



Amazon OpenSearch Service 機能解説 - モニタリング・オブザーバビリティ編

AWS Black Belt Online Seminar

Takayuki Enomoto

Solutions Architect, Analytics

2023/01

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下の URL より、過去のセミナー含めた資料などをダウンロードできます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- 本資料では 2023 年 01 月時点のサービス内容および価格について説明しています。最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) よりご確認ください
- 資料作成には十分注意しておりますが、資料に記載した情報と AWS 公式ウェブサイトの情報が異なる場合は、AWS 公式ウェブサイトの情報が優先されます
- 価格は税抜の表記です。日本居住のお客様には、別途消費税が請求されます

自己紹介

名前：榎本 貴之 (Enomoto, Takayuki)

所属：アマゾンウェブサービスジャパン
アナリティクス事業本部
ソリューションアーキテクト部
アナリティクスソリューションアーキテクト

経歴：インフラエンジニア @システムインテグレーター
-> インフラエンジニア @ゲーム会社
-> Cloud Support Engineer @AWS
-> **Solution Architect @AWS**

好きなAWSサービス: **Amazon OpenSearch Service**,
Amazon QuickSight, Amazon Neptune,
Amazon Kinesis, AWS Config,
Amazon CloudWatch, **AWS Support**



トピック

1. モニタリング
2. 異常検知
3. オブザーバビリティ

OpenSearch



オープンソースの分散型検索・分析スイート

OpenSearch Project によって開発され、Apache 2.0
ライセンスで提供されている

データストア、検索エンジンの **OpenSearch**、
可視化、UI ツールの **OpenSearch Dashboards** から
構成されている

セキュリティ、パフォーマンス分析、機械学習など
様々なプラグインによる機能拡張が可能



Amazon OpenSearch Service

OpenSearch を簡単にデプロイ・管理、
スケール可能なフルマネージドサービス



フルマネージド: リソースのデプロイ、
管理に費やす時間を削減



セキュリティ: 認証、認可、暗号化、監査、
およびコンプライアンスのための高度な
セキュリティを維持



データ分析・オブザーバビリティ:
潜在的な脅威を体系的に検出し、機械学習、
アラート、可視化を活用して対処

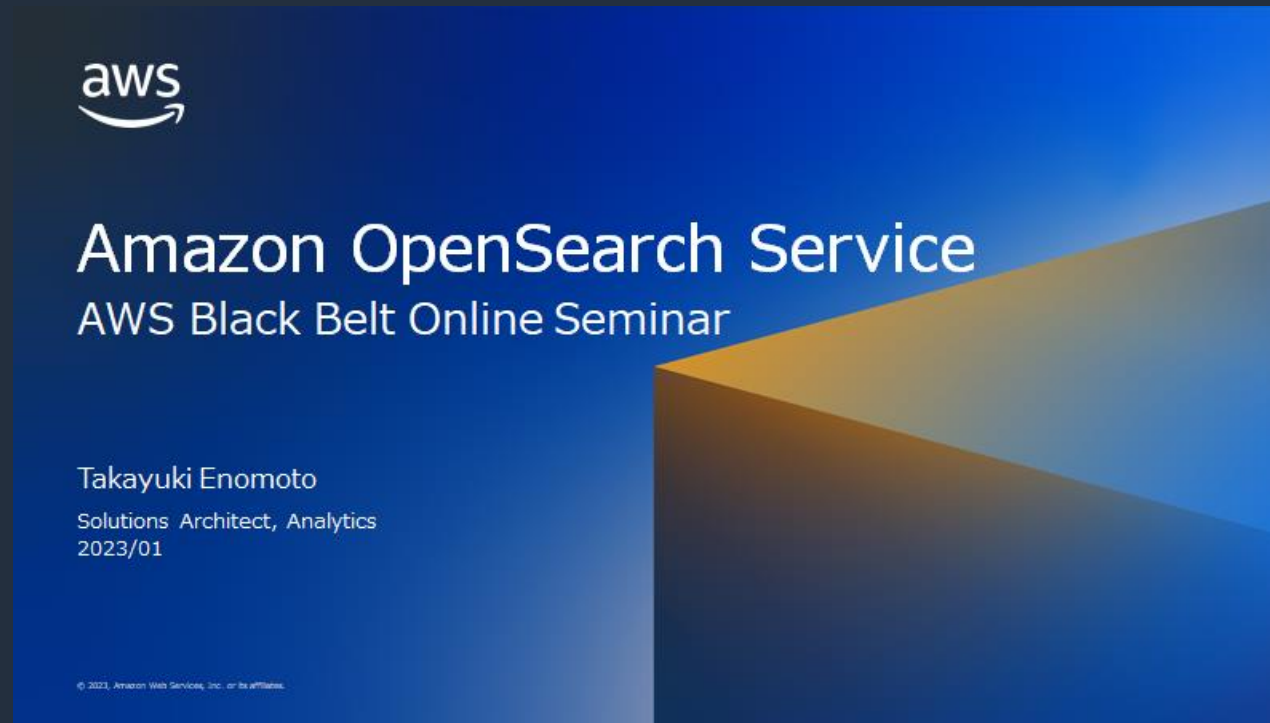


コスト最適化: 各種リソースを最適化し、
戦略的な作業に注力

Amazon OpenSearch Service 概要

サービス概要については

[“AWS Black Belt Online Seminar Amazon OpenSearch Service”](#) を参照のこと



https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2023_Amazon-OpenSearch-Service-Basic_0131_v1.pdf

モニタリング

Alerting

- インデックスに対してクエリを発行し、結果が閾値を超えた場合にトリガを実行する機能
- トリガが実行されると、通知機能と連携し、登録した宛先に対して通知メッセージを送信
- 通知メッセージはカスタマイズが可能
- アラート履歴はダッシュボード、API から取得可能

Data source

Index
opensearch_dashboards_sample_data_logs ×

You can use a * as a wildcard or date math index re: index pattern

Time field
timestamp

Choose the time field you want to use for your x-axis

Query

Metrics - optional ⓘ
COUNT OF documents

+ Add metric
You can add up to 1 metric.

Time range for the last ⓘ
1 minute(s)

Data filter - optional ⓘ
response starts with 5 ×

You have reached the limit of 1 data filter.

Group by - optional ⓘ
No group bys defined.

