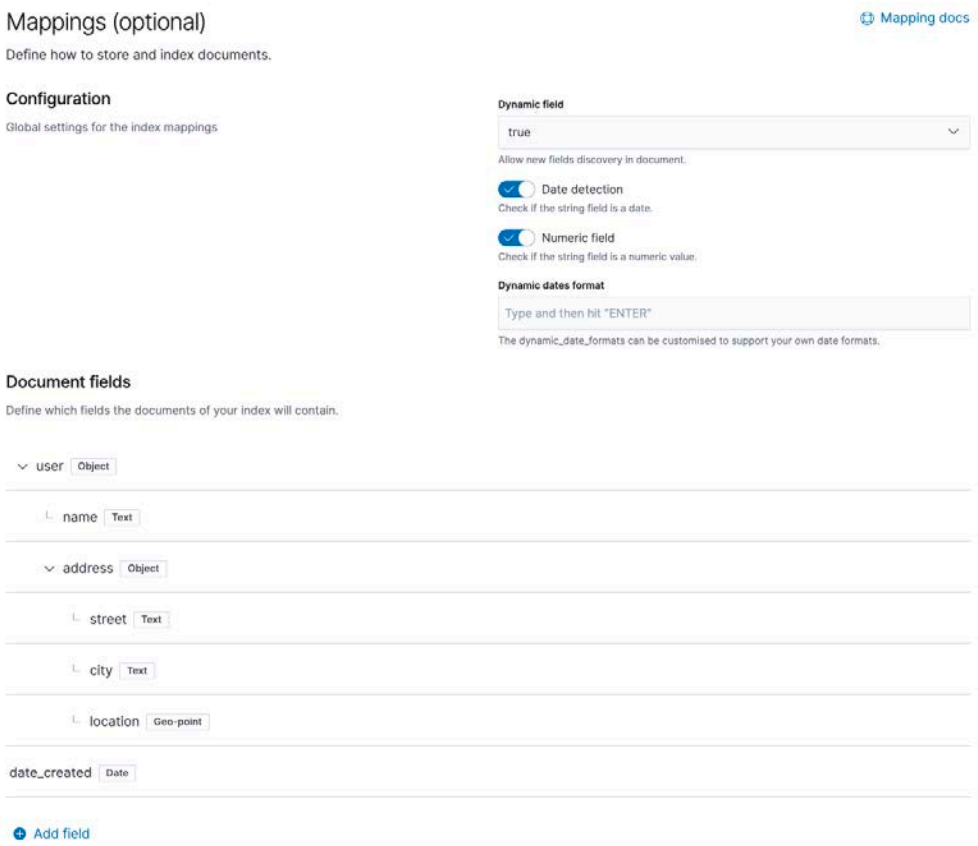
https://www.elastic.co/jp/blog/elasticsearch-7-6-0-released

elastic

新機能

Index template mappings

- Index template mappings 作成をGUIで可能に
- 面倒なJSONでのmappings 作成から解放！



https://www.elastic.co/guide/en/kibana/current/managing-indices.html

新機能

Histogram Datatype

```
PUT my_index
{
  "mappings": {
    "properties": {
      "my_histogram": {
        "type" : "histogram"
      },
      "my_text" : {
        "type" : "keyword"
      }
    }
  }
}
```

```
PUT my_index/_doc/1
{
  "my_text" : "histogram_1",
  "my_histogram" : {
      "values" : [0.1, 0.2, 0.3, 0.4, 0.5], 1
      "counts" : [3, 7, 23, 12, 6] 2
   }
}

PUT my_index/_doc/2
{
  "my_text" : "histogram_2",
  "my_histogram" : {
      "values" : [0.1, 0.25, 0.35, 0.4, 0.45, 0.5], 1
      "counts" : [8, 17, 8, 7, 6, 2] 2
   }
}
```

https://www.elastic.co/guide/en/elasticsearch/reference/7.6/histogram.html

新機能

String Stats Aggregation

```
POST /twitter/_search?size=0
{
  "aggs" : {
    "message_stats" : {
      "string_stats" : {
        "field" : "message.keyword”
      }
    }
  }
}
```

```
{
    ...
    "aggregations": {
          "message_stats" : {
           "count" : 5,
           "min_length" : 24,
           "max_length" : 30,
           "avg_length" : 28.8,
           "entropy" : 3.94617750050791
        }
    }
}
```

- Count
- Minimum length/Maximum length
- Average length
- Shannon entropy

https://www.elastic.co/guide/en/elasticsearch/reference/7.6/search-aggregations-metrics-string-stats-aggregation.html

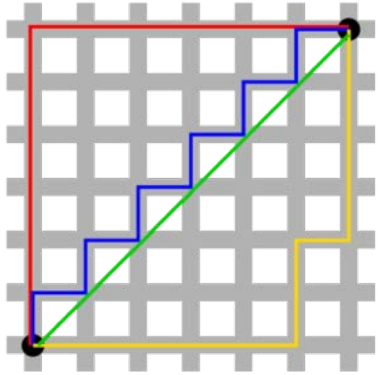
BASIC

GA

New Vector Distance Functions

ベクトルを使った関連度ランキングの拡張

- 文書の類似性をベクトルを使って測定するシナリオは無数にある
- ベクトル化した文書から、文書（イメージやテキスト）を表現する様々なアルゴリズムを使ったベクトル化に至る幅広い応用
- 7.4から二つの類似性を測定するFunctionを導入
  - Manhattan Distance (L1 norm)
  - Euclidean Distance (L2 norm)
- 定義済みのPainless functionとして提供され、Script score queryの一部として他のクエリーに統合可能



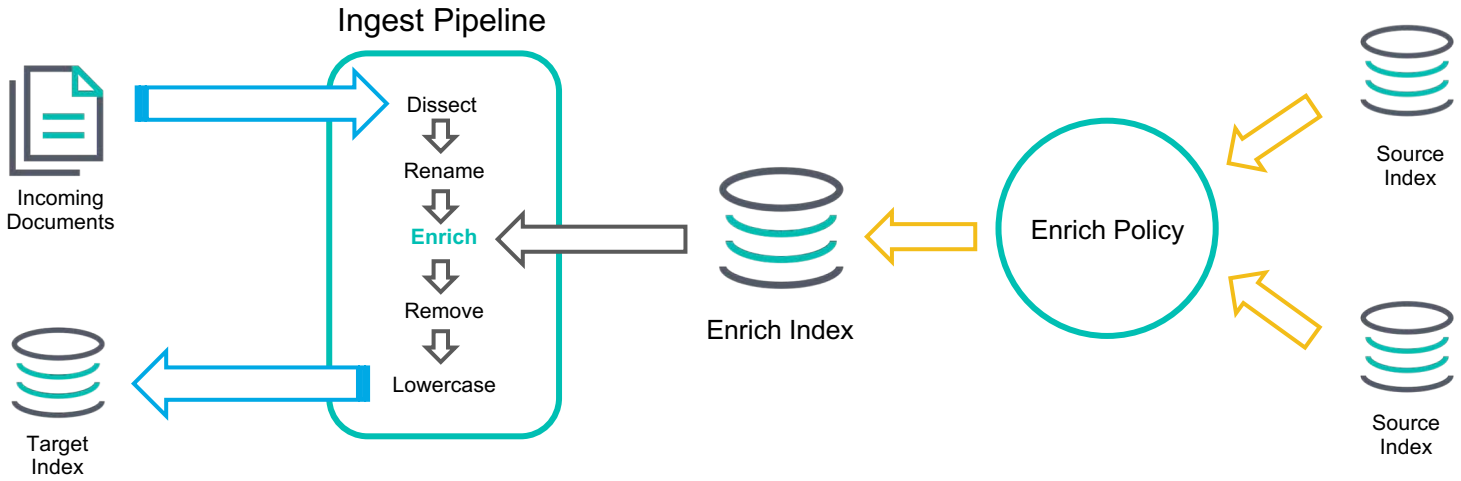
https://www.elastic.co/jp/blog/text-similarity-search-with-vectors-in-elasticsearch

https://www.elastic.co/guide/en/elasticsearch/reference/current/dense-vector.html

elastic

Enrich Processor

データ投入をよりシンプルに



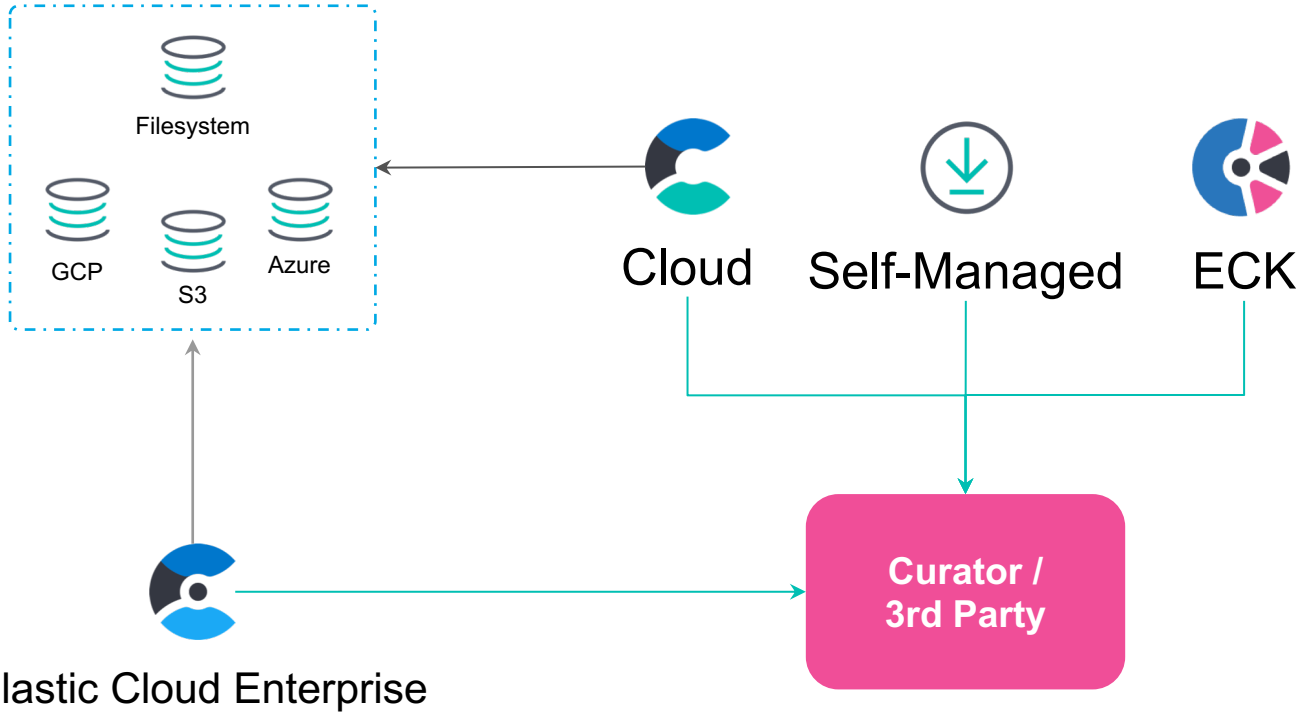
https://www.elastic.co/guide/en/elasticsearch/reference/7.6/ingest-enriching-data.html

elastic

Snapshot **L**ifecycle **M**anagement
SLM

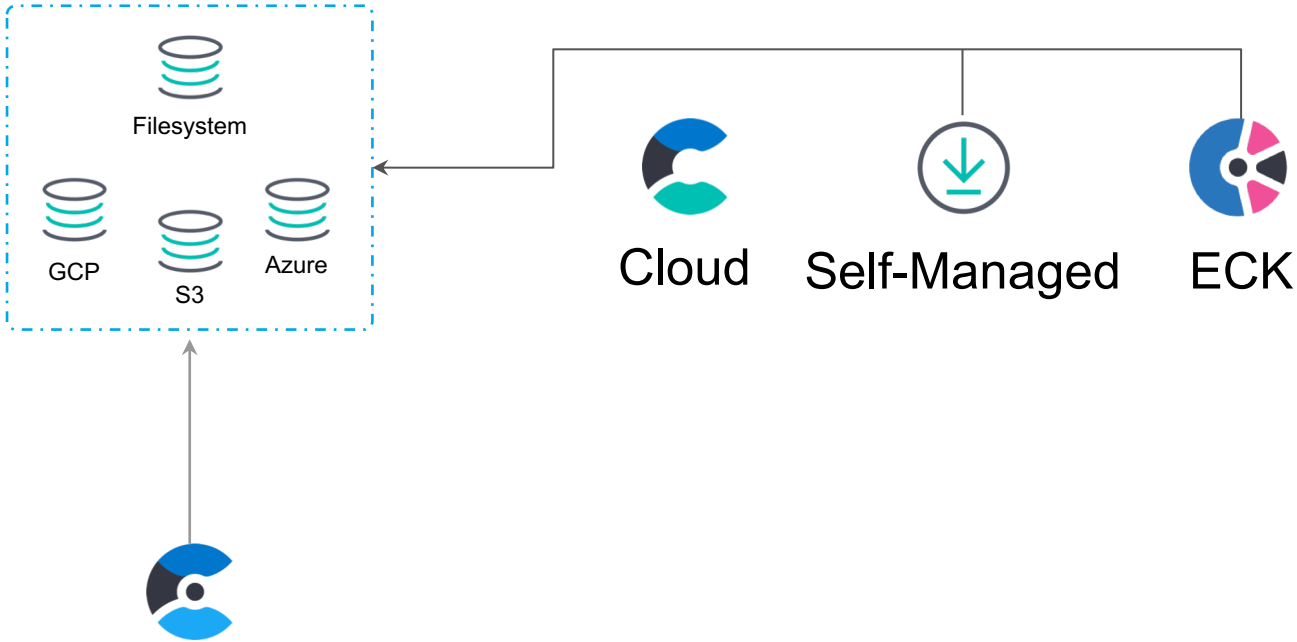
Snapshot Lifecycle Management（これまで）

Snapshotの管理には、Curatorや3rd Partyツールが必要だった…

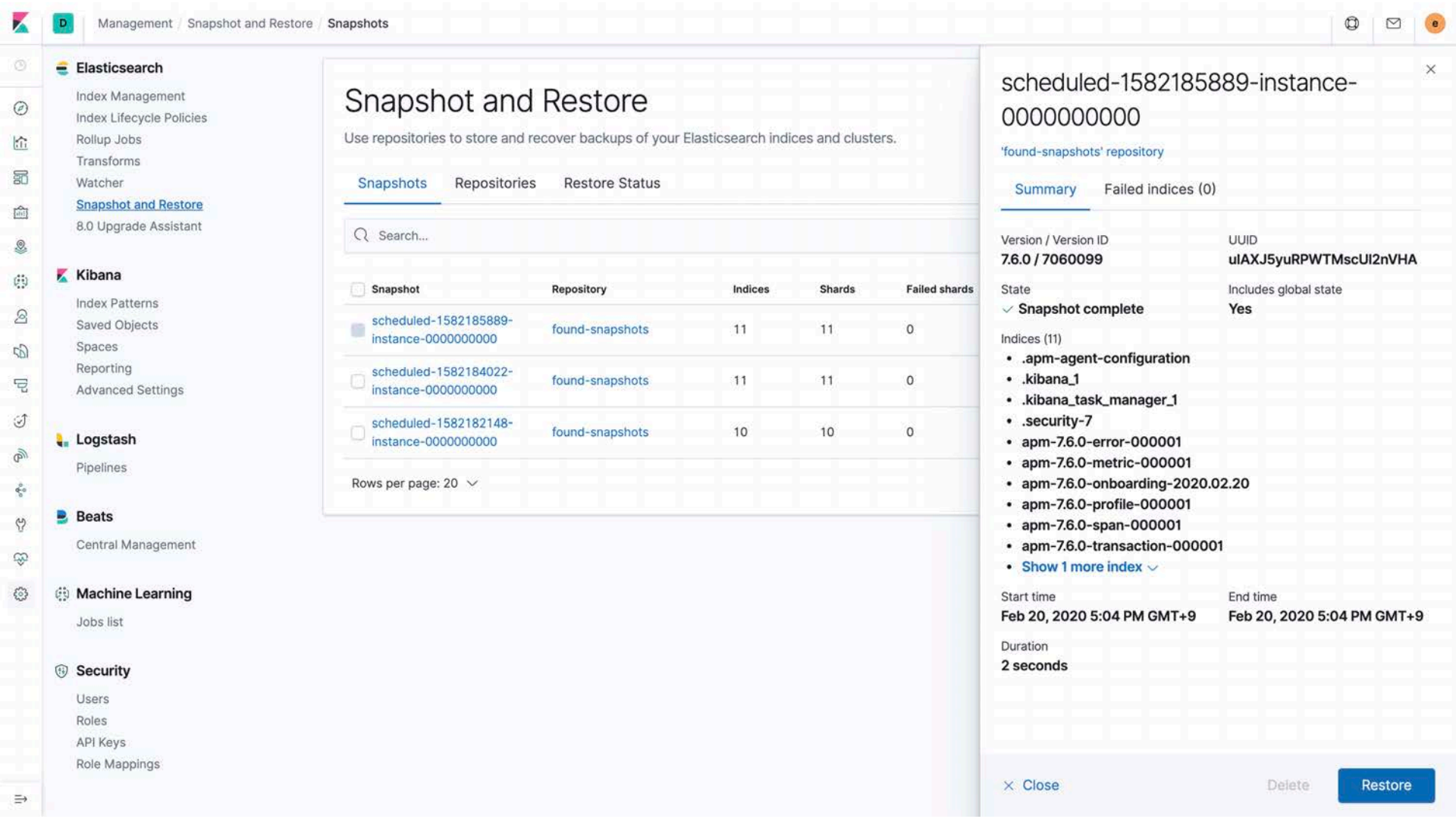


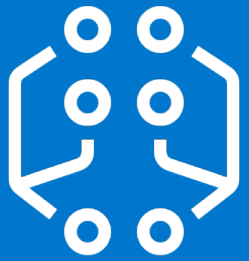
Snapshot Lifecycle Management (これから)

最早、Curatorや3rd Partyツールは必要なし



https://www.elastic.co/guide/en/elasticsearch/reference/7.6/getting-started-snapshot-lifecycle-management.html


Management / Snapshot and Restore / Snapshots
Elasticsearch
Index Management
Index Lifecycle Policies
Rollup Jobs
Transforms
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
Security
Users
Roles
API Keys
Role Mappings
Snapshot and Restore
Use repositories to store and recover backups of your Elasticsearch indices and clusters.
Snapshots
Repositories
Restore Status
Search...
Snapshot
Repository
Indices
Shards
Failed shards
scheduled-1582185889-instance-0000000000
found-snapshots
11
11
0
scheduled-1582184022-instance-0000000000
found-snapshots
11
11
0
scheduled-1582182148-instance-0000000000
found-snapshots
10
10
0
Rows per page: 20
scheduled-1582185889-instance-0000000000
'found-snapshots' repository
Summary
Failed indices (0)
Version / Version ID
7.6.0 / 7060099
UUID
ulAXJ5yuRPWTMscUl2nVHA
State
Snapshot complete
Includes global state
Yes
Indices (11)
.apm-agent-configuration
.kibana_1
.kibana_task_manager_1
.security-7
apm-7.6.0-error-000001
apm-7.6.0-metric-000001
apm-7.6.0-onboarding-2020.02.20
apm-7.6.0-profile-000001
apm-7.6.0-span-000001
apm-7.6.0-transaction-000001
Show 1 more index
Start time
Feb 20, 2020 5:04 PM GMT+9
End time
Feb 20, 2020 5:04 PM GMT+9
Duration
2 seconds
Close
Delete
Restore