Triggers (1)

5xx > 100

Trigger name
5xx > 100

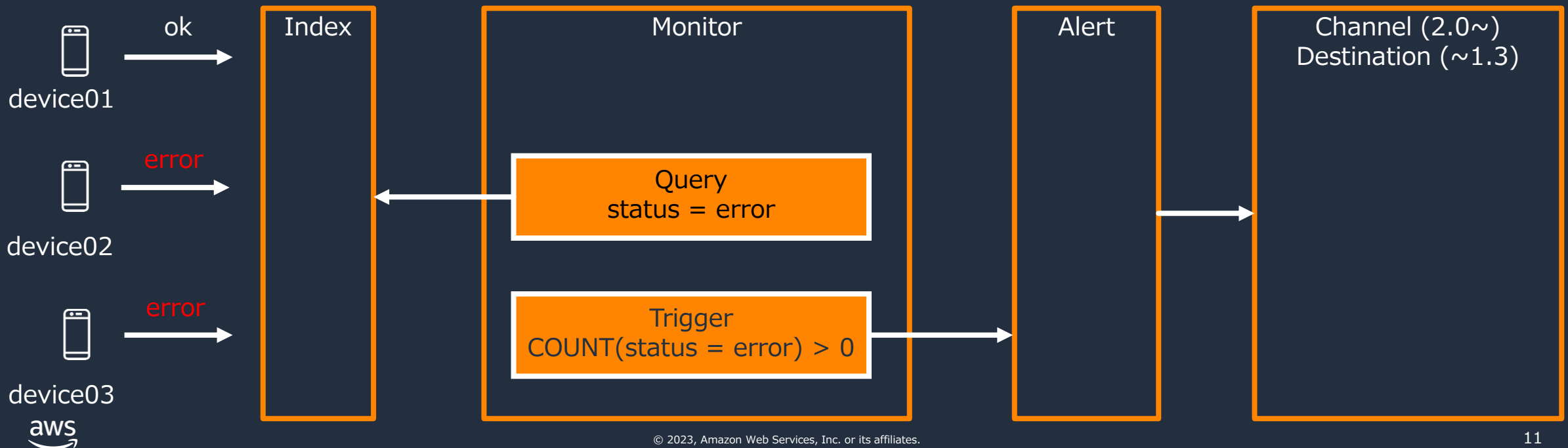
Severity level
2 (High)

Trigger condition
IS ABOVE 100

インデックスパターンやクエリ、閾値を指定

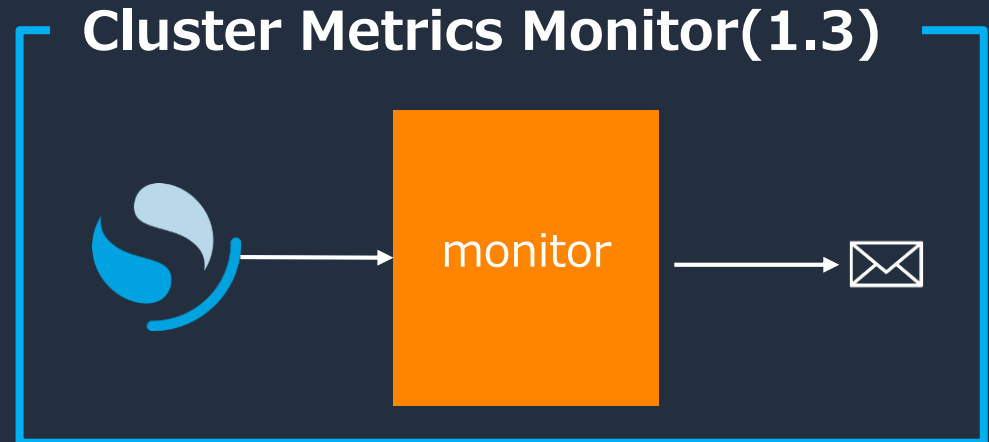
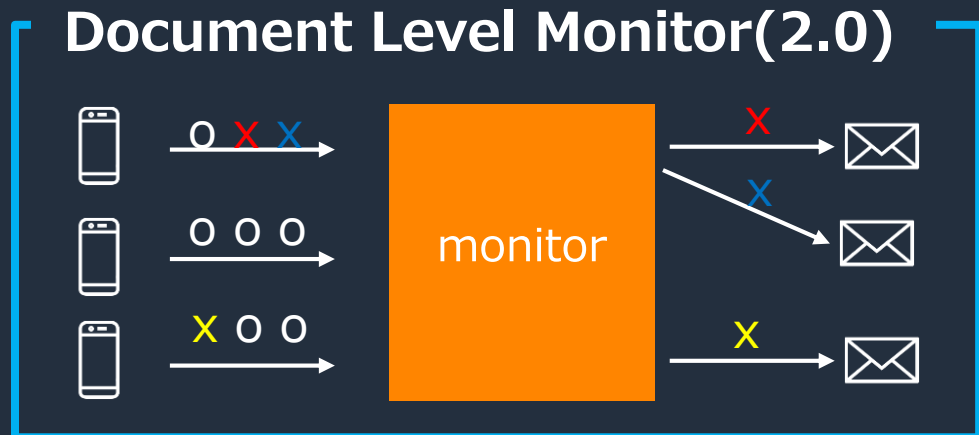
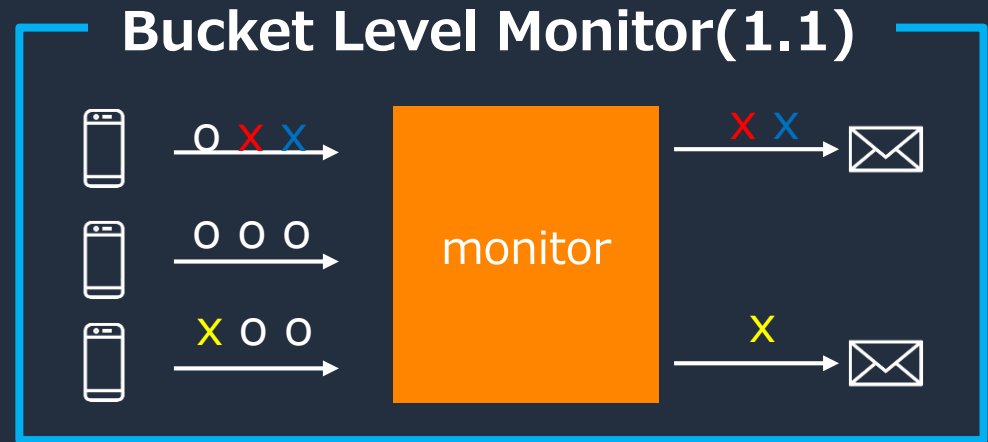
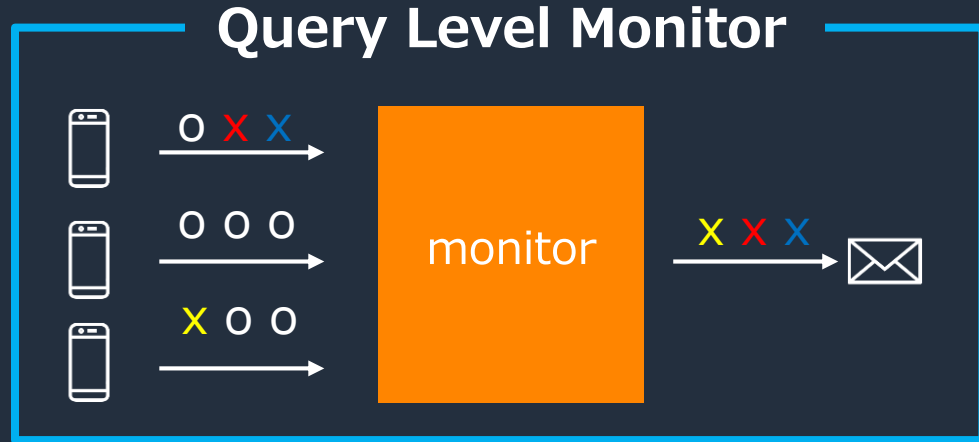
Alerting の全体像

- **モニター:** インデックスに対して定期的に**クエリ**を発行し、閾値を超えた場合に**トリガ**を発動させアラートを生成する
- **アラート:** メッセージテンプレートからアラートメッセージを作成し、チャンネル(1.3 およびそれ以前はデスティネーション)に連携する
- **チャンネル(デスティネーション):** アラートから通知されたメッセージを登録されたリソースに対して送信する