Machine Learning

Elastic Transforms

目標

データを新しい形式に “transform” することを可能に

- 元々のデータを変更せずに違うデータ形式を提供し、機械学習に活用する
- Transformのステップ
  - Pivot
  - Aggregation

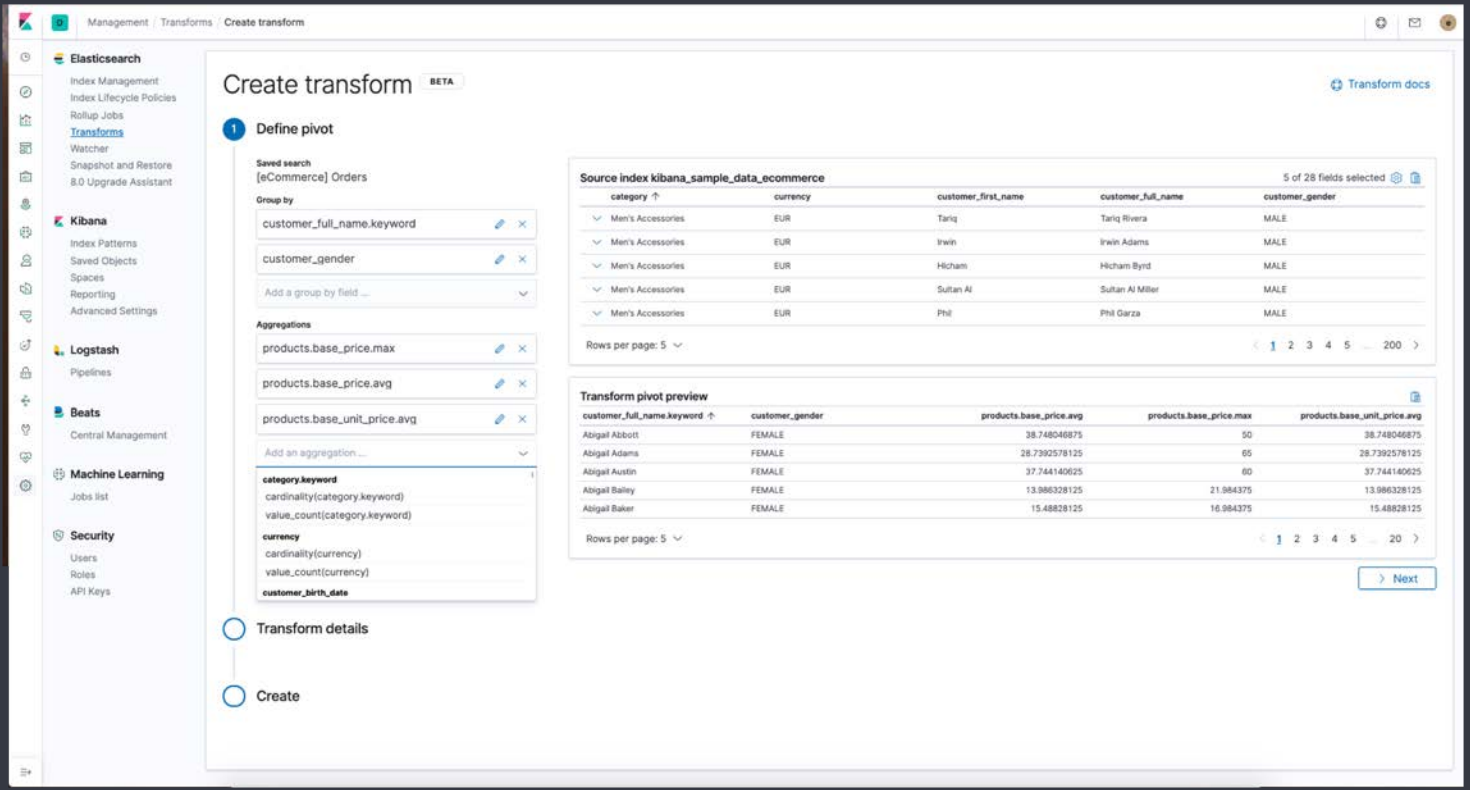
多次元の分析を可能に

- Outlier detection(はずれ値検知)
- Regression(回帰) と Classification(分類)
- 教師あり学習のモデル構築

https://www.elastic.co/guide/en/elasticsearch/reference/current/transform-overview.html

BASIC

Elastic Transforms

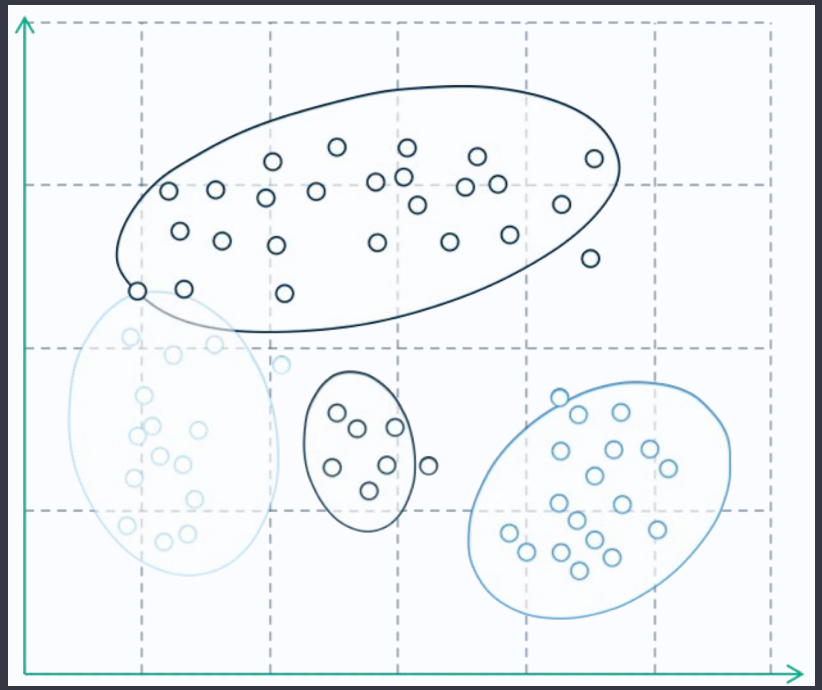


https://www.elastic.co/guide/en/elasticsearch/reference/current/ecommerce-transforms.html

elastic

PLATINUM

Outlier Detection



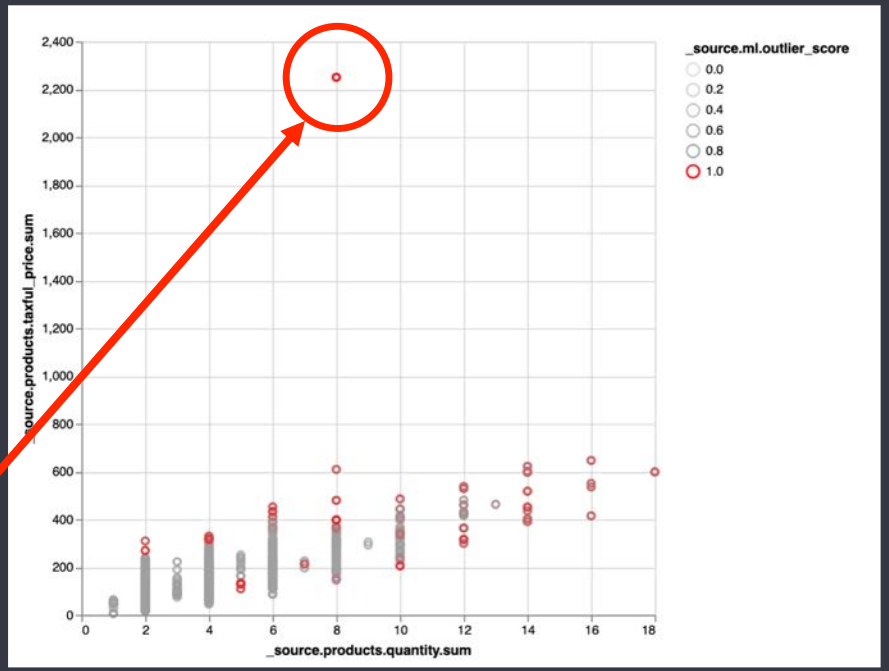
elastic

PLATINUM

Elastic Data Frame Analytics

Outlier Detectionの活用

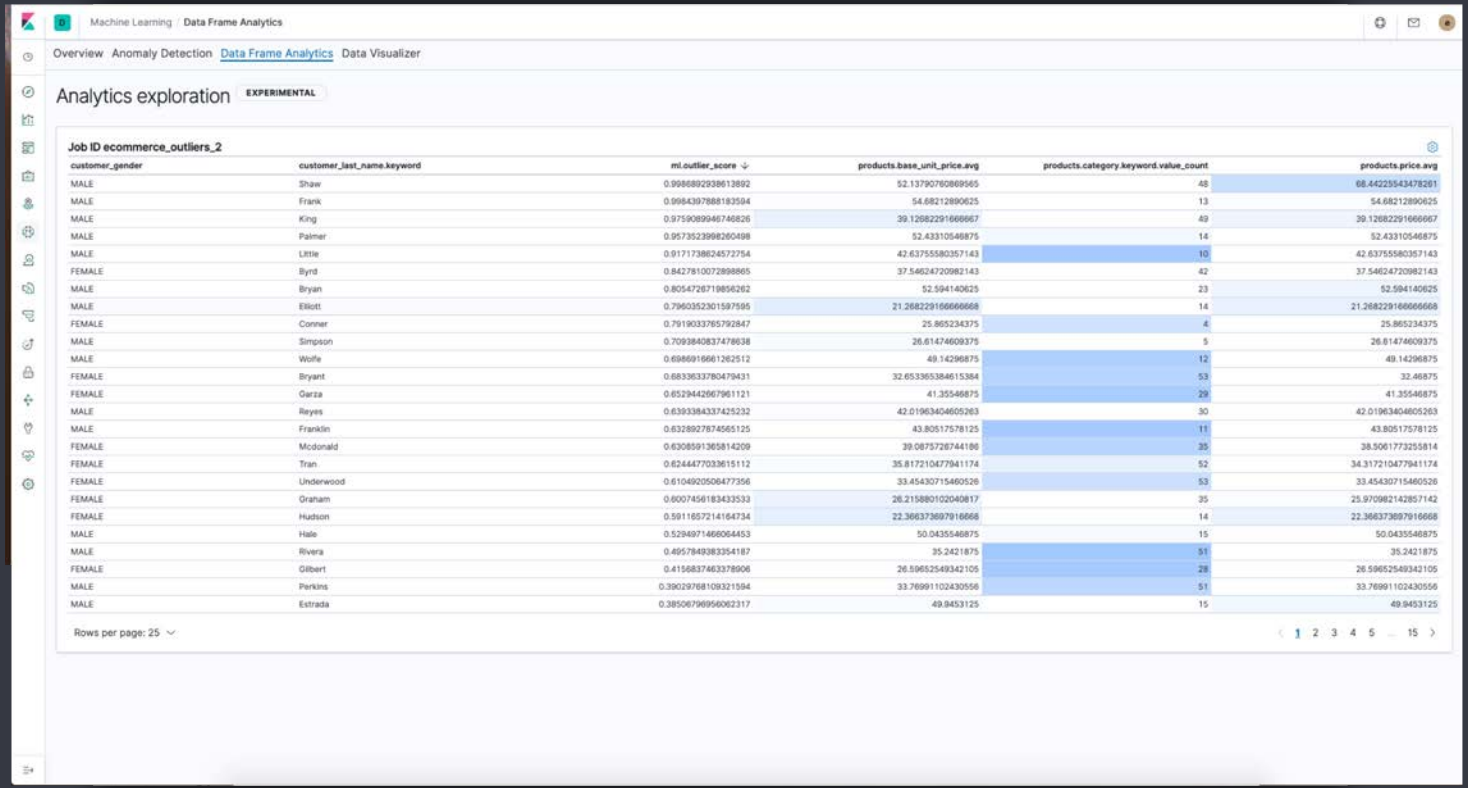

```
"customer_full_name" : {
  "keyword" : "Wagdi Shaw"
},
"ml__id_copy" : "Vyu9e08pKNasT-9TLV9p3k0AAAAAAAAA",
"products" : {
  "taxful_price" : {
    "sum" : 2250.0
  },
  "quantity" : {
    "sum" : 8.0
  }
},
"ml" : {
  "outlier_score" : 0.9848338961601257,
  "feature_influence.products.quantity.sum" : 0.007586637046188116,
  "feature_influence.products.taxful_price.sum" : 0.992413341999054
}
```

elastic

PLATINUM

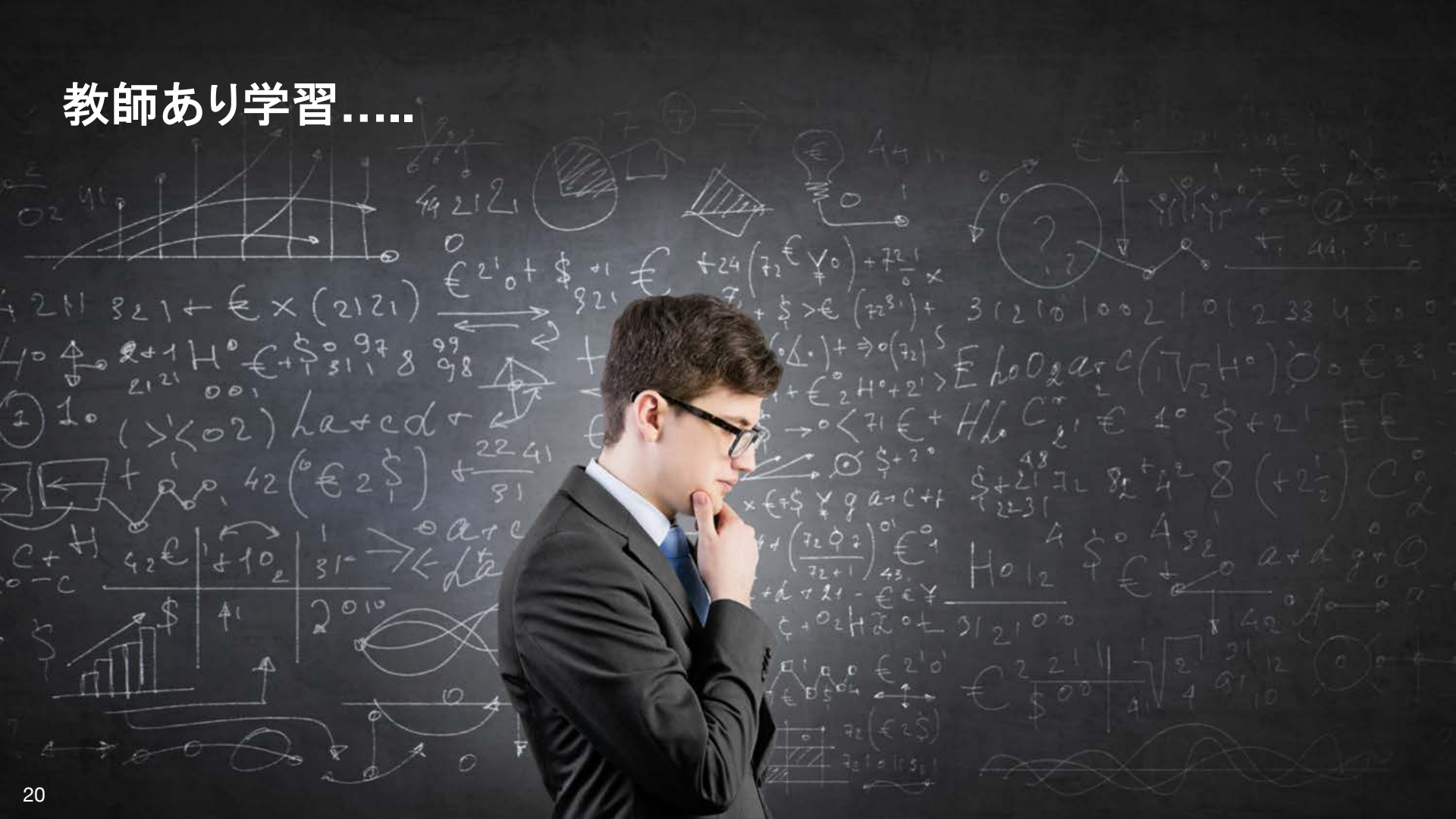
Elastic Data Frame Analytics



https://www.elastic.co/guide/en/machine-learning/current/ecommerce-outliers.html

elastic

教師あり学習.....

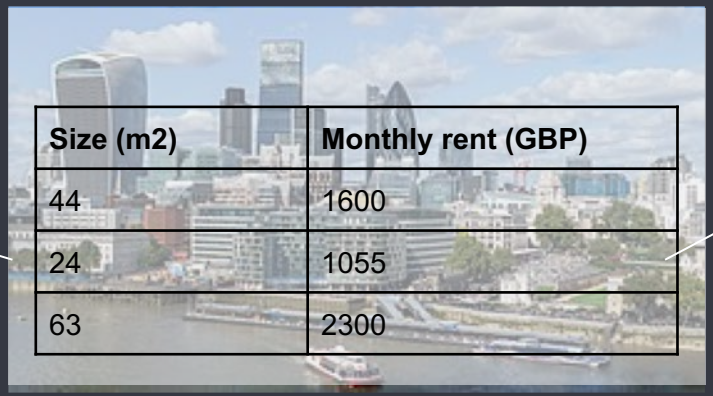


PLATINUM

Regression（回帰）

回帰とは、複数の変数、又は**特徴量**から**連続値**を予測する方法の一つ

例えば、ロンドン市内のアパートの広さと家賃の関係を知りたい場合



Size (m2)	Monthly rent (GBP)
44	1600
24	1055
63	2300

特徴量

連続値

elastic

PLATINUM

Classification（分類）

分類とは、所与のデータのクラス、又は種類を予測するプロセス

cancerous

benign

country

hip-hop

avant garde

default

safe

elastic

PLATINUM

教師あり学習
Regression

ラベル付されたデータ

モデルを学習

dependent variable = how much?

analyzed fields: 分析に使うフィールド

テストデータを使ってモデルを評価

```
PUT _ml/data_frame/analytics/model-flight-delays
{
  "source": {
    "index": [
      "kibana_sample_data_flights" 1
    ],
    "query": { 2
      "range": {
        "DistanceKilometers": {

    ...
    "DestRegion" : "UK",
    "OriginAirportID" : "LHR",
    "DestCityName" : "London",
    "FlightDelayMin" : 66,        1
    "ml" : {
      "FlightDelayMin_prediction" : 62.527,    2
      "is_training" : false    3
    }
    ...

    "excludes": [    6
      "Cancelled",
      "FlightDelay",
      "FlightDelayType"
    ]
  },
  "model_memory_limit": "100mb" 7
}
```

https://www.elastic.co/guide/en/machine-learning/current/flightdata-regression.html

elastic

PLATINUM

教師あり学習
Classification

ラベル付されたデータ

モデルを学習

dependent variable = true/false

analyzed fields: 分析に使うフィールド

テストデータを使ってモデルを評価

```
PUT _ml/data_frame/analytics/model-flight-delay-classification
{
  "source": {
                ...
                "FlightDelay" : false, 1
  },            ...
  "d            "ml" : {
                  "top_classes" : [ 2
                    {
  },                  "class_probability" : 0.939335365058496,
  "a                  "class_name" : "false"
                    },
                    {
                      "class_probability" : 0.06066463494150393,
  },                  "class_name" : "true"
  "a                }
                  ],
                  "FlightDelay_prediction" : "false", 3
                  "is_training" : false 4
                }

  },
  "model_memory_limit": "100mb" 7
}
```

https://www.elastic.co/guide/en/machine-learning/current/flightdata-classification.html

elastic

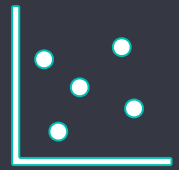
PLATINUM

モデルの評価
Regression example

```
{
  "regression" : {
    "mean_squared_error" : {
      "error" : 3759.7242253334207
    },
    "r_squared" : {
      "value" : 0.5853159777330623
    }
  }
}
```

Mean Squared Error:
低い方が良い

R Squared (0-1):
高い方が良い



https://www.elastic.co/guide/en/machine-learning/current/ml-dfanalytics-evaluate.html#ml-dfanalytics-classification

elastic

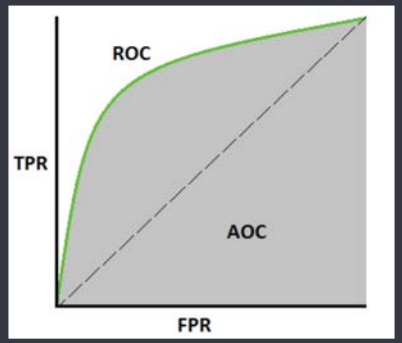
PLATINUM

モデルの評価
Classification example

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Confusion Matrix:

True/False
Positives/Negatives

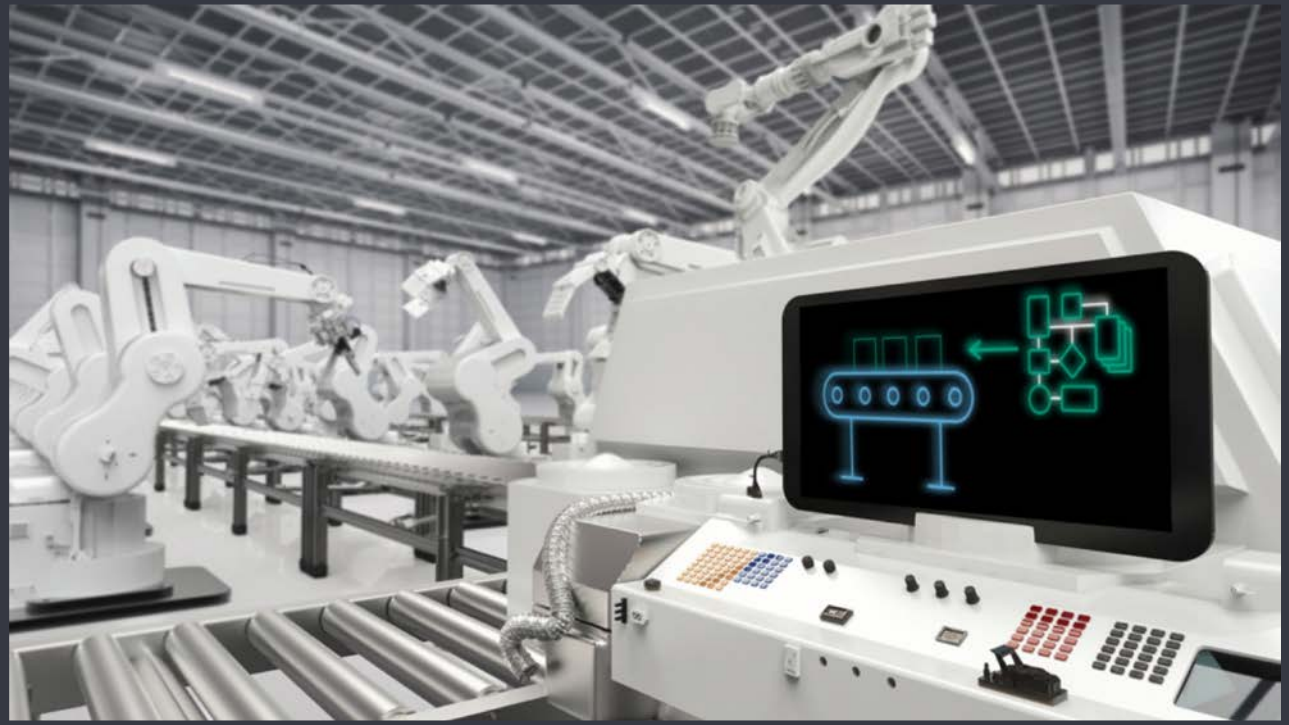



```
{
  "classification" : {
    "multiclass_confusion_matrix" : {
      "confusion_matrix" : [
        {
          "actual_class" : "false", 1
          "actual_class_doc_count" : 8778, 2
          "predicted_classes" : [
            {
              "predicted_class" : "false", 3
              "count" : 7509 4
            },
            {
              "predicted_class" : "true",
              "count" : 1269
            }
          ],
          "other_predicted_class_doc_count" : 0
        },
        {
          "actual_class" : "true",
          "actual_class_doc_count" : 2939,
          "predicted_classes" : [
            {
              "predicted_class" : "false",
              "count" : 1213
            },
            {
              "predicted_class" : "true",
              "count" : 1726
            }
          ],
          "other_predicted_class_doc_count" : 0
        }
      ],
      "other_actual_class_count" : 0
    }
  }
}
```


https://www.elastic.co/guide/en/machine-learning/current/ml-dfanalytics-evaluate.html#ml-dfanalytics-classification

elastic

さらに ....



運用可能に！

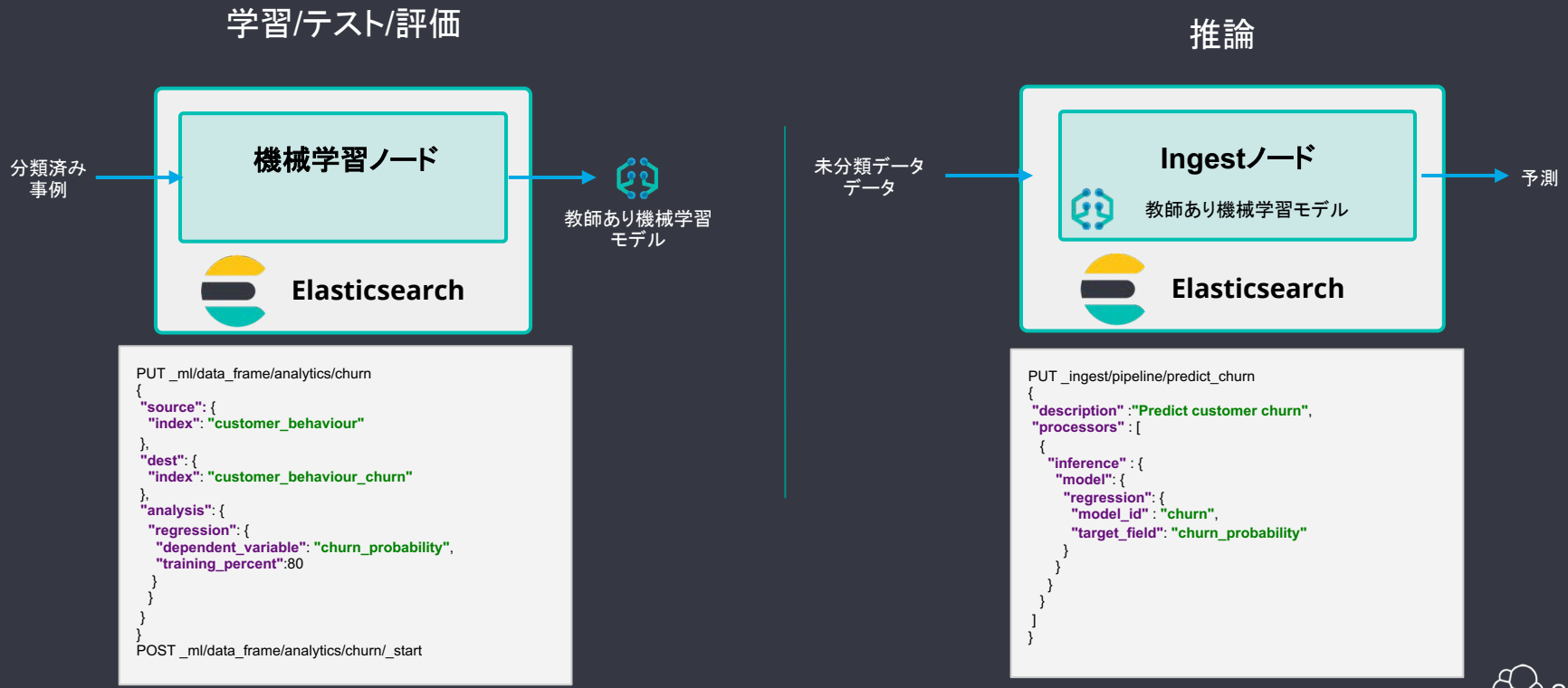
…推論

elastic

PLATINUM

モデルの学習と推論

教師あり学習



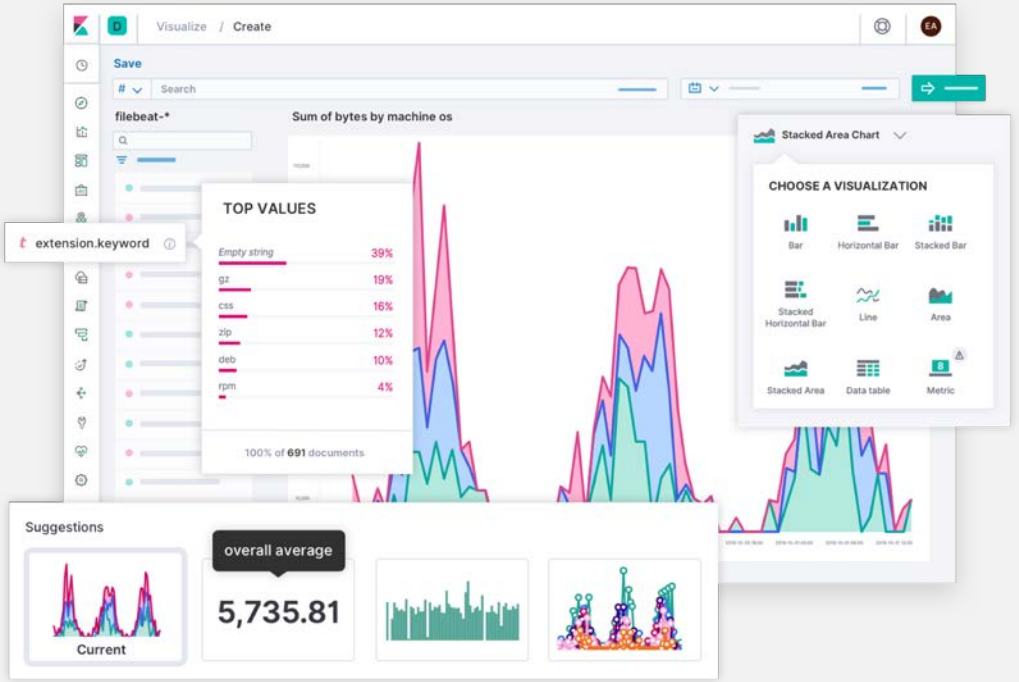
https://www.elastic.co/guide/en/machine-learning/current/ml-inference.html

elastic

Kibana

Kibana Lens

Kibanaでデータを可視化する簡単で直感的な新しい方法



データは目の前に
フィールドをクリックして探索を開始

ドラッグ＆ドロップ
マウス一つの操作から目的地がわからない場合も、気軽に探索を

スマートなサジェスチョン
便利なチャートをサジェストして、Lensが分析を支援

https://www.elastic.co/guide/en/kibana/current/lens.html

elastic

Kibanaのイノベーションにおけるガイドライン

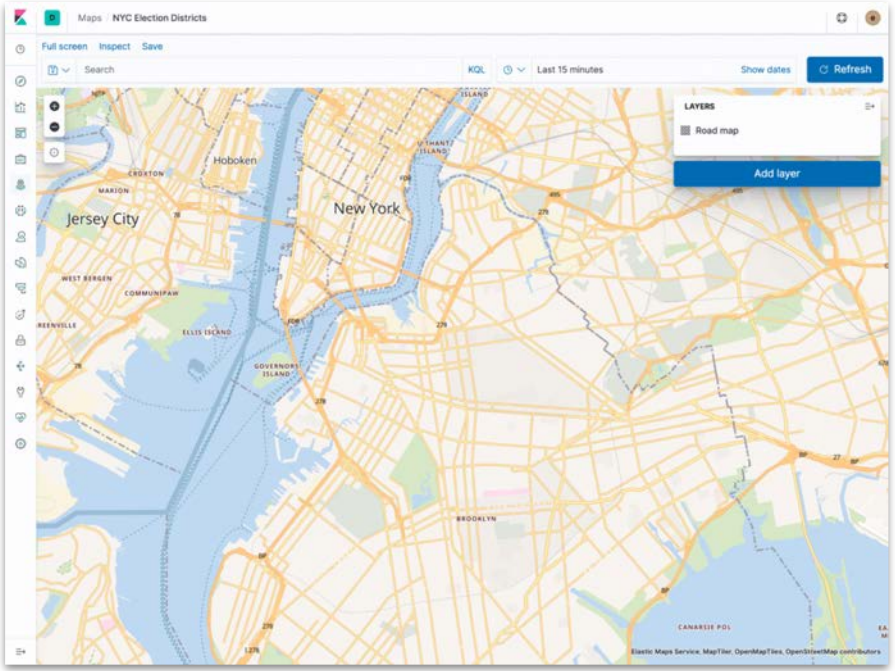
1. 過去のKibanaの経験がないユーザーをエンパワー
2. 簡単にデータフィールドの気付きや理解を促進
3. アドホックなシナリオに柔軟性をサポート
4. スピードやスケール、Elasticsearchのフィーチャーを活用
5. 簡単に使えて、しかもパワフルなインパクト

Elastic Maps

GeoJSONアップロードがGAに

カスタムシェイプをMapsに追加する最速の方法

- 7.3からBeta提供され、現在GAとなり安定性も向上
- 営業テリトリーやオフィスの分散など、顧客固有のデータに最適
- 生のデータにフィルターやアグリゲーションといった分析を可能に



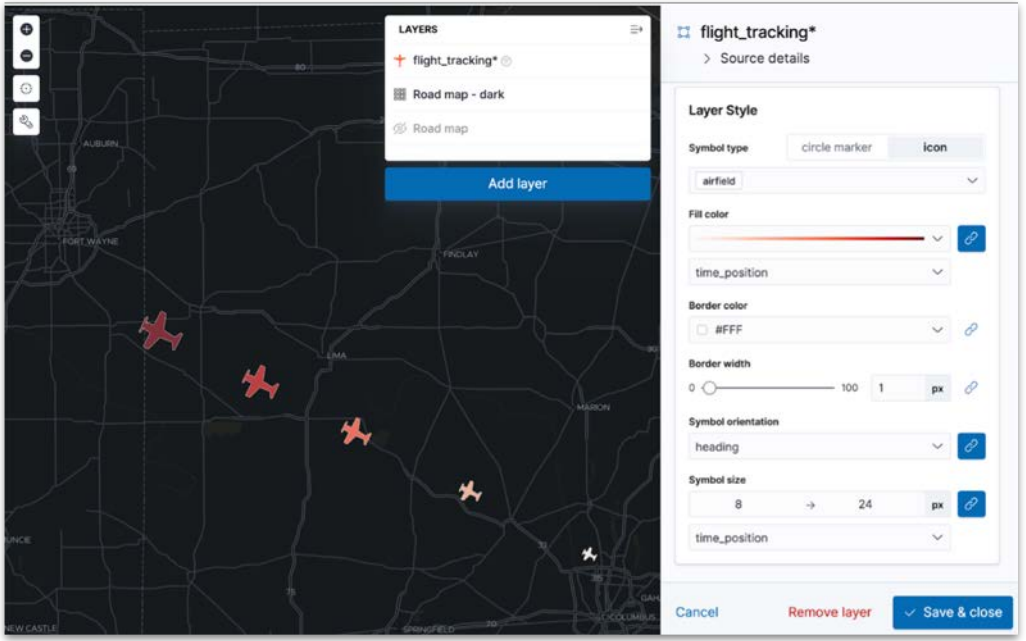
https://www.elastic.co/guide/en/kibana/current/geojson-upload.html

elastic

時系列データにスタイルを追加

日付/タイムフィールドと色やサイズを関連付ける

- アセットトラッキングやその他時系列データに最適
- 直近の車の位置、荷物の位置、人の位置などのトラッキング
- 従来は数値フィールドにのみ対応



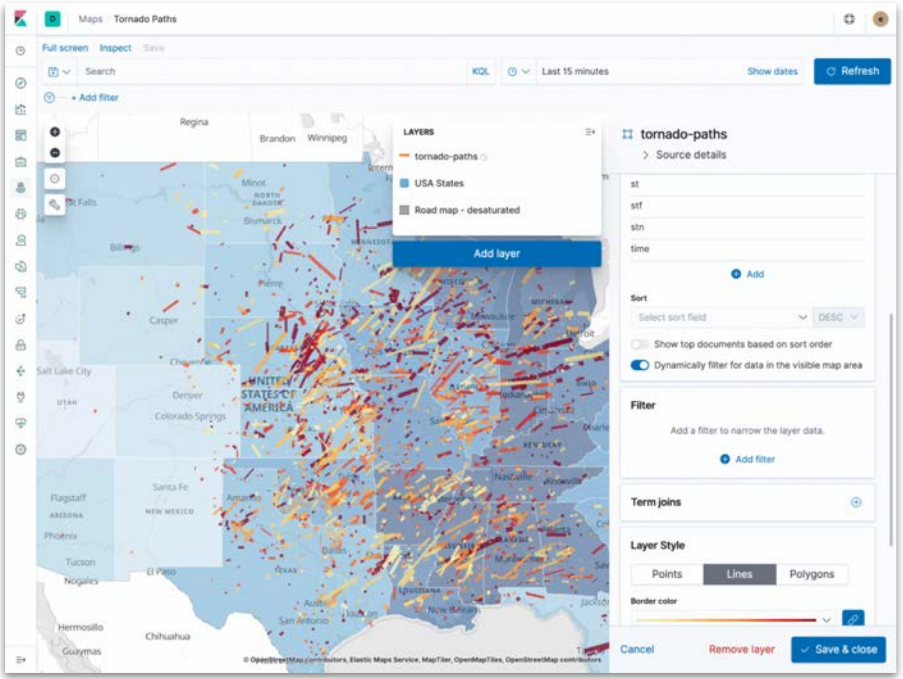
https://www.elastic.co/blog/elastic-maps-7-5-0-released