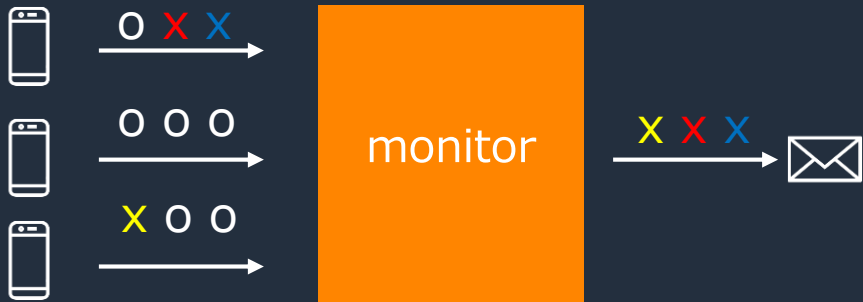


Monitor

用途に応じた 4 種類の Monitor が用意されている



Query Level Monitor



- モニターとアラートは 1:1 対応
- 複数データソースから集めたデータに対して集計を行い、その結果に対して閾値判定を行う場合に用いる

例:

複数 Web サーバーから送信されるアクセスログを集計し、**1 分間の 5xx** エラー件数の**合計**が N 件以上の場合にアラートを通知する。



The screenshot shows the configuration interface for a Query Level Monitor. The title is "Query". Under "Metrics - optional (?)", the metric "COUNT OF documents" is selected and highlighted with an orange box. Below it is a "+ Add metric" button and the text "You can add up to 1 metric." Under "Time range for the last (?)", the value "1" is entered in a text box, and "minute(s)" is selected in a dropdown menu, both highlighted with an orange box. Under "Data filter - optional (?)", the filter "response starts with 5 x" is selected and highlighted with an orange box. Below it is the text "You have reached the limit of 1 data filter." Under "Group by - optional (?)", the text "No group bys defined." is displayed.

Bucket Level Monitor



- モニターとアラートは 1:N 対応
- バケットと呼ばれる集計単位ごとに集計、閾値判定を行う。バケットには任意のフィールドを指定可能
- 複数データソースから集めたデータに対して、ソースごとに個別アラートを通知したいケースで有用

例:

キャンセルされたフライトの件数を航空会社ごとに集計し、1日あたり N 件以上キャンセルが発生している航空会社ごとにアラートを通知する

Query

Metrics - optional ⓘ

COUNT OF documents

+ Add metric

You can add up to 5 more metrics.

Time range for the last ⓘ

1 day(s)

Data filter - optional ⓘ

Cancelled is true ×

You have reached the limit of 1 data filter.

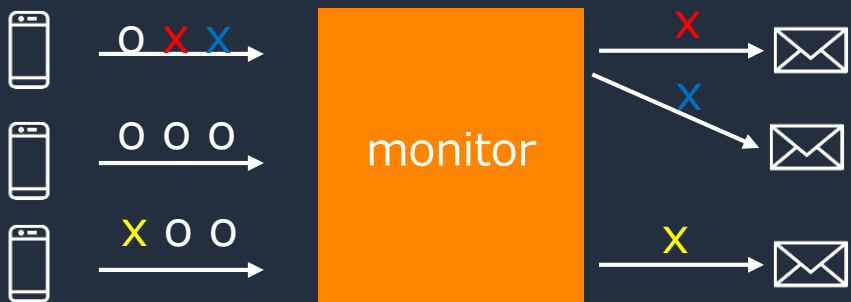
Group by ⓘ

Carrier ×

+ Add group by

You can add up to 1 more group by.

Document Level Monitor



- インデックス内のドキュメントごとに閾値を判定し、ドキュメント単位でアラートを作成する
- セキュリティイベントモニタリングなど、イベントごとに通知を行うようなケースで有効
- アラートごとに **Finding** と呼ばれる情報が作成される

例:

“**score**” が “**high**” のイベント情報が含まれるドキュメントごとに個別に通知を送りたい

Query

Query name

Field

score	is	high
-------	----	------

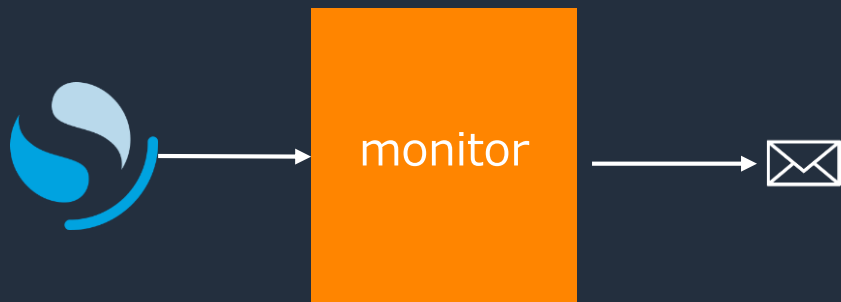
Tags - optional ?

No tags defined.

+ Add tag

You can add up to 10 more tags.

Cluster Metrics Monitor



- モニターとアラートは 1:1 対応
- クラスタやノードの状態を取得する API の実行結果に対して閾値を設定し、超過した場合に通知を行うことが可能

Query

Request type
Specify a request type to monitor and CPU usage. [Learn more](#)

Nodes stats

Preview query

Trigger name

Severity level

1 (Highest) ▼

Trigger condition [Info](#)

```
1 ctx.results[0].nodes.NODE_ID.jvm.mem.heap_used_percent > 60
```

Response

```

1 {
2   "nodes": {
3     "NSWq92yeSR-VeUZVnnTu5w": {
4       "jvm": {
5         "mem": {
6           "heap_committed_in_bytes": 1073741824,
7           "heap_used_percent": 35,
8           "heap_max_in_bytes": 1073741824,
9           "non_heap_committed_in_bytes": 328658944,
10          "pools": {
11            "young": {
12              "used_in_bytes": 221249536,
13              "peak_used_in_bytes": 640679936,
14              "max_in_bytes": 0,
15              "last_gc_stats": {
16                "used_in_bytes": 0,
17                "max_in_bytes": 0,
18                "usage_percent": -1
19              },
20              "peak_max_in_bytes": 0
          }
        }
      }
    }
  }

```


Destination (OpenSearch 1.3 およびそれ以前)

- アラート通知先の管理機能
- OpenSearch 2.0 以降は後述の“Notification” 機能に移管

Add destination

Destination

Name

Specify a name of the destination.

Type

Slack

- Amazon SNS
- Amazon Chime
- Slack
- Custom webhook

Channel (OpenSearch 2.0 以降)

- 外部への通知先を管理するもの。
Alerting 専用ではなく、他の機能からも通知先として参照可能
- Slack、Webhook、Amazon SES、Amazon Chime、Amazon SNS を宛先としてサポート
 - SMTP は Amazon OpenSearch Service では利用不可

Create channel

Name and description

Name

Enter channel name

Description - optional

What is the purpose of this channel?

Configurations

Channel type

Channel type cannot be changed after the channel is created.

Slack

✓ Slack

Chime

Custom webhook

Email

Amazon SNS

Send test message

Create

Email senders / recipient groups

- Eメールの送信元として Amazon SES を登録可能
- 複数の E メールアドレスをグループに登録可能

Configurations

Channel type

Channel type cannot be changed after the channel is created.

Email

SES sender

example

A destination only allows one SMTP or SES sender. Use "Create SES sender" to create a sender with its email address, IAM role, AWS region.

Default recipients

example

Add recipient(s) using an email address or pre-created email group. Use "Create email group" to create an email group.

SES senders (1)

Delete

Edit

Create SES sender

Search

<input type="checkbox"/> Name ↑	Outbound email address	AWS region	Role ARN
<input type="checkbox"/> example	opensearch@example.com	us-east-1	arn:aws:iam::123456789012:role/ExampleRole

Recipient groups (1)

Delete

Edit

Create recipient group

Search

<input type="checkbox"/> Name ↑	Email addresses	Description
<input type="checkbox"/> example	sample01@example.com, sample02@example.com	-

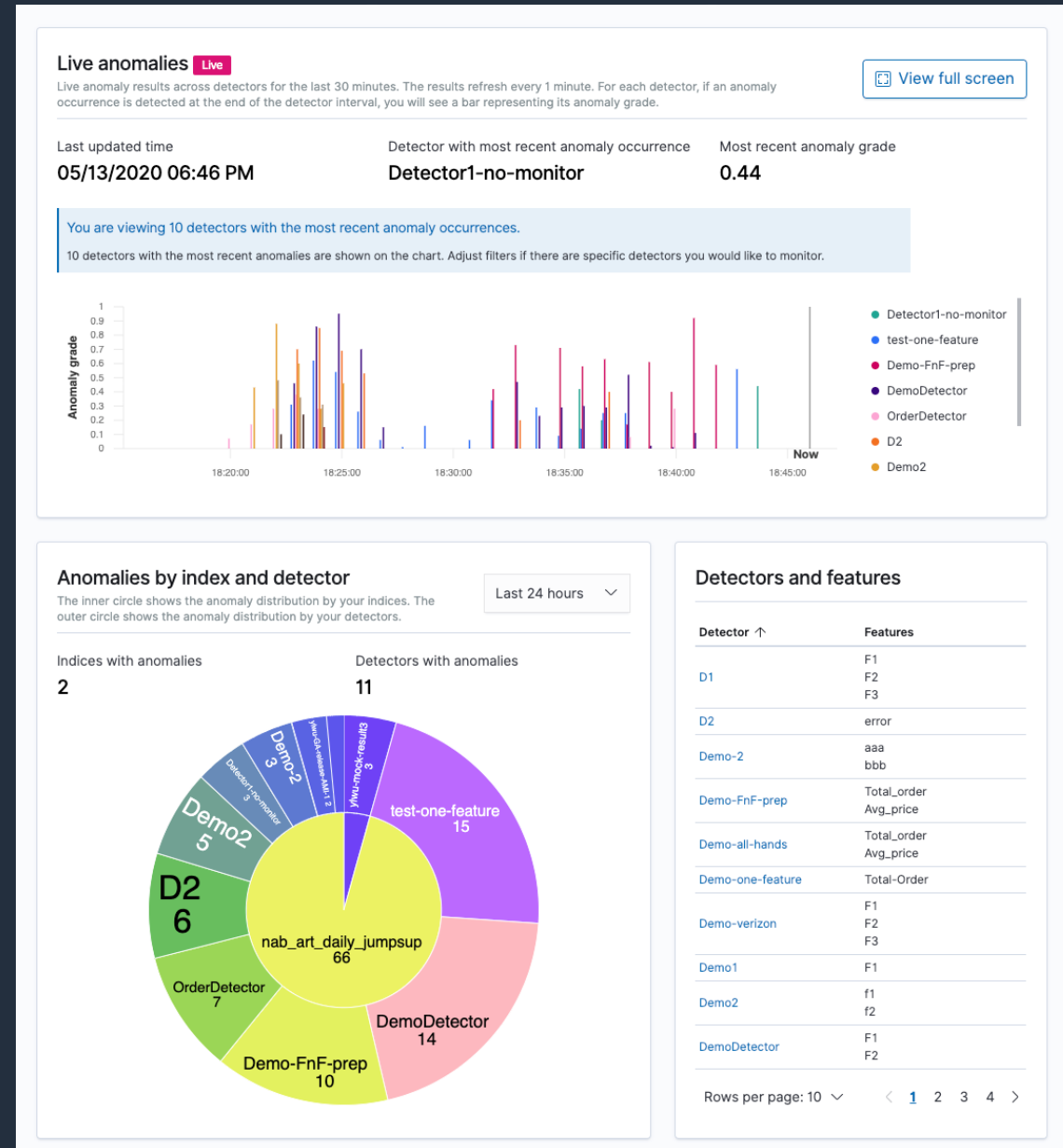
Rows per page: 5

< 1 >

異常検知

Anomaly Detection

- Random Cut Forest アルゴリズムを用いた時系列データの異常検出機能
- 検知した異常は Alerting 機能で通知可能
- リアルタイムデータに対する異常検出、過去の履歴データに対する異常検出の 2 通りの検出をサポート



Detector

- 異常検出機能のメインコンポーネント
- 対象のインデックス、フィールド、フィルタ条件、集計関数または任意のクエリ結果を元に異常値検出を行う

Data Source

Index
Choose an index or index pattern as the data source.

opensearch_dashboards_sample_data_logs

You can use a wildcard (*) in your index pattern.

Data filter- optional
Choose a subset of your data source to focus your data stream and reduce noisy data.

+ Add data filter

Timestamp

Select the time field you want to use for the time filter.

Timestamp field
Choose the time field you want to use for time filter.

timestamp

accesscount

Feature name

accesscount

Enter a descriptive name. The name must be unique within this detector. Feature name must contain 1-64 characters. Valid characters are a-z, A-Z, 0-9, -(hyphen) and _(underscore).

Feature state

Enable feature

Find anomalies based on

Field value

Aggregation method

count()

The aggregation method determines what constitutes an anomaly. For example, if you choose min(), the detector focuses on finding anomalies based on the minimum values of your feature.

Field

timestamp

accesscount

Feature name

accesscount

Enter a descriptive name. The name must be unique within this detector. Feature name must contain 1-64 characters. Valid characters are a-z, A-Z, 0-9, -(hyphen) and _(underscore).