elastic

レイヤーにおけるドキュメントのソート

最も大切なデータをトップに

- 数値もしくは日付フィールドで
  ソートした結果を、表示順に反映
- データの表現にさらなる一貫性
- 10kドキュメントが上限



https://www.elastic.co/blog/elastic-maps-7-5-0-released

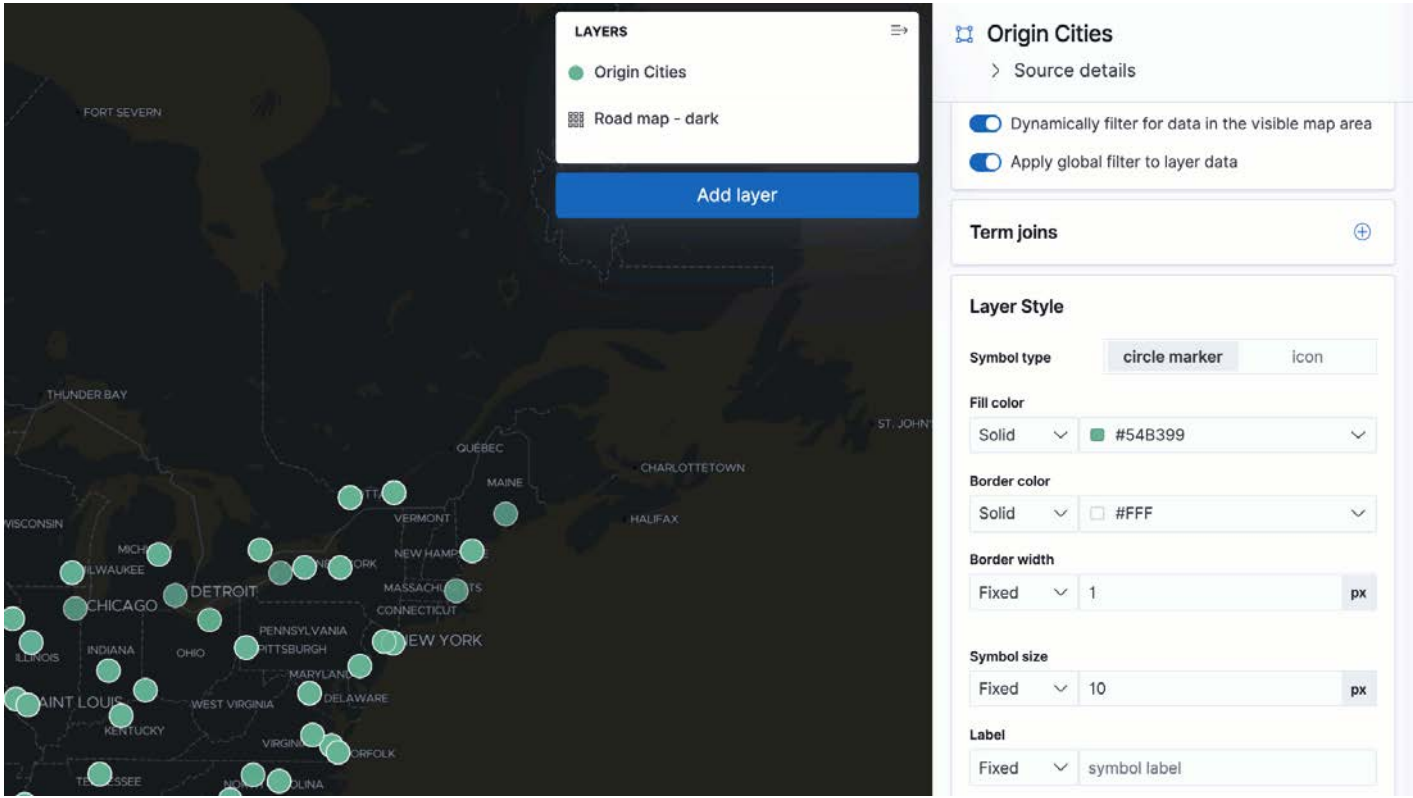
elastic

https://www.elastic.co/blog/keeping-up-with-kibana-2020-01-20

BASIC

Categorical Styling

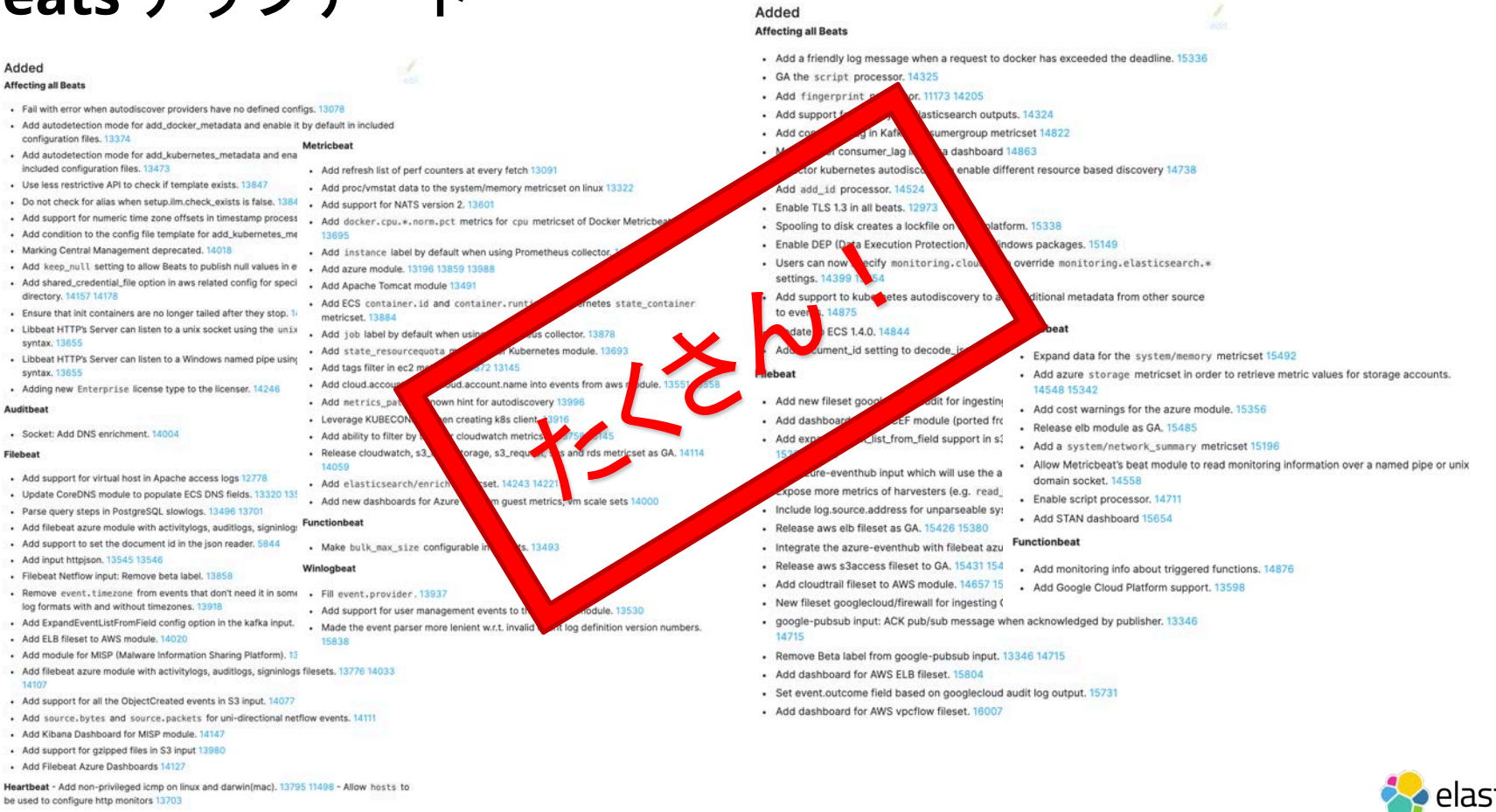
分類フィールドの値によって、データポイントを色付け



elastic

Beats

Beats アップデート



Added

Affecting all Beats

- Fail with error when autodiscover providers have no defined configs. 13078
- Add autodetection mode for add_docker_metadata and enable it by default in included configuration files. 13374
- Add autodetection mode for add_kubernetes_metadata and ena included configuration files. 13473
- Use less restrictive API to check if template exists. 13847
- Do not check for alias when setup.ilm.check_exists is false. 1384
- Add support for numeric time zone offsets in timestamp process
- Add condition to the config file template for add_kubernetes_me
- Marking Central Management deprecated. 14018
- Add `keep_null` setting to allow Beats to publish null values in e
- Add shared_credential_file option in aws related config for speci directory. 14157 14178
- Ensure that init containers are no longer tailed after they stop. 1
- Libbeat HTTP's Server can listen to a unix socket using the `unix` syntax. 13655
- Libbeat HTTP's Server can listen to a Windows named pipe usin syntax. 13655
- Adding new `Enterprise` license type to the licenser. 14246

Auditbeat

- Socket: Add DNS enrichment. 14004

Filebeat

- Add support for virtual host in Apache access logs 12778
- Update CoreDNS module to populate ECS DNS fields. 13320 13
- Parse query steps in PostgreSQL slowlogs. 13496 13701
- Add filebeat azure module with activitylogs, auditlogs, signinlog
- Add support to set the document id in the json reader. 5844
- Add input httpjson. 13545 13546
- Filebeat Netflow input: Remove beta label. 13858
- Remove `event.timezone` from events that don't need it in som log formats with and without timezones. 13918
- Add ExpandEventListFromField config option in the kafka input.
- Add ELB fileset to AWS module. 14020
- Add module for MISP (Malware Information Sharing Platform). 13
- Add filebeat azure module with activitylogs, auditlogs, signinlogs filesets. 13776 14033 14107
- Add support for all the ObjectCreated events in S3 input. 14077
- Add `source.bytes` and `source.packets` for uni-directional netflow events. 14111
- Add Kibana Dashboard for MISP module. 14147
- Add support for gzipped files in S3 input 13980
- Add Filebeat Azure Dashboards 14127

Metricbeat

- Add refresh list of perf counters at every fetch 13091
- Add proc/vmstat data to the system/memory metricset on linux 13322
- Add support for NATS version 2. 13601
- Add `docker.cpu.*.norm.pct` metrics for `cpu` metricset of Docker Metricbea 13695
- Add `instance` label by default when using Prometheus collector
- Add azure module. 13196 13859 13988
- Add Apache Tomcat module 13491
- Add ECS `container.id` and `container.runti` `rnetes state_container` metricset. 13884
- Add `job` label by default when usin `us collector. 13878
- Add `state_resourcequota` m Kubernetes module. 13693
- Add tags filter in ec2 m 972 13145
- Add cloud.accoun `oud.account.name` into events from aws `dule. 13551 `058`
- Add `metrics_pa` `nown hint for autodiscovery 13996
- Leverage KUBECON `en creating k8s client. `3916`
- Add ability to filter by `cloudwatch metrics `7758 `145`
- Release cloudwatch, s3_ `torage, s3_requ `s and rds metricset as GA. 14114 14059
- Add `elasticsearch/enrich` `set. 14243 14221
- Add new dashboards for Azure `m guest metrics, vm scale sets 14000

Functionbeat

- Make `bulk_max_size` configurable in `ts. 13493

Winlogbeat

- Fill `event.provider`. 13937
- Add support for user management events to t `module. 13530
- Made the event parser more lenient w.r.t. invalid `t log definition version numbers. 15838

Heartbeat - Add non-privileged icmp on linux and darwin(mac). 13795 11498 - Allow `hosts` to be used to configure http monitors 13703

Added

Affecting all Beats

- Add a friendly log message when a request to docker has exceeded the deadline. 15336
- GA the `script` processor. 14325
- Add `fingerprint` `or. 11173 14205
- Add support `lasticsearch outputs. 14324
- Add co `g in Kaf `sumergroup metricset 14822
- M `consumer_lag `a dashboard 14863
- `ctor kubernetes autodisc `enable different resource based discovery 14738
- Add `add_id` processor. 14524
- Enable TLS 1.3 in all beats. 12973
- Spooling to disk creates a lockfile on `latform. 15338
- Enable DEP (D `ata Execution Protection) `indows packages. 15149
- Users can now `ecify `monitoring.clou `override `monitoring.elasticsearch.*` settings. 14399 `54`
- Add support to kub `etes autodiscovery to a `ditional metadata from other source to ev `s. 14875
- `date `o ECS 1.4.0. 14844
- Ad `cument_id setting to decode_j

Filebeat

- Add new fileset goog `dit for ingestin
- Add dashboard `EF module (ported fr
- Add exp `_list_from_field support in s3 15
- `ure-eventhub input which will use the a
- Expose more metrics of harvesters (e.g. `read_`
- Include log.source.address for unparseable sy
- Release aws elb fileset as GA. 15426 15380
- Integrate the azure-eventhub with filebeat azu
- Release aws s3access fileset to GA. 15431 154
- Add cloudtrail fileset to AWS module. 14657 15
- New fileset googlecloud/firewall for ingesting
- google-pubsub input: ACK pub/sub message when acknowledged by publisher. 13346 14715
- Remove Beta label from google-pubsub input. 13346 14715
- Add dashboard for AWS ELB fileset. 15804
- Set event.outcome field based on googlecloud audit log output. 15731
- Add dashboard for AWS vpcflow fileset. 16007

`beat

- Expand data for the `system/memory` metricset 15492
- Add azure `storage` metricset in order to retrieve metric values for storage accounts. 14548 15342
- Add cost warnings for the azure module. 15356
- Release elb module as GA. 15485
- Add a `system/network_summary` metricset 15196
- Allow Metricbeat's beat module to read monitoring information over a named pipe or unix domain socket. 14558
- Enable script processor. 14711
- Add STAN dashboard 15654

Functionbeat

- Add monitoring info about triggered functions. 14876
- Add Google Cloud Platform support. 13598

elastic

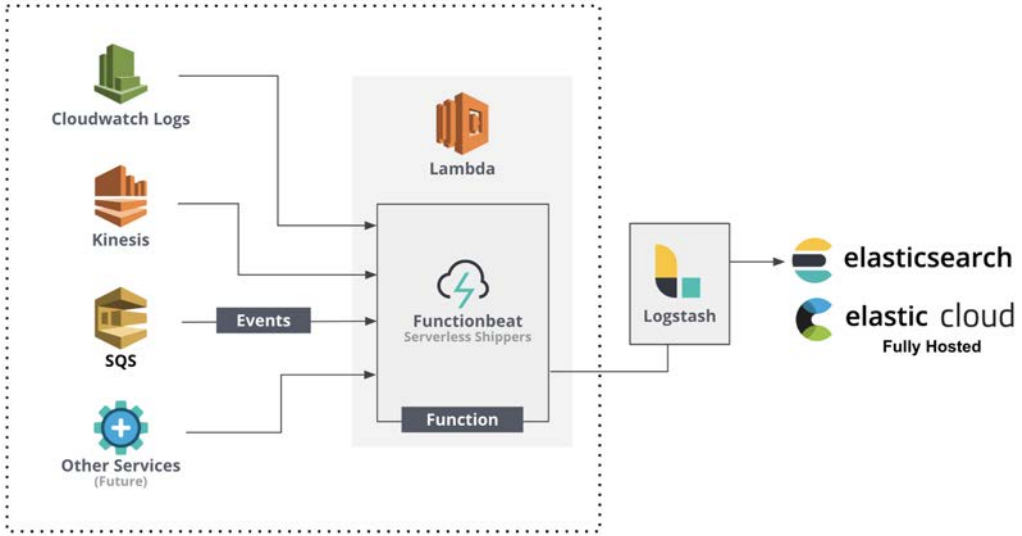
Functionbeat 機能向上

サーバレス環境のデータ収集

Logstash outputをダウンロードのストリーム処理用に追加

構成可能な**function tags**を追加

- グルーピングと
  フィルタリング
- コスト賦課やチャージバック




```
# Tags are key-value pairs attached to the function.
#tags:
#  department: ops
```

functionbeat.yml

https://www.elastic.co/guide/en/beats/functionbeat/current/logstash-output.html

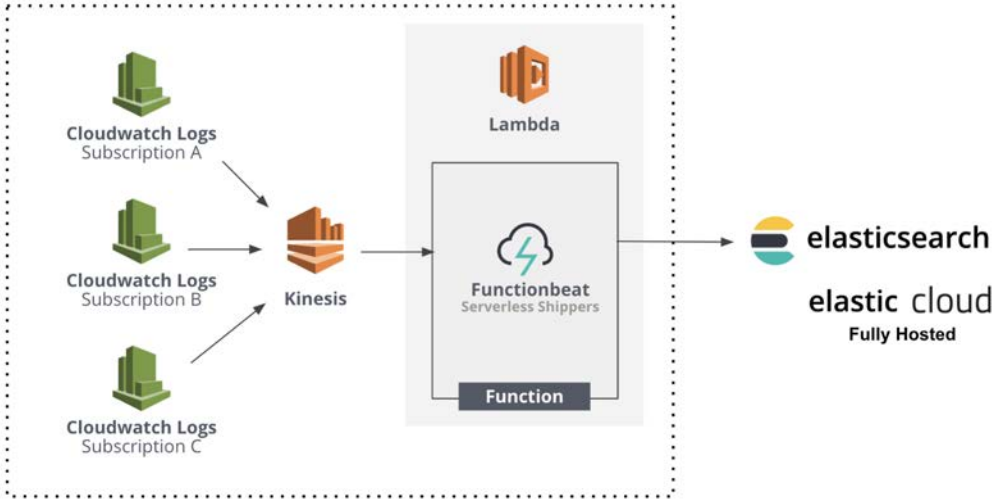
CloudWatch LogsのKinesis経由での投入

サーバレス環境のデータ収集

AWS CloudWatch LogsをKinesis経由で収集する、人気のあるクラウドモニタリングのアーキテクチャを可能に

新しい **Cloudwatch Logs Kinesis** function typeを追加

さらに**マルチサブスクリプションの** CloudWatch Logsモニタリングも可能に

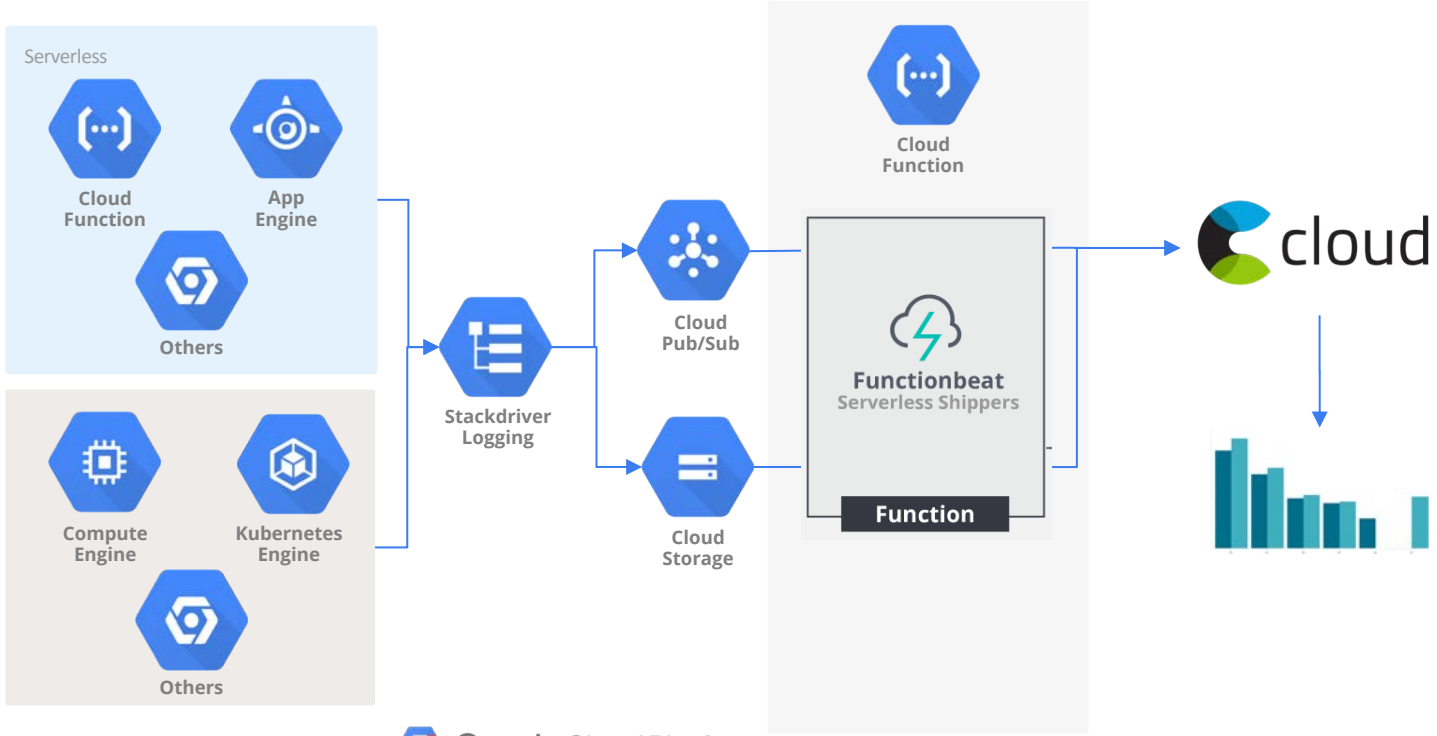


https://www.elastic.co/guide/en/beats/functionbeat/current/functionbeat-reference-yml.html

Functionbeat for Google Function

サーバレス環境のデータ収集

https://www.elastic.co/guide/en/beats/functionbeat/current/configuration-functionbeat-gcp-options.html



Google Cloud Platform

elastic

プラットフォームサポートの拡張

Beats Feature ハイライト

新しい **operating systems**

- RHEL 8
- Amazon Linux 2
- Ubuntu 18.04
- Windows Server 2019

Windows Server 2019

プラットフォームの拡張 = さらなるデータの拡張

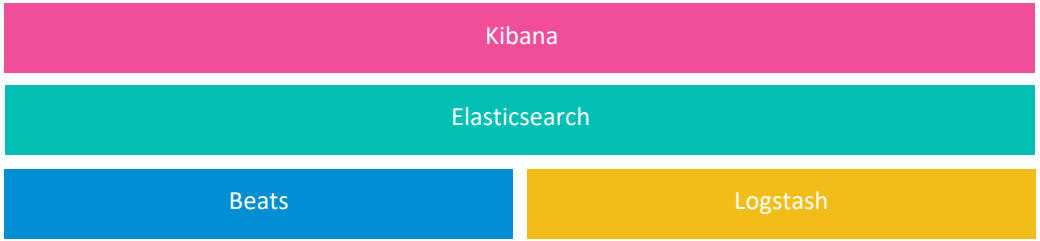
elastic

Search. Observe. Protect.

Elastic エンタープライズサーチ

Elastic オブザーバビリティ

Elastic セキュリティ



Elastic Stack

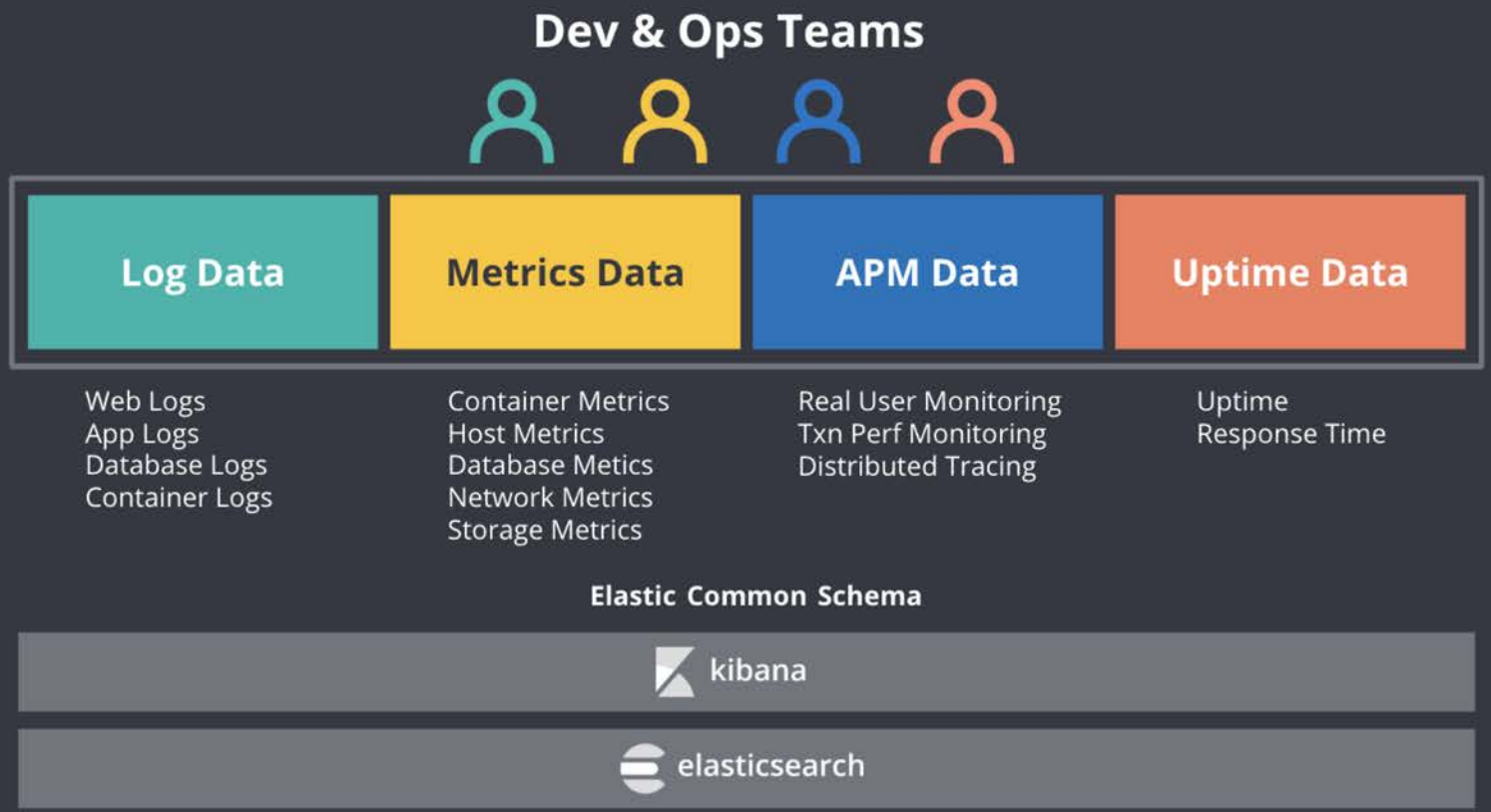
elastic

Elastic オブザーバビリティ

Logs Metrics APM Uptime

elastic

Elastic Approach to Observability

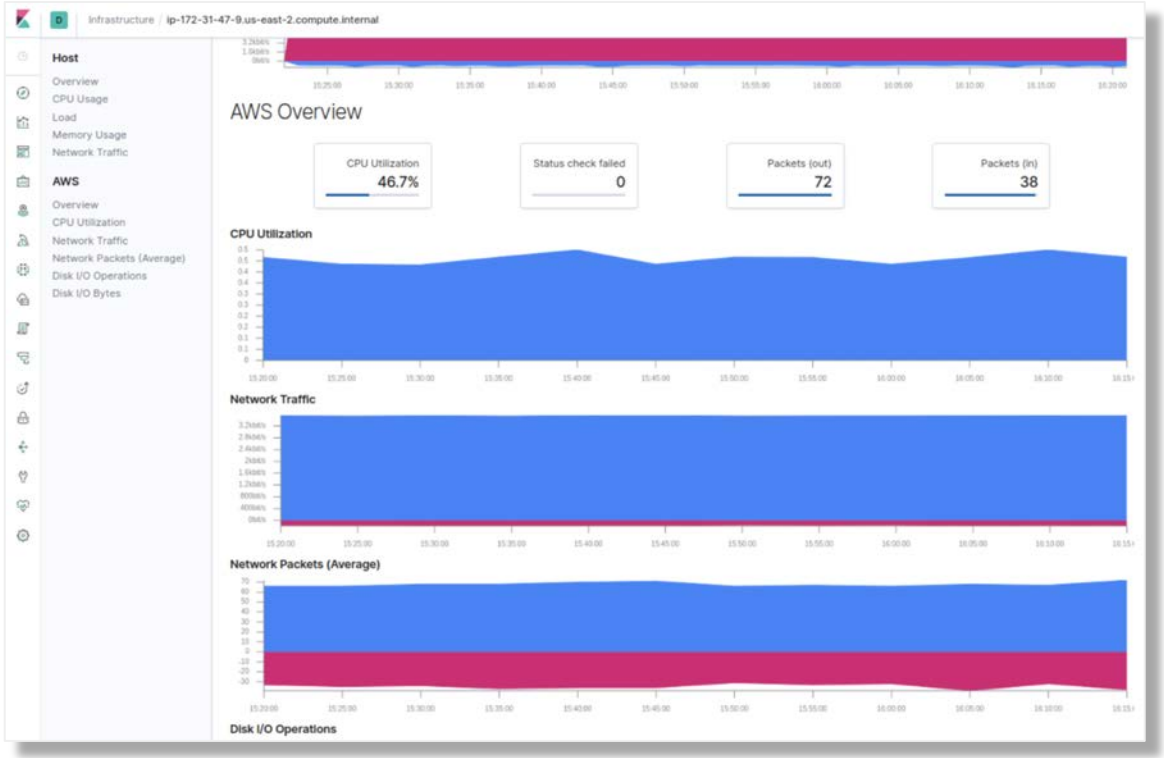


Cloud Monitoring

elastic

AWSオーバービューページ

AWS環境のヘルスを可視化



https://www.elastic.co/blog/elastic-infrastructure-7-4-0-released

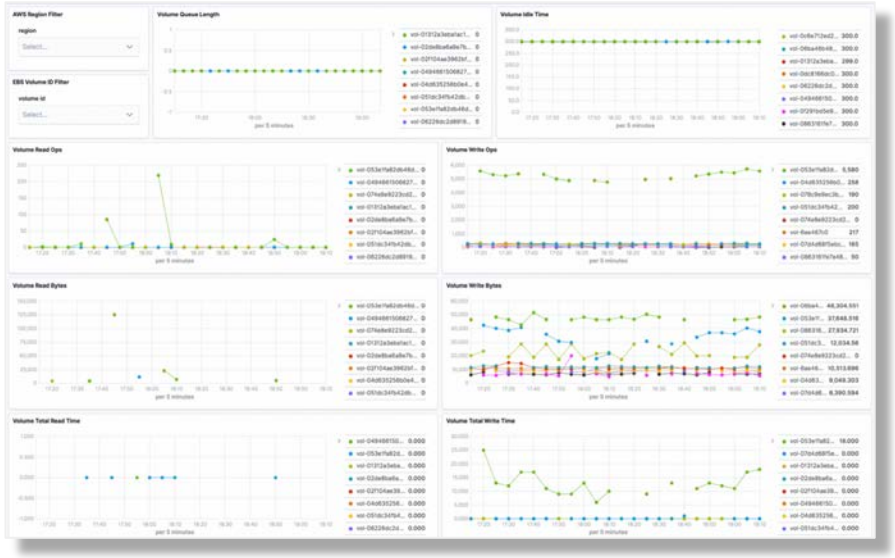
AWSメトリクスの統合

#welovecloud

Metricsets

- ec2
- sqs
- s3_requires/s3_daily_storage
- cloudwatch
- ebs
- elb
- rds
- sns
- sqs

CloudWatch Statistics(Metric Aggregation)



```
metricsets:
   - cloudwatch
 metrics:
   - namespace: AWS/EC2
     name: ["DiskWriteOps"]
     statistic: ["Maximum", "Minimum"]
```


https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-module-aws.html

AWS Tags as Filters

ユーザーのコンテキストでモニタリング

Tagによってユーザーコンテキストをリソースに追加可能に

AWS moduleに新しい構成オプション

ユーザーのコンテキストでフィルター可能に

```
- module: aws
  period: 300s
  metricsets:
    - cloudwatch
  metrics:
    - namespace: AWS/EC2
      tags.resource_type_filter:ec2:instance
      statistic: ["Average"]
      tags:
        - key: "Organization"
          value: "Engineering"
```

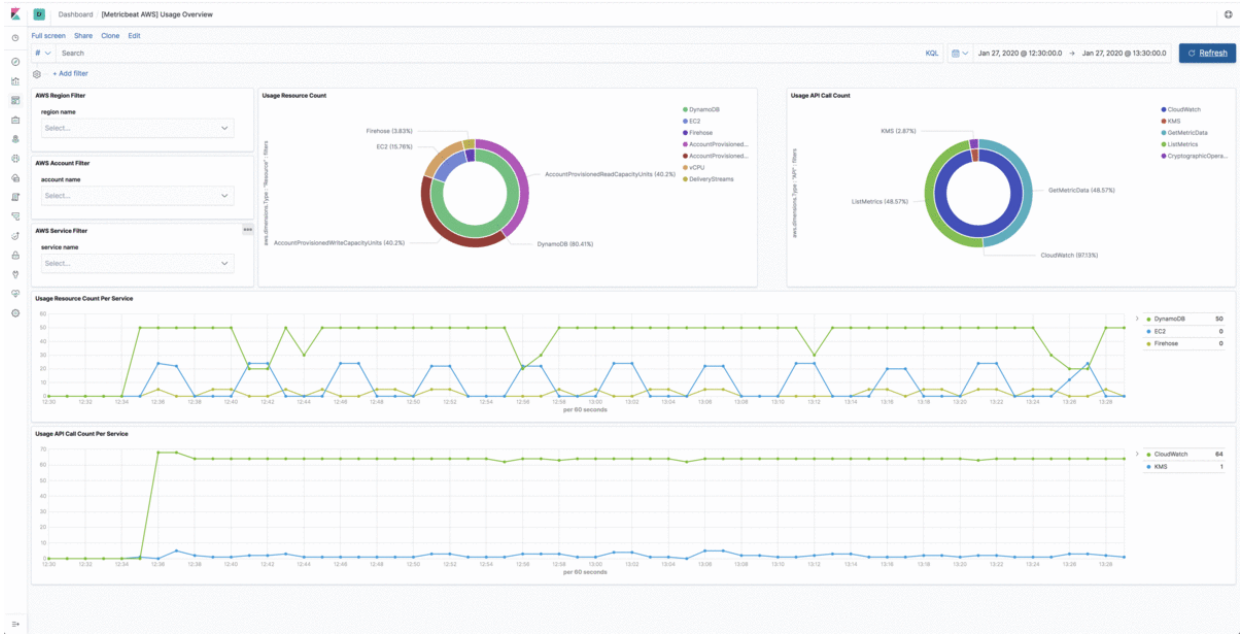

https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-module-aws.html

BASIC

AWS billing and usage

リソース利用状況と課金情報を素早く可視化

- billing:
  AWSのEstimated Chargeを収集
- usage:
  AWS Cloudwatch API を使ってAWSリソースの利用状況を取得



https://www.elastic.co/guide/en/beats/metricbeat/7.6/metricbeat-metricset-aws-billing.html

https://www.elastic.co/guide/en/beats/metricbeat/7.6/metricbeat-metricset-aws-usage.html

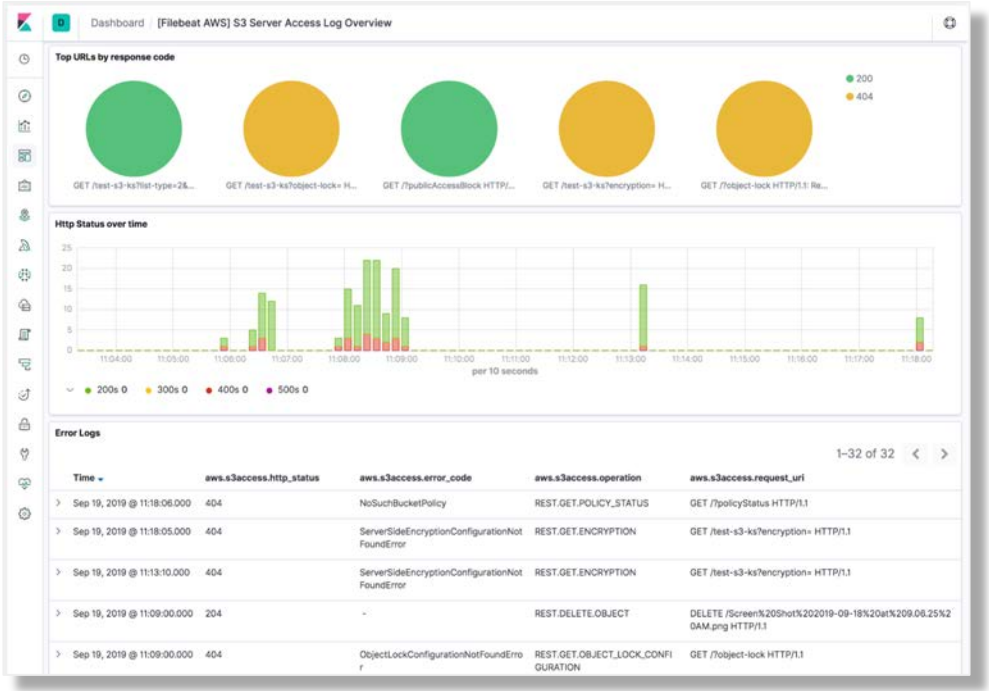
elastic

BASIC

AWS S3 Server Log 向けモジュール

S3のアクセスログとS3に溜められたログを収集

- S3に溜められた各種サービスログ
  - VPC flow logs
  - ELB access logs
  - CloudTrail logs
- S3 Serverアクセスログ
  - Security Audits
  - Access Logs
  - S3の利用率を見るのに有効
- プリセットのDashboard



https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-input-s3.html

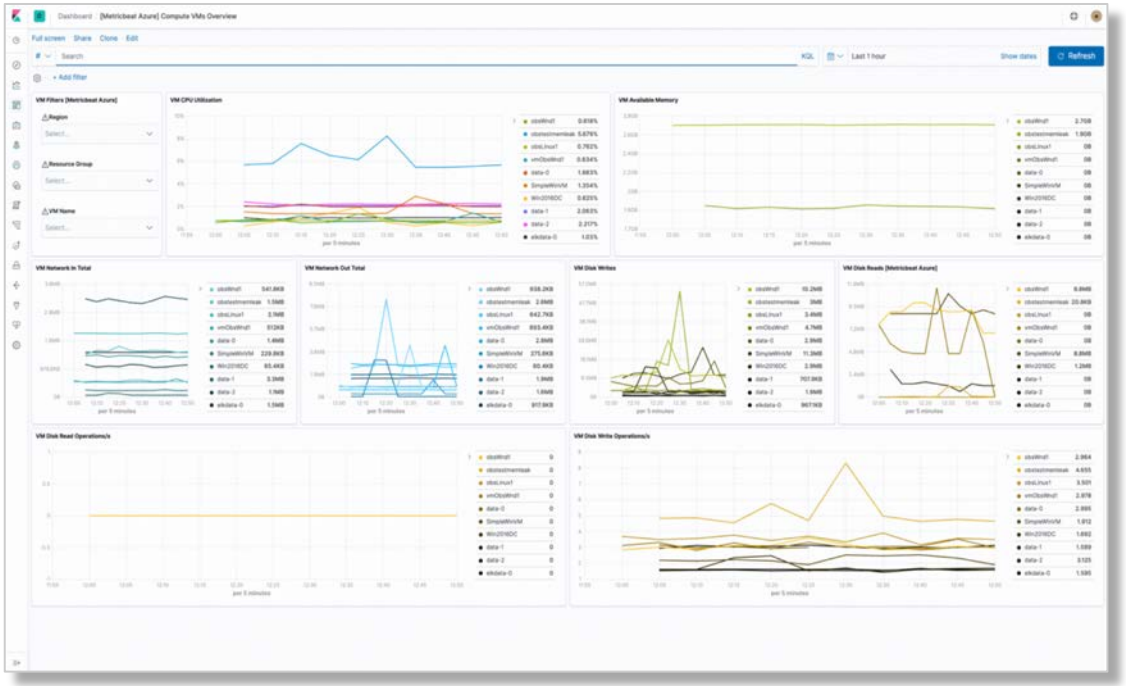
https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-aws.html

elastic

Azureモニタリング

Achievement unlocked!

- Azure環境をモニタリング
- Metricsets
  - `monitor`
  - `compute_vm`
  - `compute_vm_scaleset`
  - `storage`
- プリセットのDashboard
- Multi cloud monitoring
  - `Azure | AWS | *`



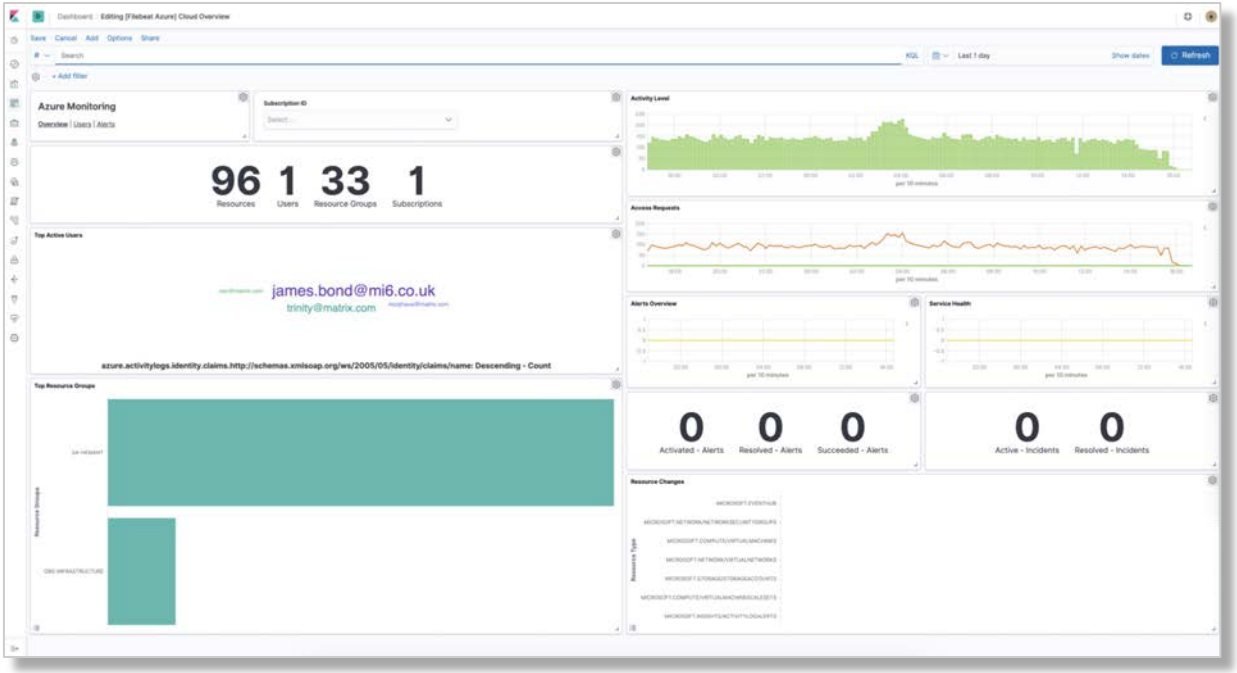
https://www.elastic.co/blog/elastic-metrics-7-5-0-released
https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-module-azure.html

elastic

Azure Event Hub logs

サポートされるfilesets

- activitylogs
- signinlogs
- auditlogs



https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-azure.html

GCPモニタリング

Multi-Cloud環境を単一のインターフェースでモニタリング可能に

- GCP環境をモニタリング
- Metricsets
  - Compute
- Stackdriver APIsを活用
- FilebeatにもGoogle Cloud Moduleが追加
  - VPC flow logs
  - Firewall logs

```
metricbeat.modules:
- module: googlecloud
  metricsets:
    - compute
  zone: "us-central1-a"
  project_id: "your project id"
  credentials_file_path: "your JSON credentials file path"
  exclude_labels: false
  period: 300s
```

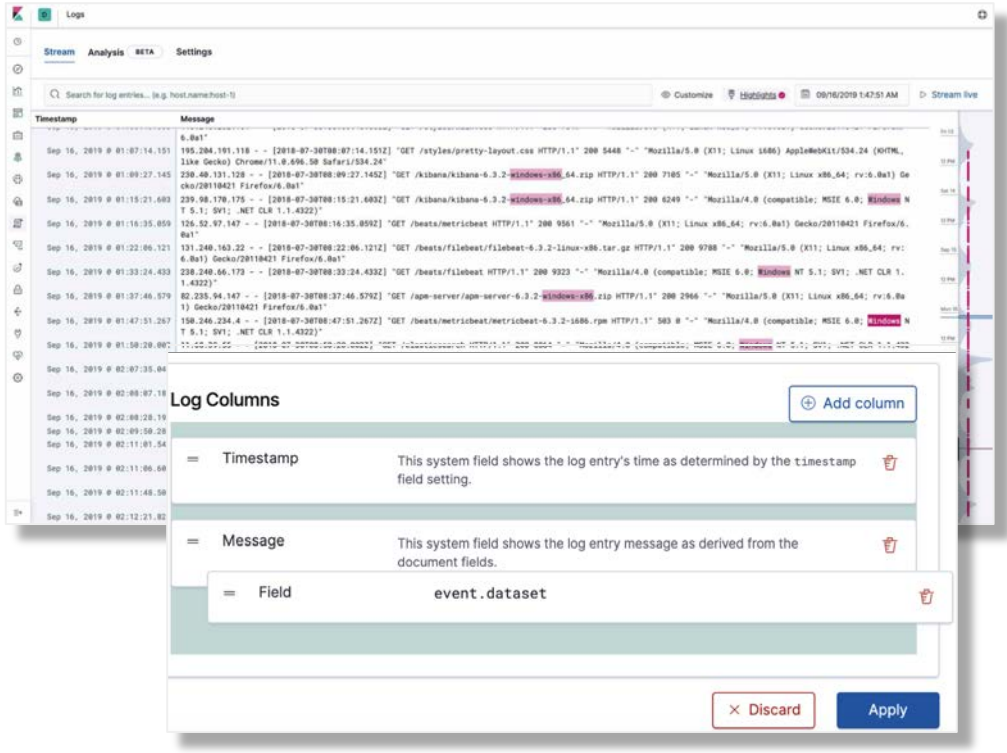
https://www.elastic.co/blog/elastic-observability-7-6-0-released
https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-module-googlecloud.html
https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-googlecloud.html