Feature state

Enable feature

Find anomalies based on

Custom expression

Expression

```
{
  "accesscount": {
    "value_count": {
      "field": "timestamp"
    }
  }
}
```

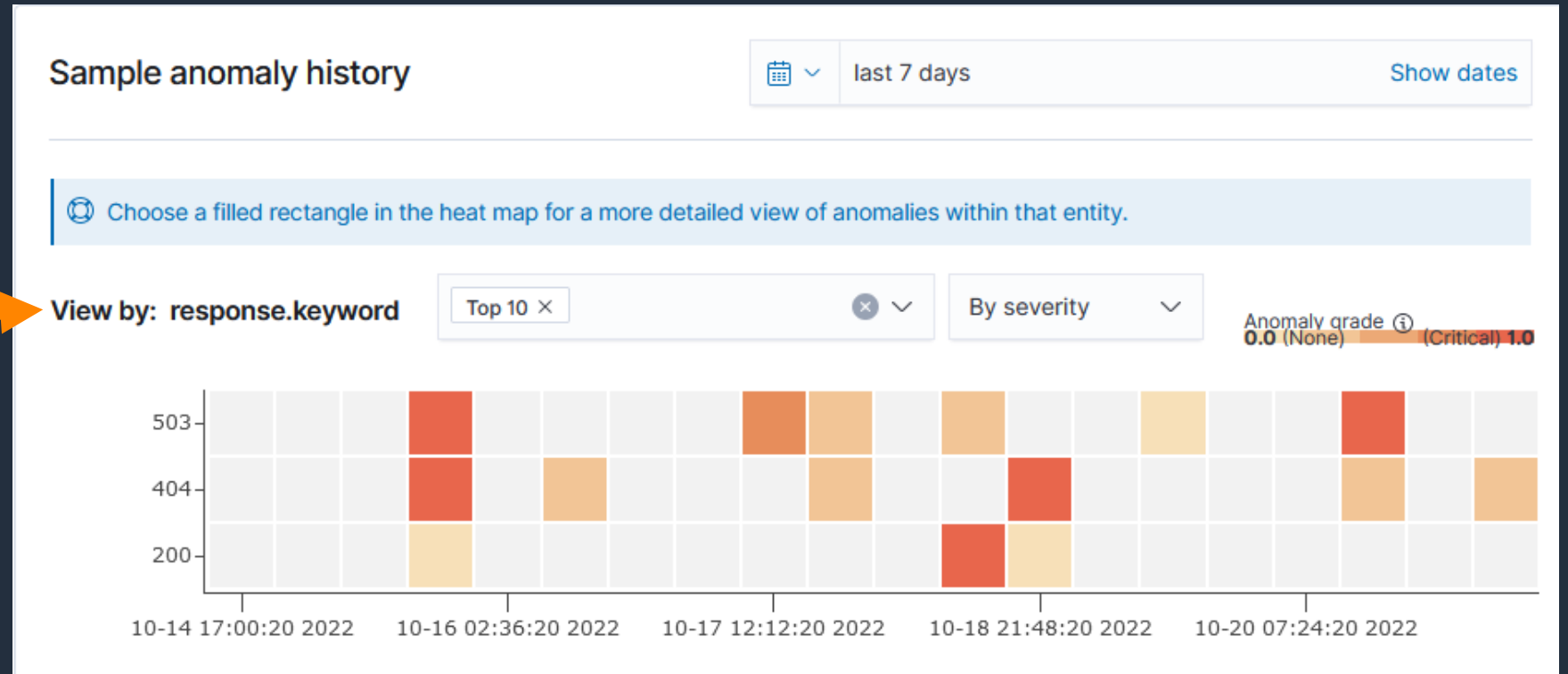
Detector > Categorical fields

- Categorical fieldsを使用すると、指定したフィールドごとにデータをバケット分割し、バケット内で個別に異常値判定を行うことが可能。
- 特定エラーコードの急増を検出したい、といったケースで有用

Field

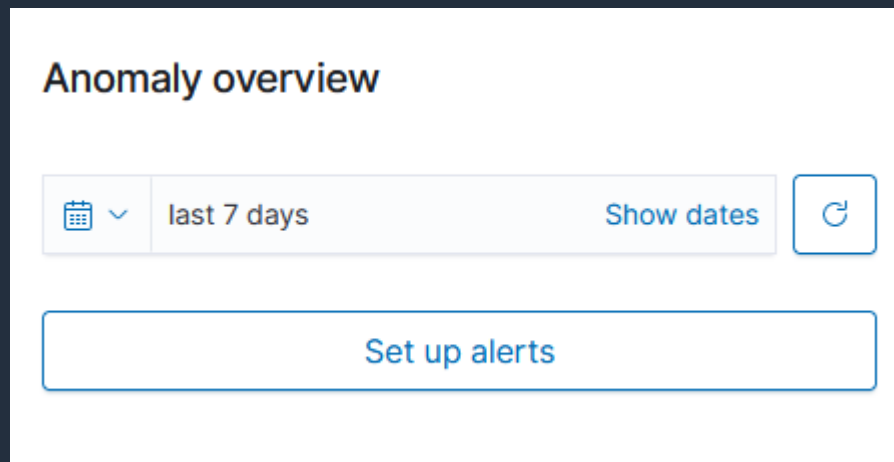
response.keyword ×

You can only apply the categorical OpenSearch data types.



Anomaly Detection と Alerting の連携

- Alerting と連携することで検出結果を通知することが可能
- Detector から Monitor を作成する機能もコンソール上で提供
- 現状は Query Level Monitor との連携のみ可能



The screenshot shows the 'Monitor configuration' page. It includes the following sections:

- Monitor name:** A text input field containing 'sample-ecommerce-detector-Monitor'.
- Monitor type:** Four radio button options:
 - Per query monitor**: Per query monitors run a specified query and define triggers that check the results of that query.
 - Per bucket monitor**: Per bucket monitors allow you to group results into buckets and define triggers that check each bucket.
 - Per cluster metrics monitor**: Per cluster metrics monitors allow you to alert based on responses to common REST APIs.
 - Per document monitor**: Per document monitors allow you to run queries on new documents as they're indexed.
- Monitor defining method:** A section with the instruction 'Specify the way you want to define your query and triggers. [Learn more](#)'. It contains three radio button options:
 - Visual editor**
 - Extraction query editor**
 - Anomaly detector**
- Detector:** A dropdown menu showing 'sample-ecommerce-detector'.

Anomaly Detection と Alerting の連携 > 閾値

- トリガの閾値判定には、Detector から連携された grade and confidence スコア、もしくは Anomaly Detection の実行結果の詳細情報を利用可能