Logs

Logs App 機能向上

さらなる機能追加

- カラム順序を自在に変更
  - ログカラムをドラッグ＆ドロップで
- キーワードのハイライト!
  - 固有のミニマップ
  - 出現数
  - 説明や推奨するアクションに活用
- UXの向上



https://www.elastic.co/blog/elastic-logs-7-4-0-released

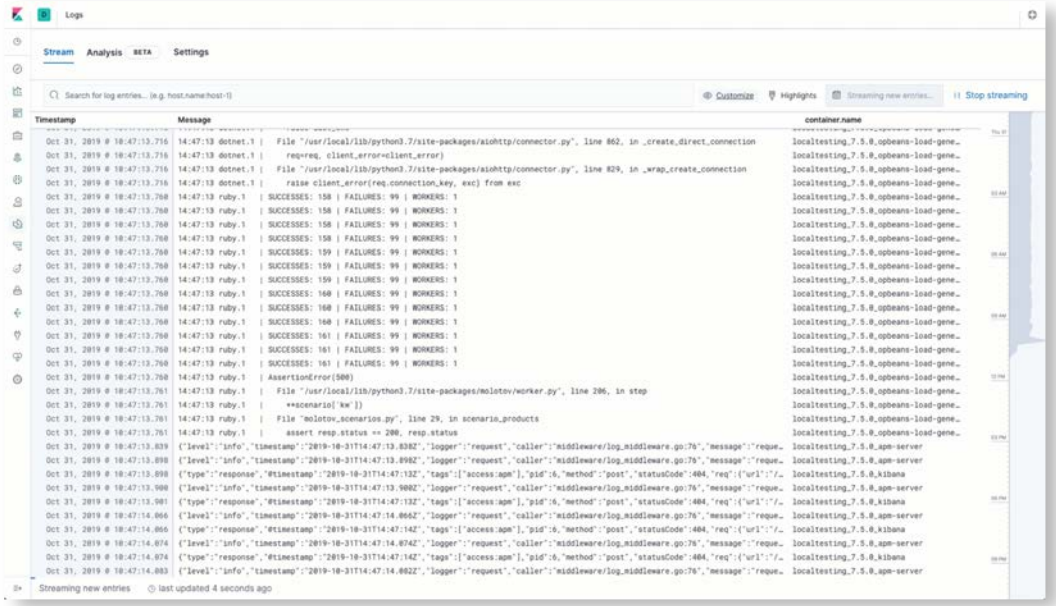
PLATINUM

Log Rate 異常検知

どこにアドレスすべきなのか？

管理者やアナリストが、データセット毎にログレートから異常を検知することを支援

- 新しくリリースしたアプリのログが急に増えた*(新規Appの影響?)*
- 既存アプリのログでスパイクが発生 *(アタック? プロモーション?)*
- 既存アプリのログが突如止まった *(Appダウン? ログシッパーのダウン?)*



https://www.elastic.co/blog/elastic-logs-7-5-0-released

elastic

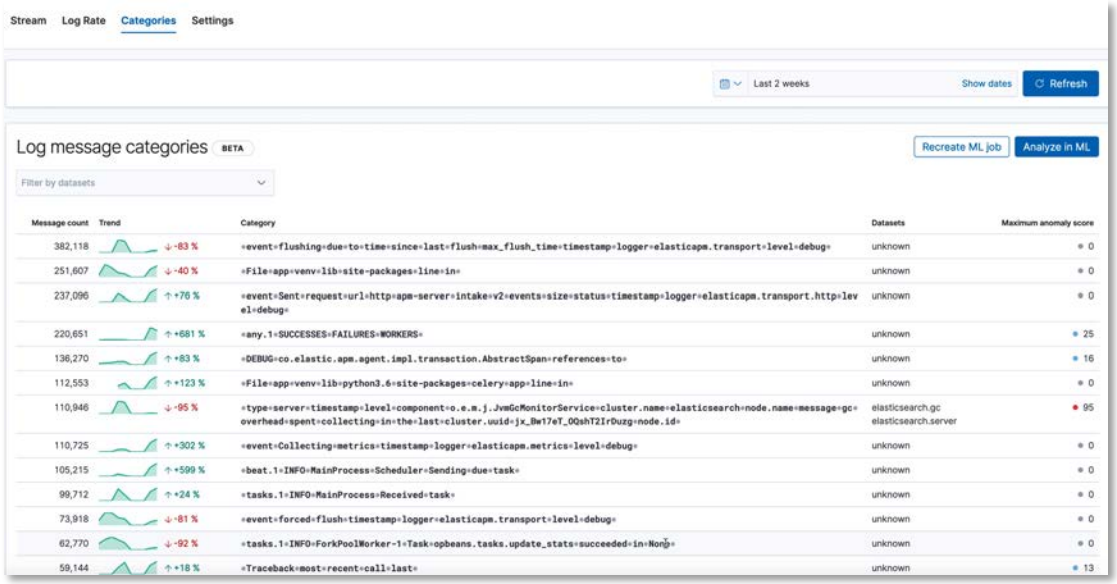
PLATINUM

Logの自動分類

根本原因の発見をスピードアップ

ログパターンを識別し、機械学習により異常を検知

- 期待される動作を予測
  機械学習を活用し異常を検知
- ログパターンを指示せずに異常を検知
  ユーザーは正確なログのパターンを意識せずとも、機械学習がログを分類
- 機械学習の経験は不要
  インデックスと学習用の期間を入力するだけでOK



https://www.elastic.co/blog/elastic-logs-7-6-0-released

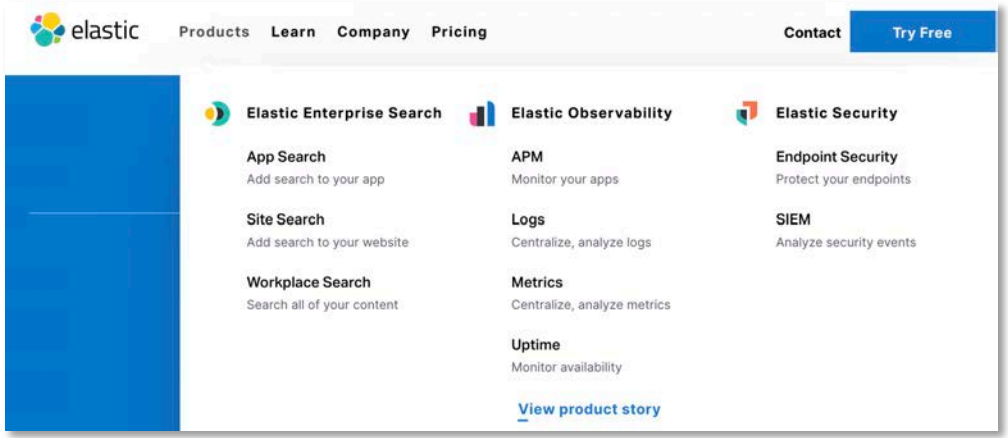
elastic

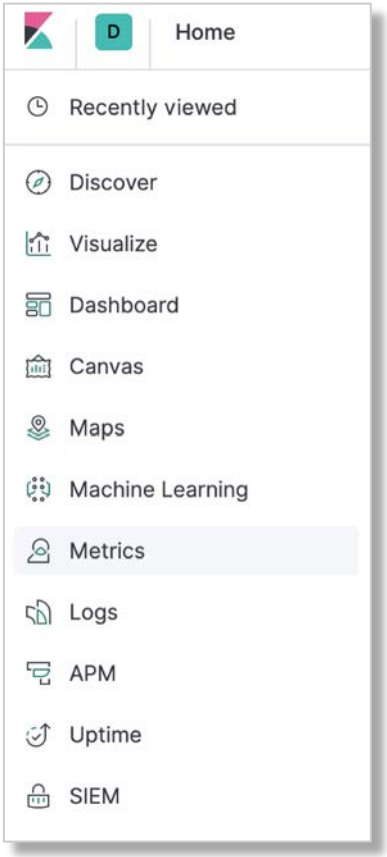
Metrics

Infrastructure app → Metrics app

オブザーバビリティ

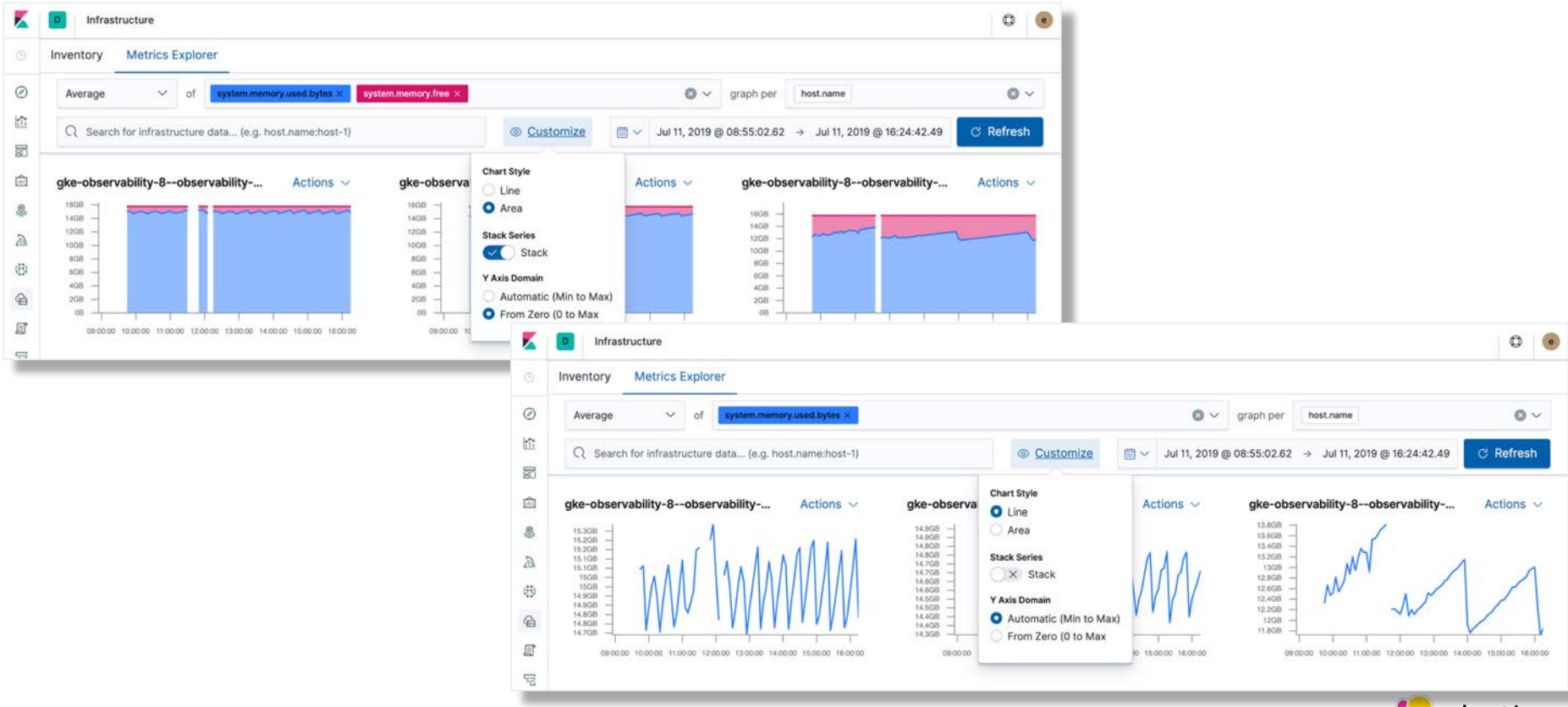
インフラのモニタリング以上の機能に！





elastic

Metrics Explorerがカスタマイズ可能に



https://www.elastic.co/blog/elastic-infrastructure-7-4-0-released

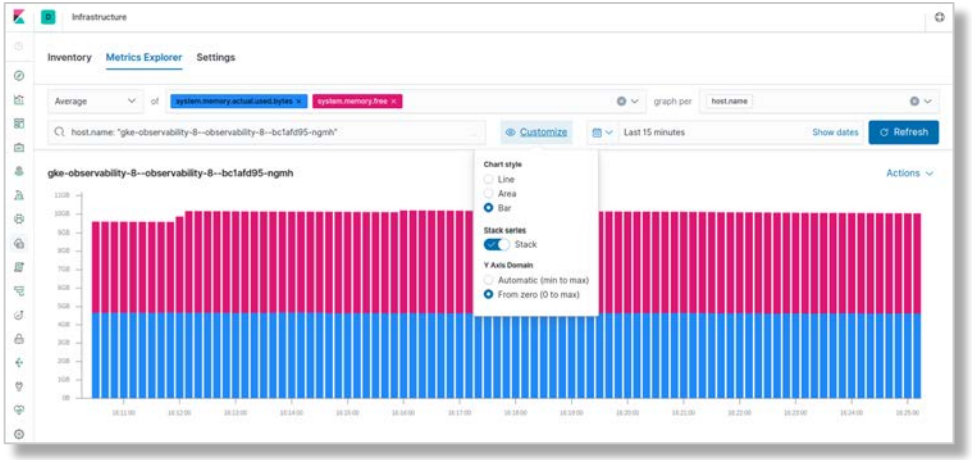
Metrics Explorerのバーチャート

how do you data?

新しいチャートのオプション

カウンターや疎らな測定値を可視化するのに便利

積み上げチャートにして比較が容易に



https://www.elastic.co/blog/elastic-metrics-7-5-0-released

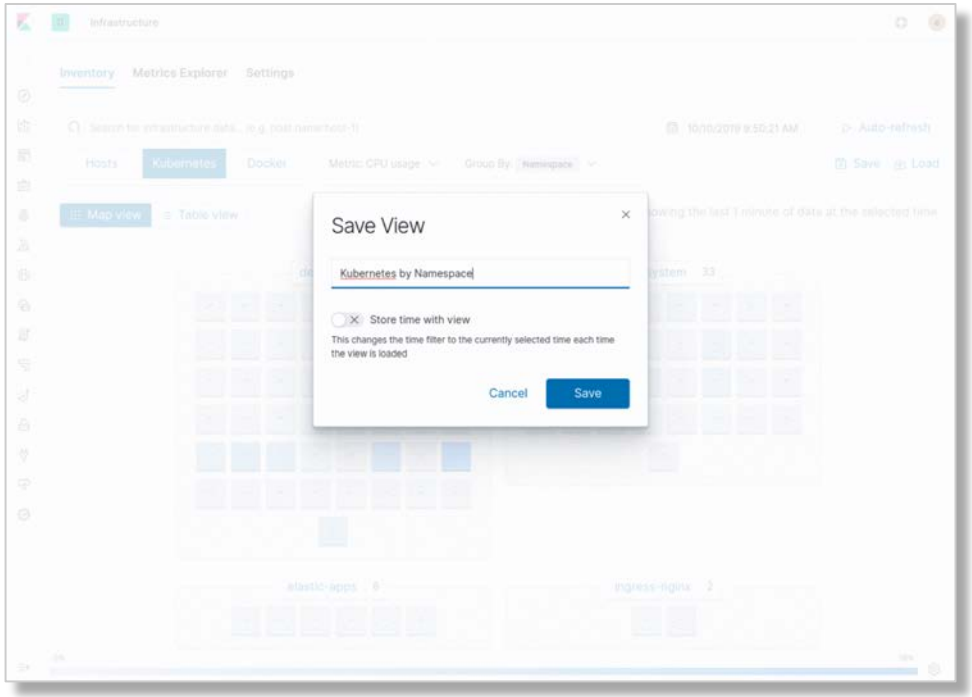
InventoryとMetrics Explorerが保存可能に

独自のプリセット

フィルター、検索、グルーピングを保存可能に

過去の保存結果をいつでもロード可能に

複数のリソースやメトリクスを見る時に便利



https://www.elastic.co/blog/elastic-metrics-7-5-0-released

APM

.NET Framework フルサポート

オートインストゥルメントをサポートし、プラグ&プレイの体験を

- アウトオブボックスのオートインストゥルメントを.NET Frameworkでサポート
  - トランザクションの作成し追跡するためのコードの変更は必要なし

- Supported Technologies
  - .NET Core 2.1~
  - .NET Framework 4.6.1~
  - Entity Framework Core 2.x
  - Entity Framework 6 6.2~
  - System.Net.Http.HttpClient on .NET Core
  - System.Net.Http.HttpClient on .NET Framework

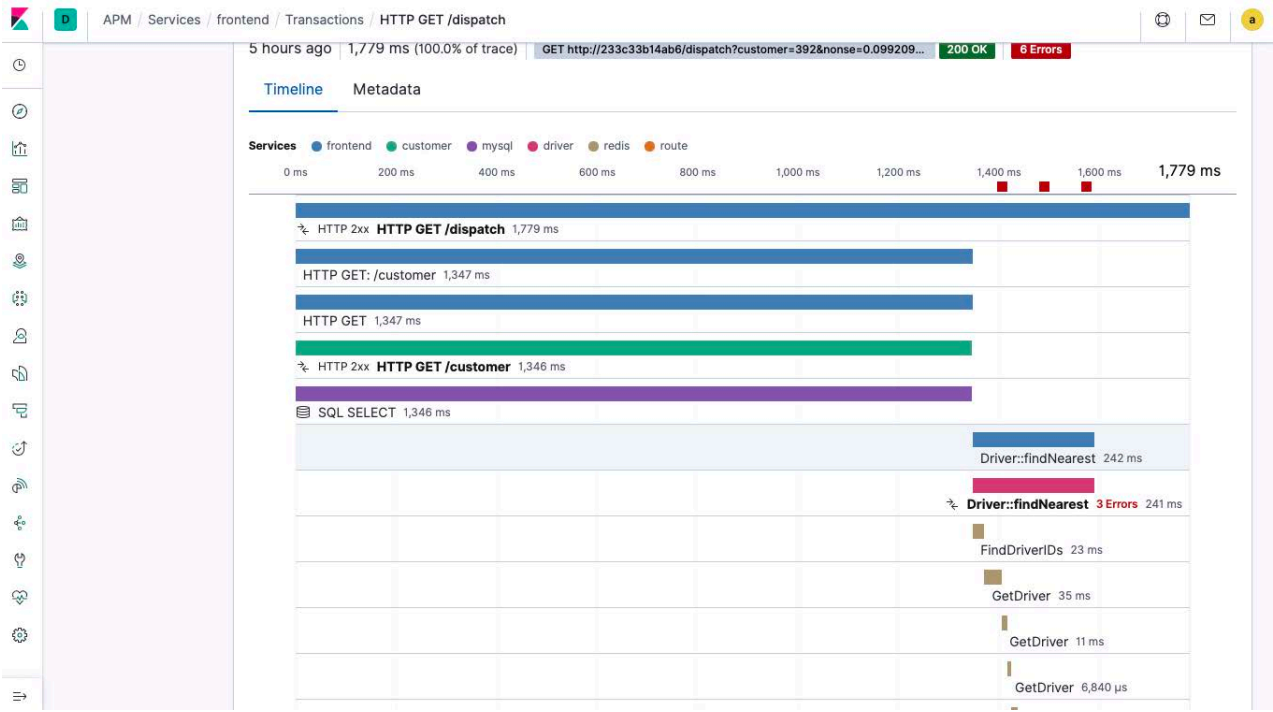
https://www.elastic.co/blog/elastic-apm-7-4-0-released

OSS

BASIC

Jaeger Intake

- Jager Agentで生成されたトレースをAPM Server経由でElasticに収集
- APM ServerのgRPCとThriftがサポートされる
- Jaegerから取り込まれたデータはElasticのデータモデルに自動的にマッピング
- トレースを受信するための新しいポートを開ける必要がある
- APM ServerはEnableに