▼ New trigger

Trigger name

Severity level

1 (Highest) ▼

Trigger type

Define type of anomaly detector trigger

Anomaly detector grade and confidence ▼

Anomaly grade threshold

IS ABOVE ▼ 0.7

Trigger type

Define type of anomaly detector trigger

Extraction query response ▼

Response

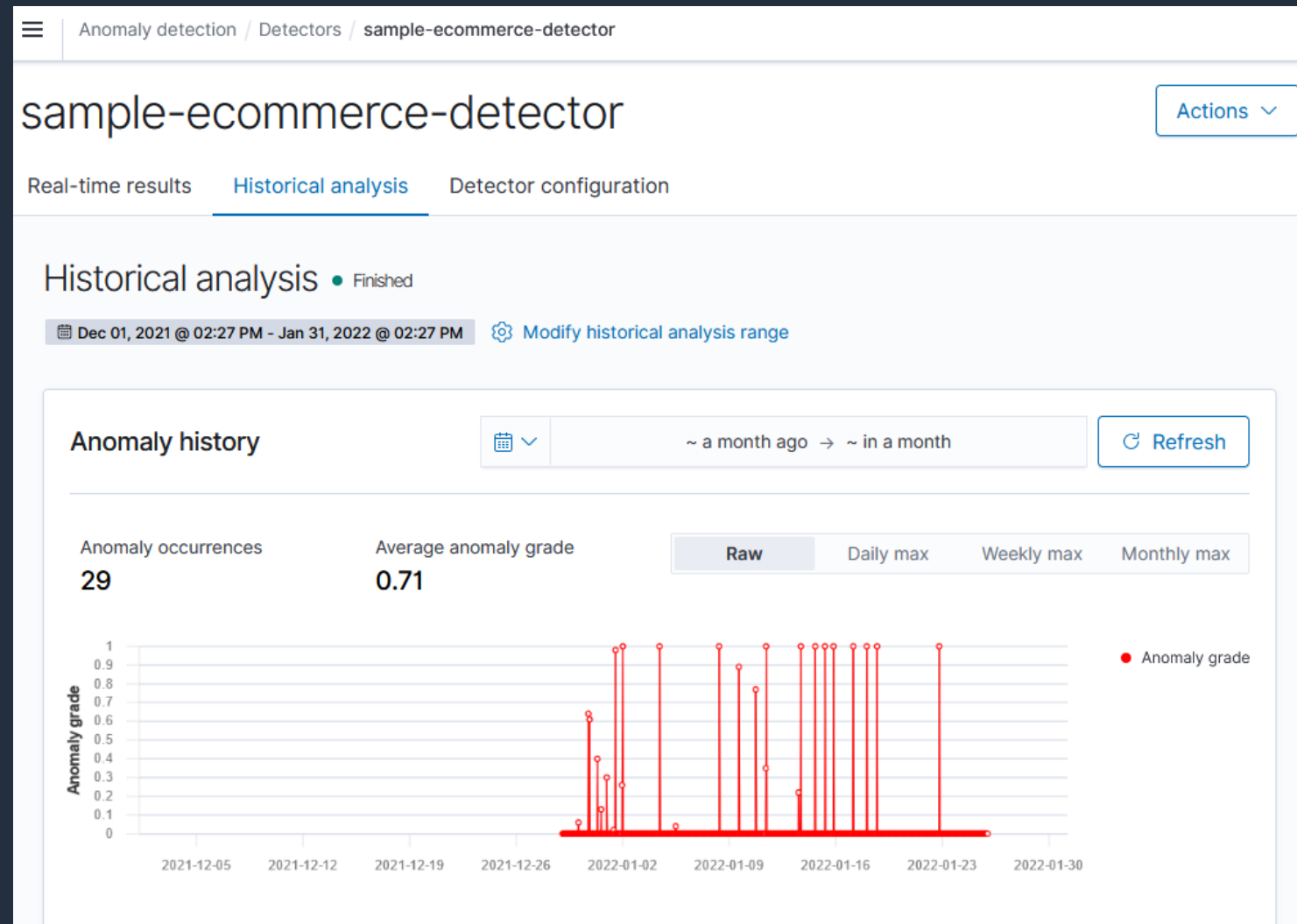
```
7     },
8     "hits": {
9     "hits": [
10    {
11      "_index": ".opendistro-anomaly-results-history-2022.10.18-1",
12      "_source": {
13        "detector_id": "eTxu-YMB3uqSc3CTMFVY",
14        "schema_version": 5,
15        "anomaly_score": 0.454583669387515,
16        "execution_start_time": 1666339705010,
17        "data_end_time": 1666339645010,
18        "confidence": 0.9383715568510591,
19        "data_start_time": 1666339045010,
20        "feature_data": [
```

Trigger condition [Info](#)

```
1 ctx.results[0].hits.total.value > 0
```

Historical analysis

- 数週間、数か月分のデータに対する分析も可能
- リアルタイムデータに対する異常検知とは異なり、アドホックに実行する
- リアルタイムデータに対する異常検知と組み合わせることで、root cause の分析やトレンド分析、モデルのチューニングに活用



Observability

**“Everything fails,
all the time.”**

—Dr. Werner Vogels, Amazon CTO

システムダウンタイムに伴うコスト



1時間あたり\$42,000
ダウンタイム1時間あたりの平均コスト



年間 87 時間
年間のダウンタイム時間

*Gartner

IT 部門の作業を阻害
機会損失、ビジネスに
直結しないコスト

SLA 違反による
ペナルティ
ブランド力低下

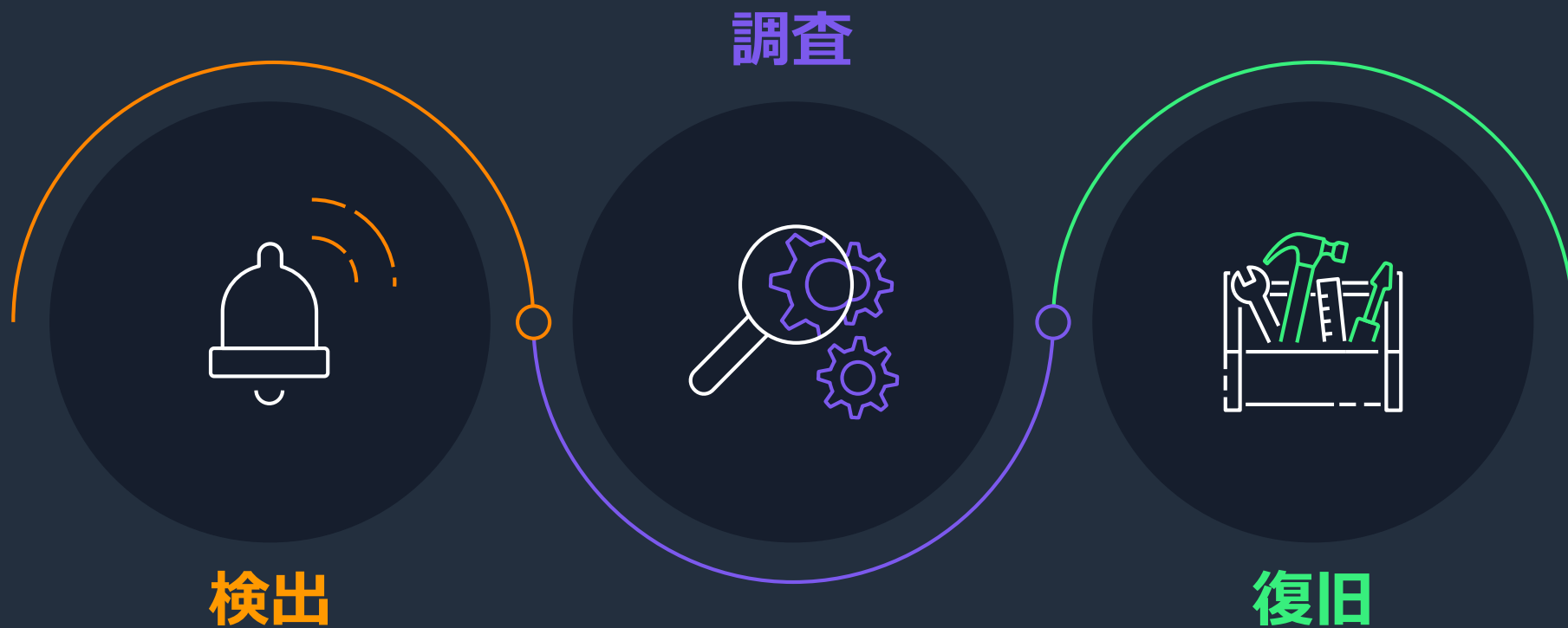
トラブルシューティングは藪の中から針を探すかのごとし

```
199.72.81.55 -- [01/Jul/1995:00:00:01 -0400] "GET /history/apollo/ HTTP/1.0" 200 6245
unicomp6.unicomp.net -- [01/Jul/1995:00:00:06 -0400] "GET /shuttle/countdown/ HTTP/1.0" 200 3985
199.120.110.21 -- [01/Jul/1995:00:00:09 -0400] "GET /shuttle/missions/sts-73/mission-sts-73.html HTTP/1.0" 200 4085
burger.letters.com -- [01/Jul/1995:00:00:11 -0400] "GET /shuttle/countdown/liftoff.html HTTP/1.0" 304 0
199.120.110.21 -- [01/Jul/1995:00:00:11 -0400] "GET /shuttle/missions/sts-73/sts-73-patch-small.gif HTTP/1.0" 200 4179
burger.letters.com -- [01/Jul/1995:00:00:12 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304 0
burger.letters.com -- [01/Jul/1995:00:00:12 -0400] "GET /shuttle/countdown/video/livevideo.gif HTTP/1.0" 200 0
205.212.115.106 -- [01/Jul/1995:00:00:12 -0400] "GET /shuttle/countdown/countdown.html HTTP/1.0" 200 3985
d104.aa.net -- [01/Jul/1995:00:00:13 -0400] "GET /shuttle/countdown/ HTTP/1.0" 200 3985
129.94.144.152 -- [01/Jul/1995:00:00:13 -0400] "GET / HTTP/1.0" 200 7074
unicomp6.unicomp.net -- [01/Jul/1995:00:00:14 -0400] "GET /shuttle/countdown/count.gif HTTP/1.0" 200 40310
unicomp6.unicomp.net -- [01/Jul/1995:00:00:14 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 200 786
unicomp6.unicomp.net -- [01/Jul/1995:00:00:14 -0400] "GET /images/KSC-logosmall.gif HTTP/1.0" 200 1204
d104.aa.net -- [01/Jul/1995:00:00:15 -0400] "GET /shuttle/countdown/count.gif HTTP/1.0" 200 40310
d104.aa.net -- [01/Jul/1995:00:00:15 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 200 786
d104.aa.net -- [01/Jul/1995:00:00:15 -0400] "GET /images/KSC-logosmall.gif HTTP/1.0" 200 1204
129.94.144.152 -- [01/Jul/1995:00:00:17 -0400] "GET /images/ksclogo-medium.gif HTTP/1.0" 304 0
199.120.110.21 -- [01/Jul/1995:00:00:17 -0400] "GET /images/launch-logo.gif HTTP/1.0" 200 1713
ppptky391.asahi-net.or.jp -- [01/Jul/1995:00:00:18 -0400] "GET /facts/about_ksc.html HTTP/1.0" 200 3977
net-1-141.eden.com -- [01/Jul/1995:00:00:19 -0400] "GET /shuttle/missions/sts-71/images/KSC-95EC-0916.jpg HTTP/1.0" 200 34029
ppptky391.asahi-net.or.jp -- [01/Jul/1995:00:00:19 -0400] "GET /images/launchpalms-small.gif HTTP/1.0" 200 11473
205.189.154.54 -- [01/Jul/1995:00:00:24 -0400] "GET /shuttle/countdown/ HTTP/1.0" 200 3985
waters-gw.starway.net.au -- [01/Jul/1995:00:00:25 -0400] "GET /shuttle/missions/51-l/mission-51-l.html HTTP/1.0" 200 6723
ppp-mia-30.shadow.net -- [01/Jul/1995:00:00:27 -0400] "GET / HTTP/1.0" 200 7074
205.189.154.54 -- [01/Jul/1995:00:00:29 -0400] "GET /shuttle/countdown/count.gif HTTP/1.0" 200 40310
alyssa.prodigy.com -- [01/Jul/1995:00:00:33 -0400] "GET /shuttle/missions/sts-71/sts-71-patch-small.gif HTTP/1.0" 200 12054
ppp-mia-30.shadow.net -- [01/Jul/1995:00:00:35 -0400] "GET /images/ksclogo-medium.gif HTTP/1.0" 200 5866
dial22.lloyd.com -- [01/Jul/1995:00:00:37 -0400] "GET /shuttle/missions/sts-71/images/KSC-95EC-0613.jpg HTTP/1.0" 200 61716
smyth-pc.moorecap.com -- [01/Jul/1995:00:00:38 -0400] "GET /history/apollo/apollo-13/images/70HC314.GIF HTTP/1.0" 200 101267
205.189.154.54 -- [01/Jul/1995:00:00:40 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 200 786
ix-orl2-01.ix.netcom.com -- [01/Jul/1995:00:00:41 -0400] "GET /shuttle/countdown/ HTTP/1.0" 200 3985
```



オブザーバビリティ

「問題を検出し、事象を調査し、対応策を実施して復旧する」
障害対応の一連のプロセスを素早く実行するための観測能力



OpenSearch の Observability 機能

統合的なアプリケーション分析機能を提供。

Trace Analytics: アプリケーショントレース分析

Event Analytics: ログ分析

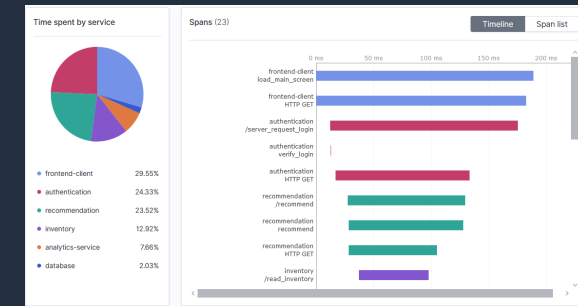
Operational Panels: 可視化ダッシュボード

Application Analytics: 統合ビュー

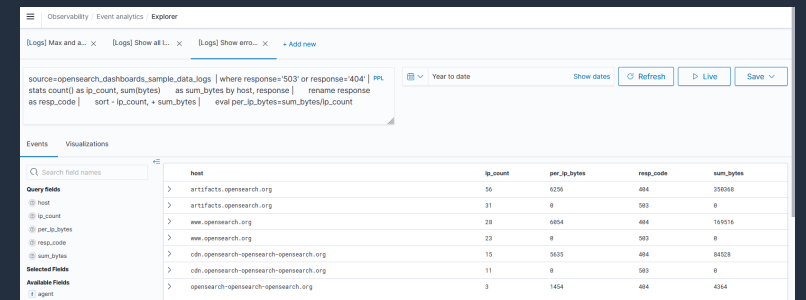
Notebook: レポートや手順書などの書類作成

Application Analytics (1.3)