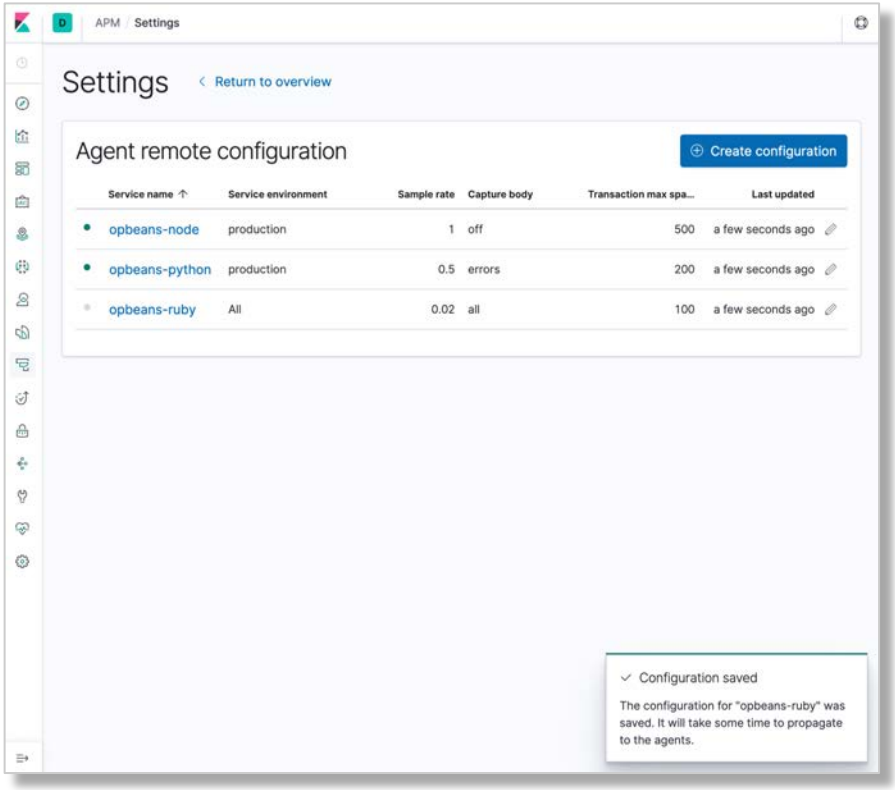


https://www.elastic.co/blog/elastic-apm-7-6-0-released
https://www.elastic.co/guide/en/apm/server/7.6/jaeger.html

elastic

KibanaからAgent Configurationが可能に

- HTTP RequestのBodyを収集するか(CAPTURE_BODY)
- 分散トレースにおける Max. number of spans (TRANSACTION_MAX_SPANS)
- サンプルレート (TRANSACTION_SAMPLE_RATE)



https://www.elastic.co/guide/en/kibana/current/agent-configuration.html

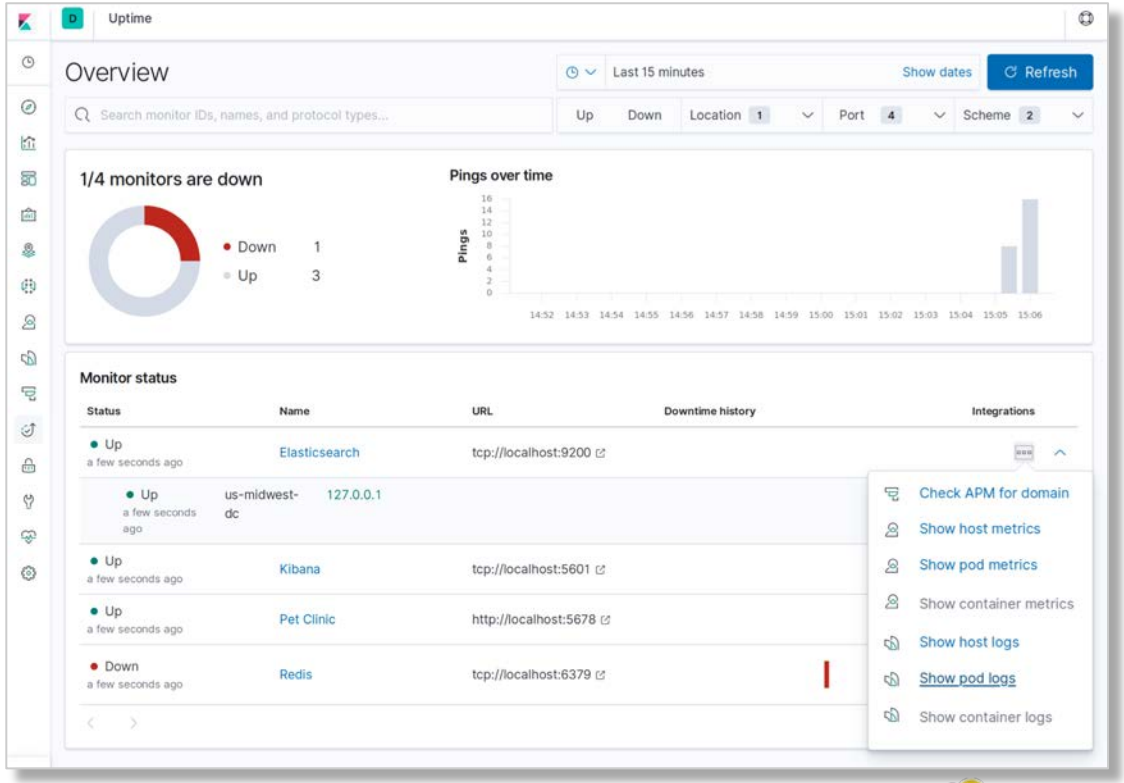
Uptime

Kubernetes Servicesのステータス監視

Hint-based auto-discovery

特別なラベルをPod/Containerに付与することで、HeartbeatがDockerおよびKubernetesから直接監視出来るように設定

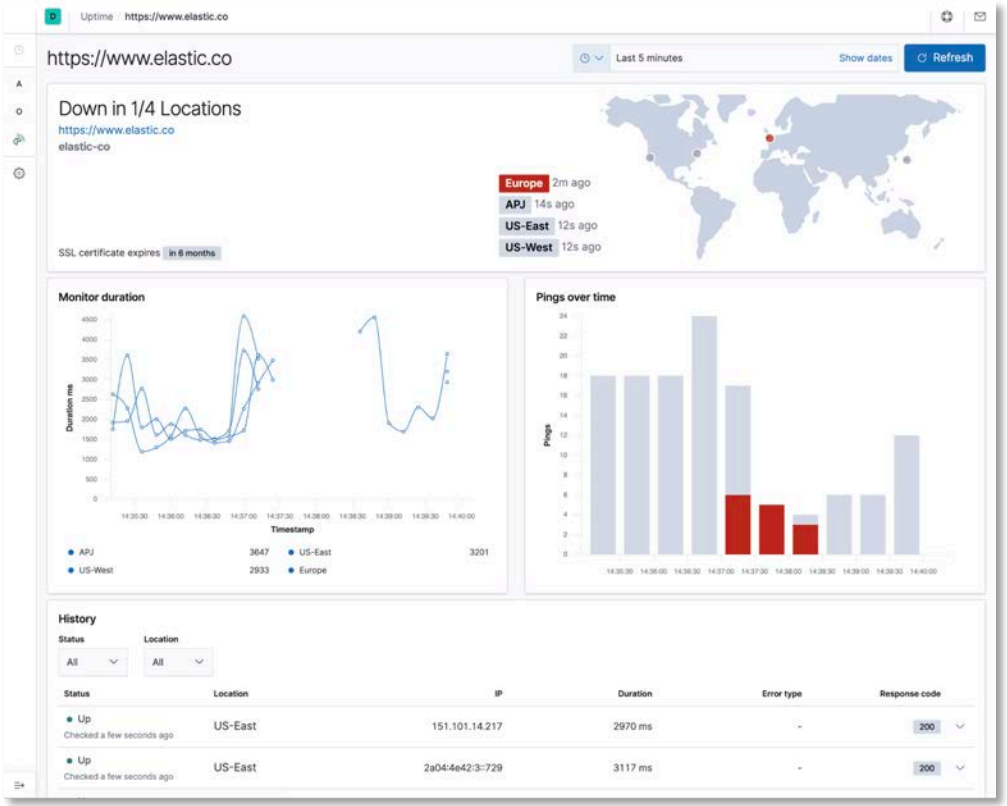
PodもしくはContainerがスタートすると、HeartbeatがHintが設定されていないかをチェックし、適切な構成で開始



https://www.elastic.co/blog/elastic-uptime-monitoring-7-5-0-released

グローバルでの分散Uptimeチェックの可視化

異なるロケーションにおいて、Uptimeを使って監視を行っている場合に、一目で理解出来るマップとステータスビューを提供



https://www.elastic.co/blog/elastic-uptime-monitoring-7-6-0-released

elastic

Elastic セキュリティ

Endpoint　　SIEM

elastic

Elastic Endpoint Security

エンドポイントから始めるセキュリティ

ダメージを受け失う前に
マルウェアや
ランサムウェアを阻止

AIベースの
エンドポイントにおける
検知と対応

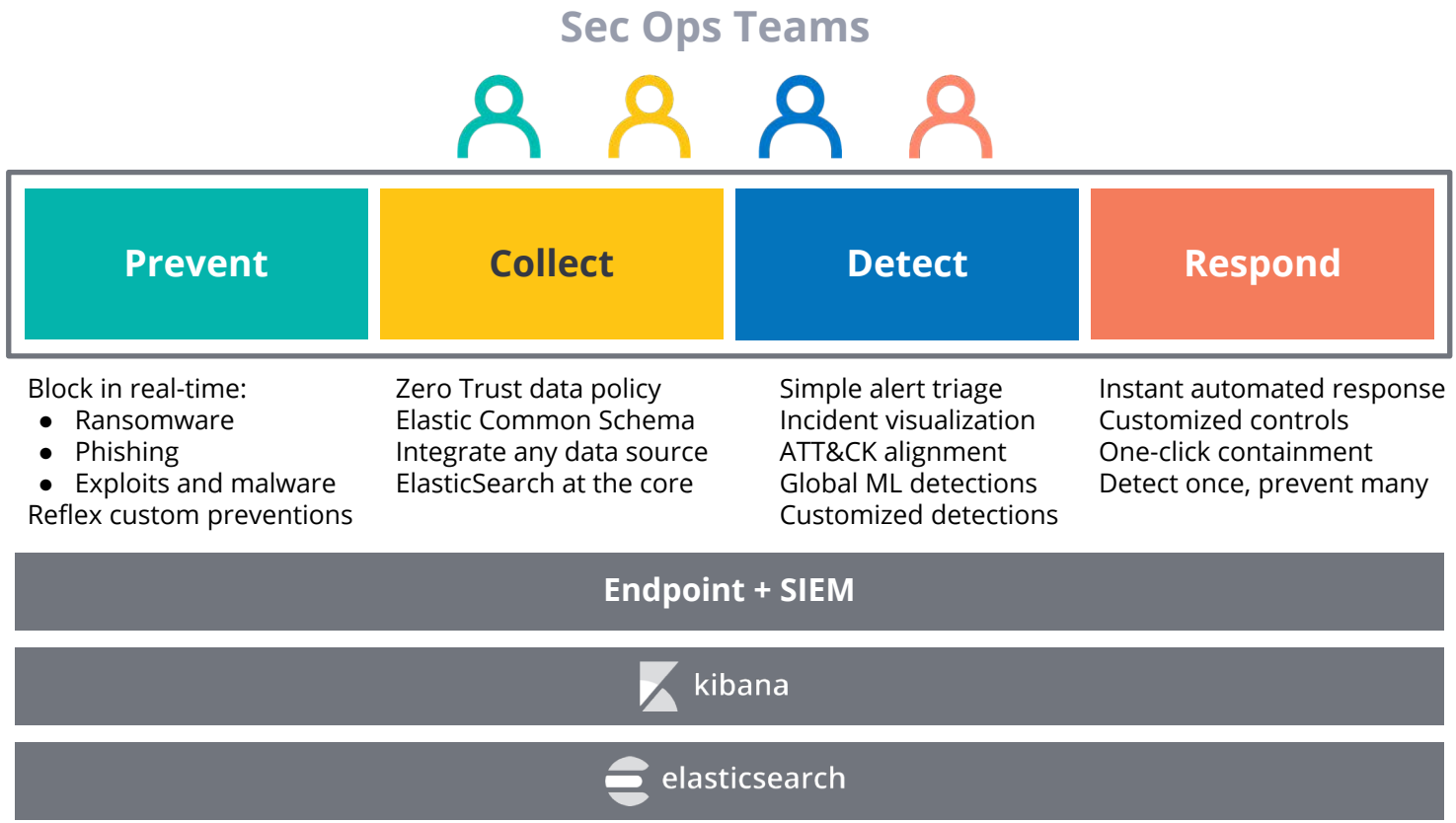
今日のハイブリッド・
クラウド環境を前提に設計

Elastic Endpoint Security

アンチウイルスソフトのように簡単で、もっとパワフル

elastic

Elastic Security



elastic

Prevent

ENTERPRISE

脅威をいち早くブロック

インラインで自律的に防止

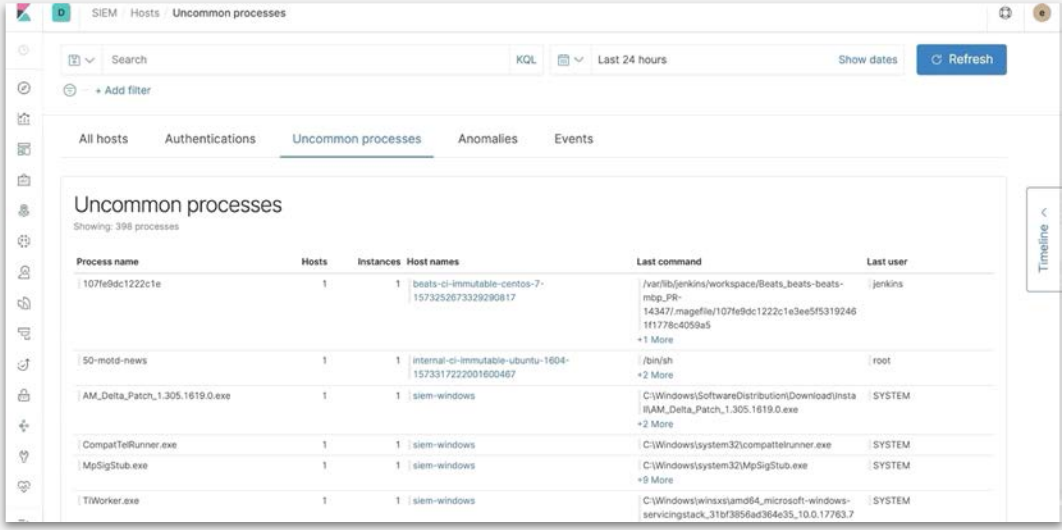
ランサムウェア、フィッシング、脆弱性への攻撃、マルウェアを厳格な第三者機関のテストで裏付けされた能力でブロック
クラウドでの分析は必要なし

MITRE ATT&CKマトリクスにマッピング

ただのペイロードではなく、何らかの破壊や損失の前に、敵対的な挙動を防止

完全にカスタマイズ可能なコントロール

固有の防止ポリシーを作成し、簡単にスケーラブルに適用可能



Collect

ENTERPRISE

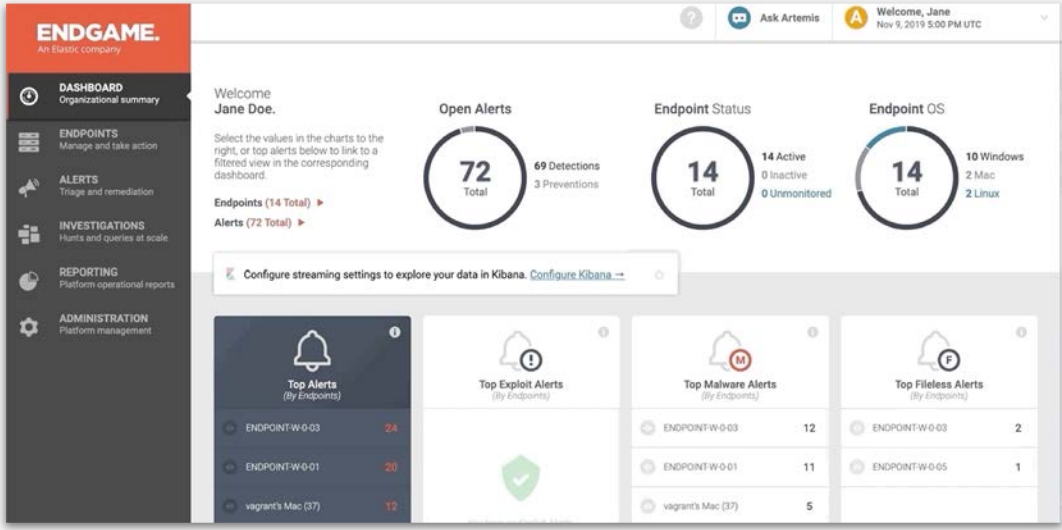
全てのセキュリティデータをストアし、検索可能に

ゼロトラスト・ポリシー
耐タンパー性のためのカーネルレベルのデータ収集とエンリッチメント

Elastic Common Schema (ECS)
データモデルの統合のためのオープンソースベースの仕様

全てのデータソースへの迅速なアクセス
制限なしに1つの製品で、セキュリティからオペレーション、他のデータソースへアクセス

Elasticsearchを中心に
全てのデータを迅速に検索



Detect

ENTERPRISE

大規模に調査し、スコープを特定

容易なアラートのトリアージ

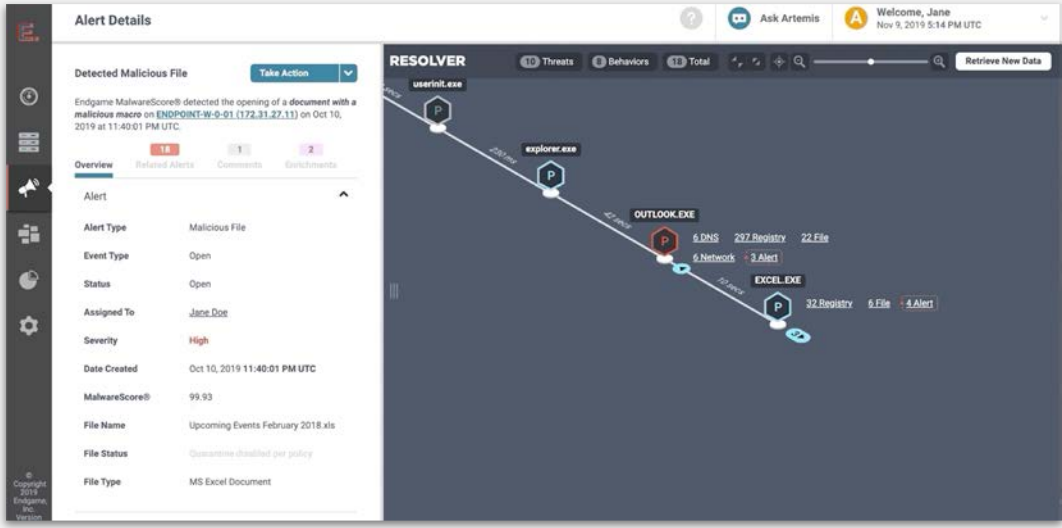
シンプルなワークフローでアラートをアサインし管理

自動的にアタックを可視化

Resolver™ Viewがアタックのスコープ特定や根本原因分析を加速し、ユーザー次の次元へ

カスタマイズした機械学習でグローバルに検知

全てのデータに対する、既にロード済の、ワンクリックの機械学習を使った分析



elastic

Respond

修正、除外、実証

ENTERPRISE

ワンクリックの封じ込め

さらなる敵対的な挙動を防ぐため、迅速にエンドポイントを隔離

リアルタイムかつ自動的なレスポンス

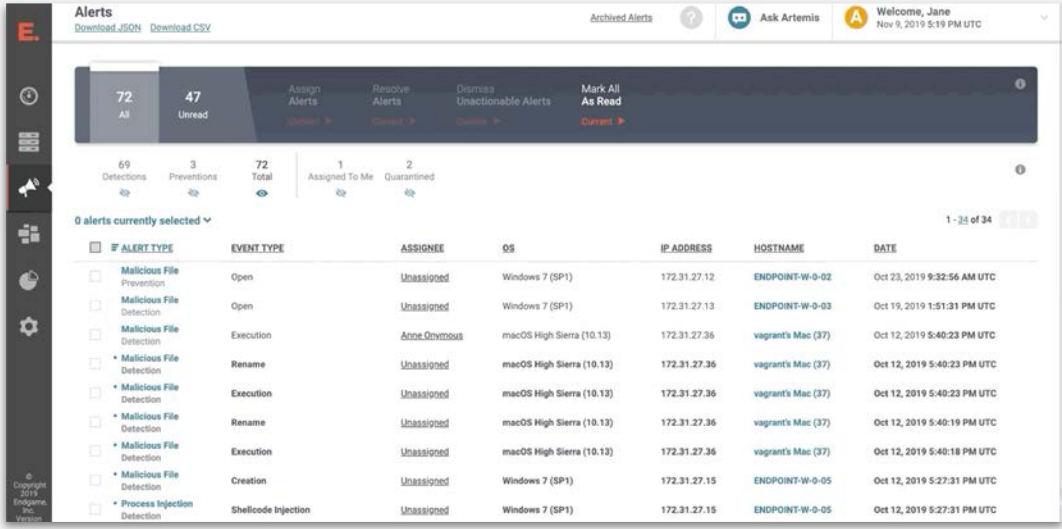
アタックのライフサイクルで、検知に対して自律的なミリ秒単位のレスポンス

一度検知したら何度でも防止

検知した脅威を簡単に防止アクションに変換

既存のワークフローに組み込み

既存のビジネスプロセスに合わせて簡単に統合可能



Elastic SIEM

BASIC

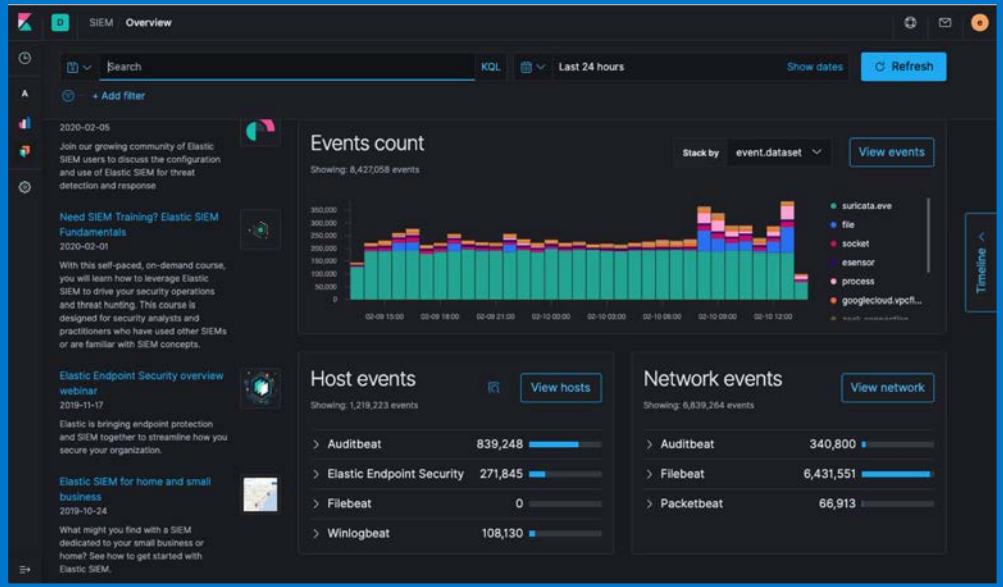
SIEM App Overview

SOCチーム向けの要約されたワークフロー

Elastic Endpointとの統合
Endgameセンサーマネジメントプラットフォームからのセキュリティイベントがendgame-* indicesとして統合

新しいUI
トップソース/デスティネーション・カントリー、TLSウィジェット、イベントヒストグラムなど

新しい機械学習Job
PacketbeatとWinlogbeatイベント向けの新しい機械学習Jobの追加



https://www.elastic.co/blog/elastic-security-7-5-0-released

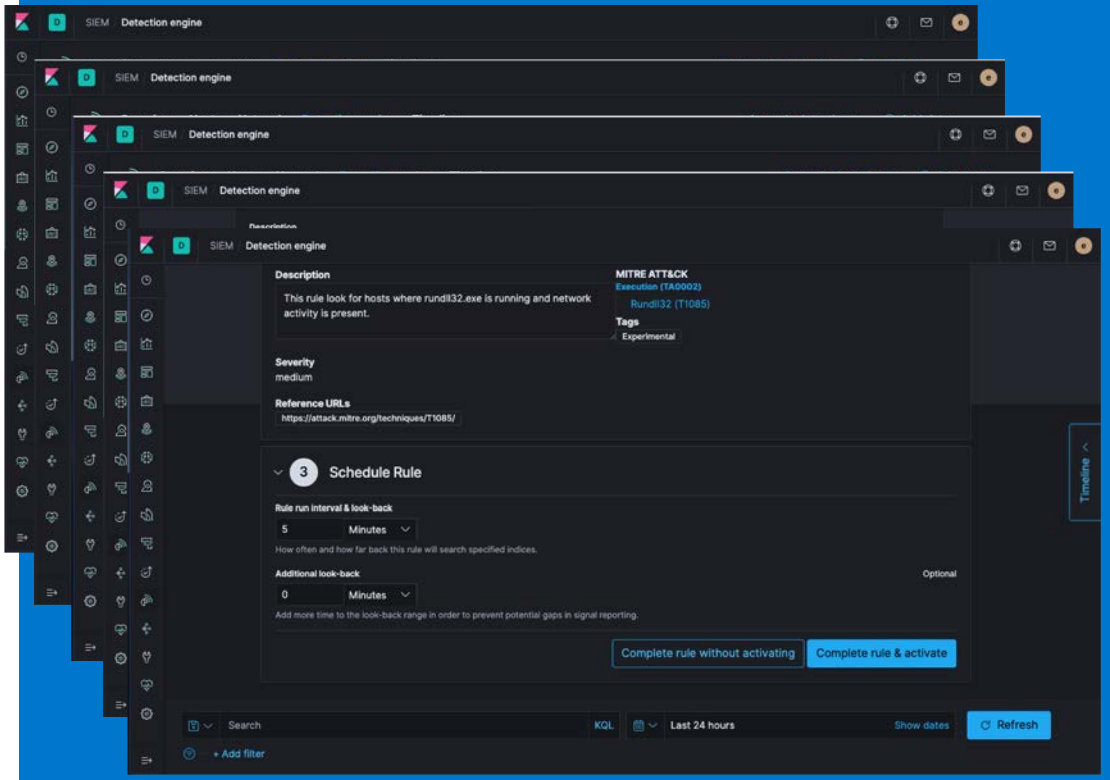
elastic

BASIC

7.6 SIEM Detection Engine

ルールとシグナルの要約と管理

- MITRE ATT&CKに準拠したアウトオブボックスのカスタムルール
- 定期的にルール実行され、シグナルを生成
- SIEM app Timelineにてシグナルの調査が可能
- シグナルはさらに複雑な検知のためのビルディングブロック



https://www.elastic.co/blog/elastic-security-7-6-0-released

elastic

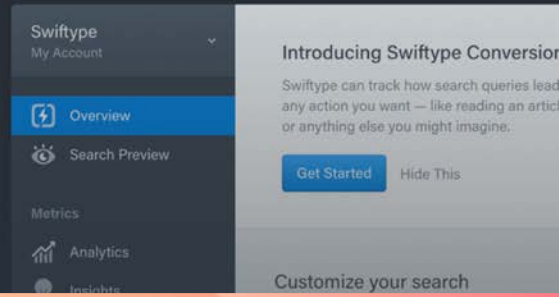
Elastic エンタープライズサーチ

Workplace Search　　App Search　　Site Search

elastic

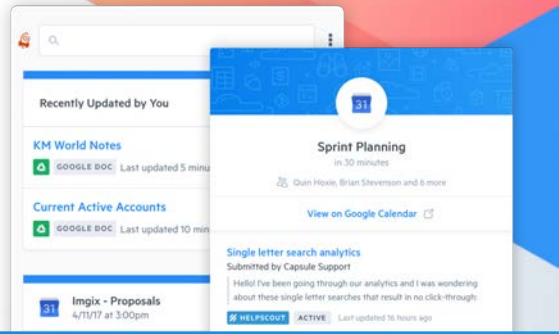
Elastic Site Search

Create and manage a tailored search experience for your website with world-class relevance, intuitive customization, and rich analytics.



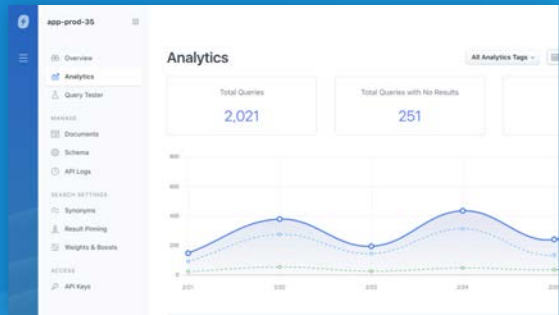
Elastic Workplace Search

Instantly search across all the tools you use at work, including Dropbox, Salesforce, G Suite, Office 365, Zendesk, and more.



Elastic App Search

A powerful set of APIs and developer tools designed for developers building rich, user-facing search applications.



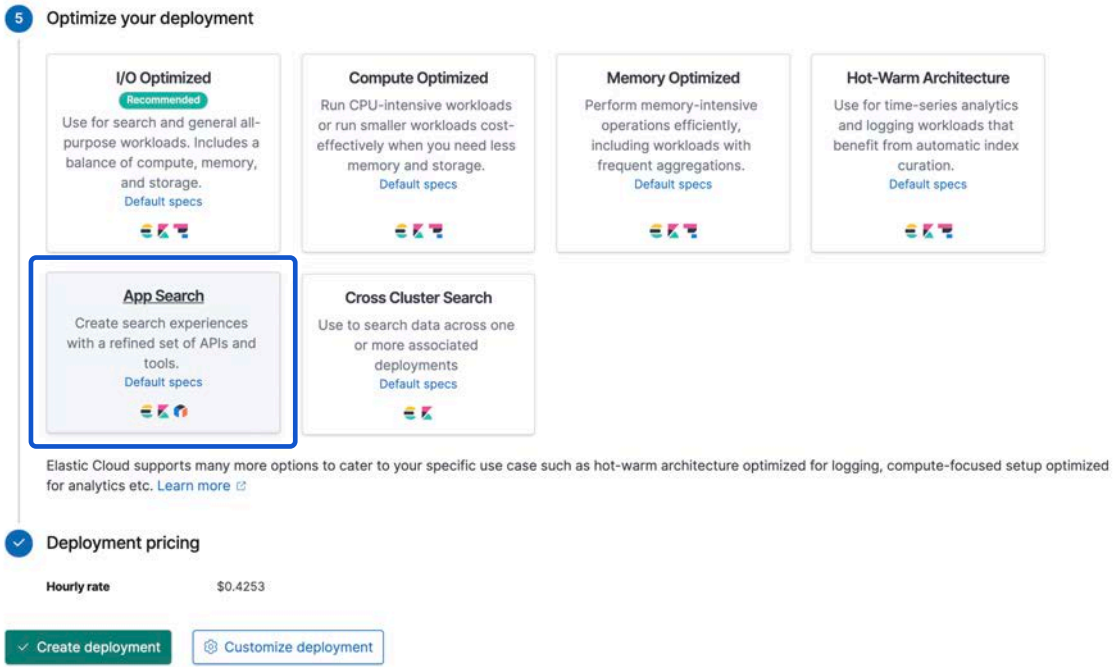
App Search

全てのESS regions で利用可能に

elastic

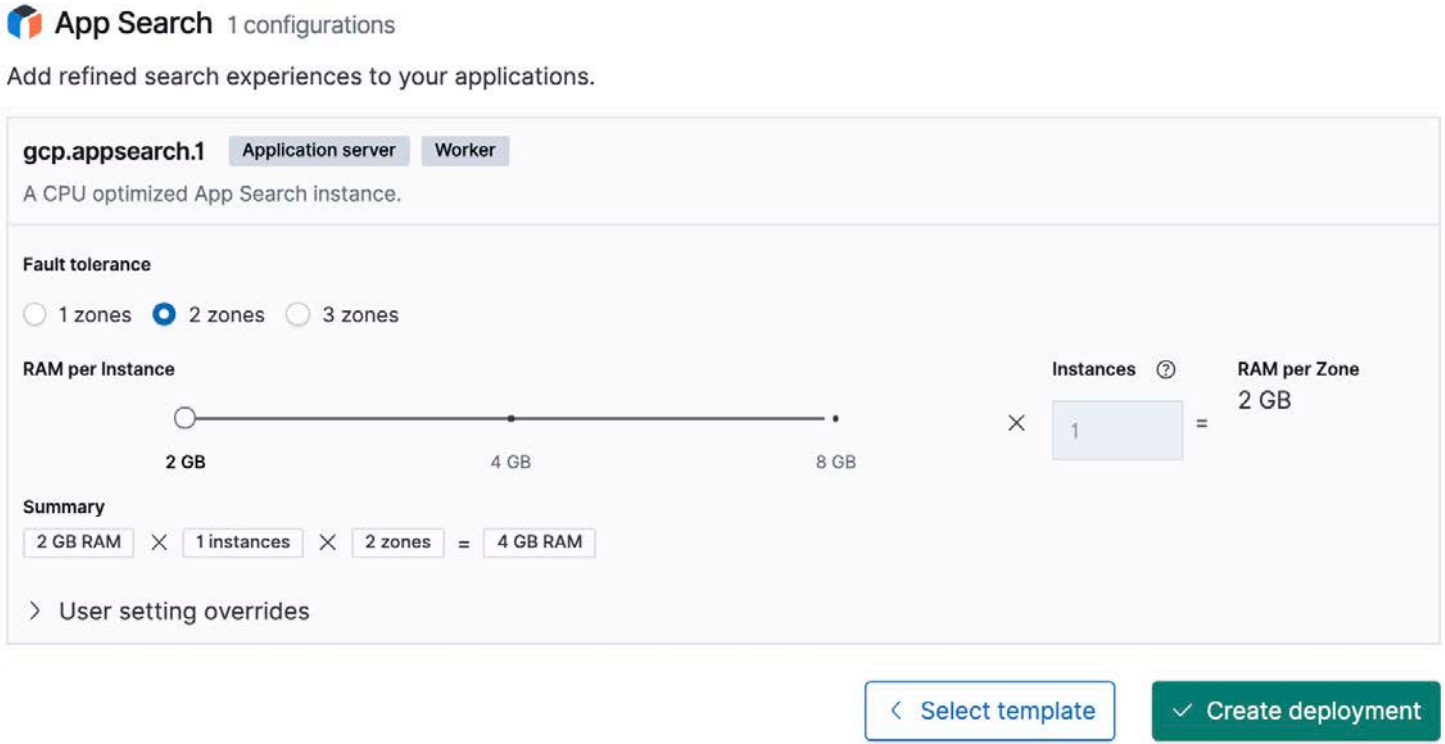
デプロイメントの詳細

- App Search テンプレートを介して利用可能



https://www.elastic.co/blog/elastic-app-search-now-available-on-elasticsearch-service

デプロイメントの構成



https://www.elastic.co/blog/elastic-app-search-now-available-on-elasticsearch-service

デプロイメントの詳細

Stores and queues everything for App Search
Based on high-CPU hardware
1–60GB x 32 nodes x 1–3 Availability Zones

Serves the application
Also based on high-CPU hardware
2–8GB x 16 nodes x 1–3 Availability Zones

Needed for stack upgrades
Can also provide user management
1 GB x 1 AZ (free tier) sufficient

elastic

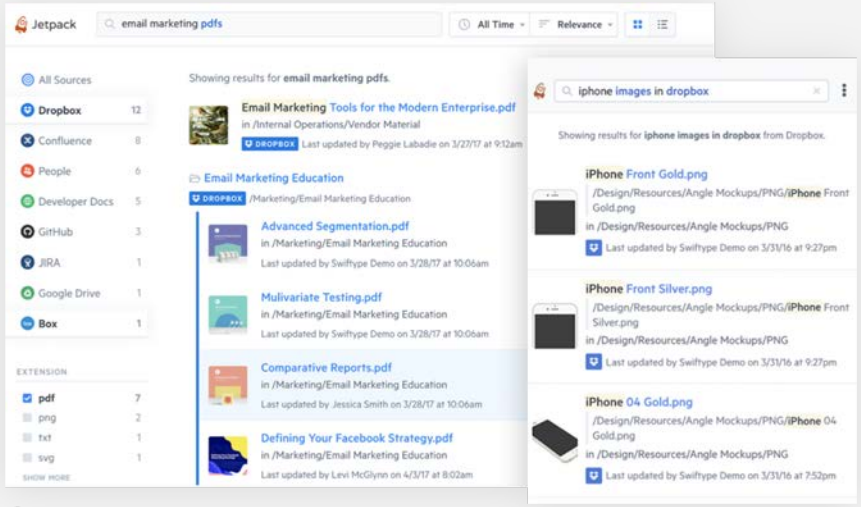
Elastic Workplace Search

is Elasticsearch and much more

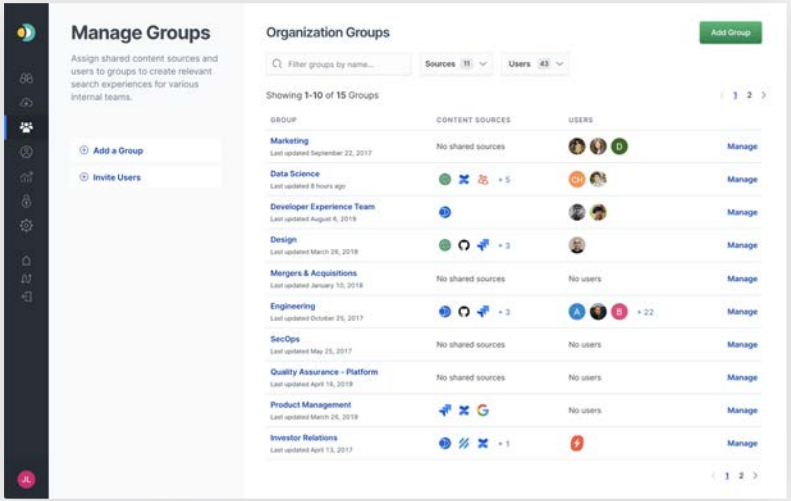
elastic

A complete solution for rolling out a personalized, centralized, secure search experience

Search clients portfolio & workflow integrations



Management Interfaces



Out-of-the-box Connectors

and more

https://www.elastic.co/downloads/enterprise-search

Deployment

16 JANUARY 2020 RELEASES

Elastic Cloud on Kubernetes (ECK) 1.0 is now generally available

By Anurag Gupta

Share

Today, we're proud to announce that Elastic Cloud on Kubernetes (ECK) is moving out of beta and into general availability! With ECK, users now have a seamless way of deploying, managing, and operating the Elastic Stack on Kubernetes. Learn more on **our ECK product page**, or **download ECK to get started**.

As we announced with the alpha release of ECK back in May 2019, our vision for ECK is to provide an official way to orchestrate Elasticsearch on Kubernetes and provide a SaaS-like experience for Elastic products on Kubernetes. Kubernetes has continued to grow in popularity and has become the standard for orchestrating container workloads, and we've seen a growing number of users deploying the Elastic Stack on Kubernetes. That's why we've taken a number of steps to support container workloads, such as releasing **official Docker images** for Elasticsearch and Kibana, joining the CNCF, and **launching our Helm charts**. Bringing ECK into general availability is the exciting next step on this journey.

The initial alpha release of ECK built on our years of operational knowledge gained from creating Elasticsearch and Elastic Cloud Enterprise and running our Elasticsearch Service. The community reception to the first alpha release (and the three early access releases that followed) has been extremely positive, and with the general availability of ECK we're excited to give our users a production-ready solution to deploy and

elastic

ECKとは？

https://www.elastic.co/products/elastic-cloud-kubernetes

- Custom Resources Definitions (**CRD**)
  - Elasticsearch, Kibana, APM を追加
  - これらのリソースでKubernetes APIを拡張
- **一連のcontrollers**
  - apiserver上のリソースを監視
  - 関連するリソースのCRUD操作
  - 実行中のESクラスタとの相互運用

→ Basicライセンスで使えます！

```yaml
apiVersion: elasticsearch.k8s.elastic.co/v1alpha1
kind: Elasticsearch
metadata:
  name: elasticsearch-sample
spec:
  version: 7.3.0
  nodes:
  - name: default
    nodeCount: 1
---
apiVersion: kibana.k8s.elastic.co/v1alpha1
kind: Kibana
metadata:
  name: kibana-sample
spec:
  version: 7.3.0
  nodeCount: 1
  elasticsearchRef:
    name: "elasticsearch-sample"
```

2020年2月19日 ニュース EN JP

Microsoft Azure、東京でElasticsearch Serviceの提供を開始

著者 Pieter Humphrey

Share

Elastic CloudのElasticsearch Serviceの提供を、Azure東京（東日本）リージョンで開始いたしました。アジア太平洋で2番目、グローバルで5番目のAzureリージョンとなります。

現在サービスをご利用のお客様は、ログインするだけで、すぐにAzure東京リージョンのElasticsearch Serviceをお使いいただくことができます。サービスをはじめてお使いになる方は、14日間の無料トライアルに登録してお試しいただけます。

パワフルなセキュリティやインデックスライフサイクル管理、機械学習など、Elasticならではのすぐれた機能が揃っています。Kibana Lensで直感的に可視化したり、Canvasでクリエイティブなプレゼンテーションを作成してみましょう。使いやすいスライダーボタンやデプロイテンプレートで、プロビジョニングから設定、デプロイのスケールまで手軽に実施できます。アプリ検索やロギング、メトリック、APM、SIEM、BI/分析など、多彩なソリューションをご用意しています。

Elasticで日本のカントリーマネージャーを務める川崎友和は、以下のように述べています。

「ITのモダナイゼーション、DXが進行する中、オンプレミスや従来型のデータセンターからパブリッククラウドに

elastic

Thank You !