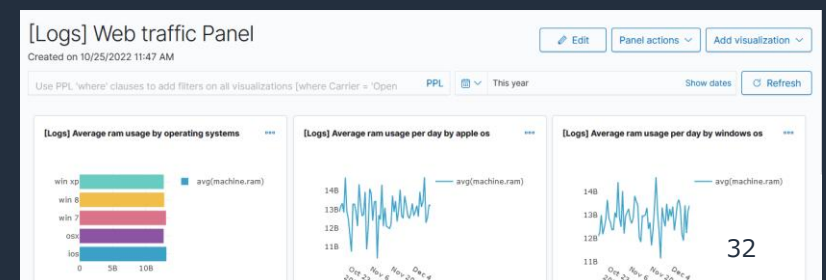
Trace Analytics



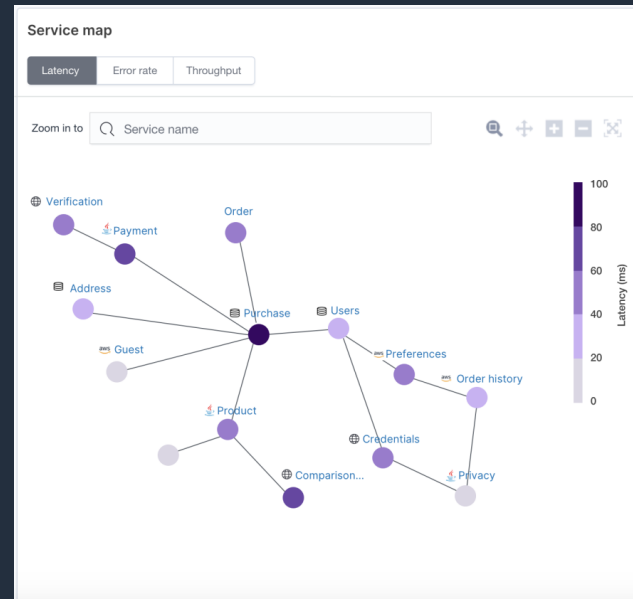
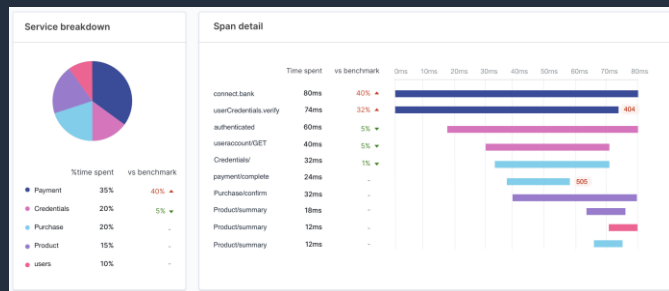
Event Analytics (1.2)



Operational Panels (1.2)



Observability > Trace Analytics



Trace group name	Latency variance	Average latency (ms)	Average latency vs benchmark	24-hour latency trend	Error rate	Traces
MakePayment.auto	45	30% ↑	20%	1,500		
Order.confirmation	48	5% ↓	1%	2,000		
MakePayment.oneoff	42	30% ↑	2%	1,200		
Product.comparison	40	5% ↓	3%	1,000		
Purchase.buynow	60	30% ↑	3%	800		
MakePayment.auto	46	30% ↑	2%	900		
Order.confirmation	64	15% ↓	0%	200		
MakePayment.oneoff...	65	30% ↑	10%	400		
Product.comparison...	43	10% ↓	10%	100		
Purchase.buynow...	28	10% ↓	10%	1,100		

Trace-Span details

- 単一リクエストのパフォーマンス
- 原因の診断

Services

- End-to-end の可視化
- マイクロサービス間での原因切り分け

Trace Groups

- パフォーマンスモニタリング
- 問題の早期特定

Observability > Trace Analytics > Trace group

Latency by trace group □ < 95th percentile ■ >= 95th percentile Benchmark This time last week

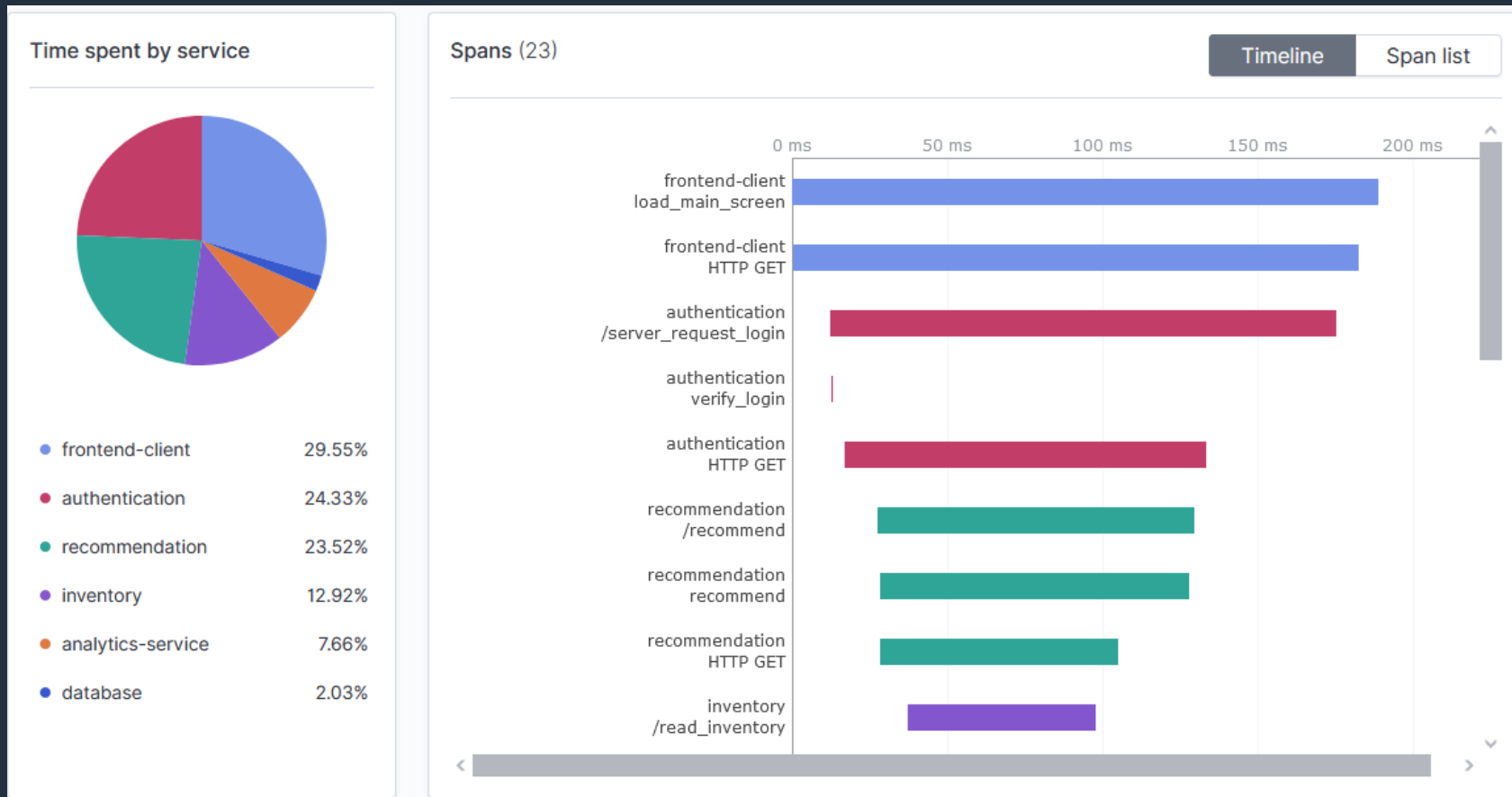
Trace group name	Latency variance ↓	Average latency (ms)	Average latency vs benchmark	24-hour latency trend	Error rate	Traces
MakePayment.auto		45	30% ▲		20%	1,500
Order.confirmation		48	5% ▼		1%	2,000
MakePayment.oneoff		42	30% ▲		2%	1,200
Product.comparision		40	5% ▼		3%	1,000
Purchase.buynow		60	30% ▲		3%	800
MakePayment.auto		46	30% ▲		2%	900
Order.confirmation		64	15% ▼		0%	200
MakePayment.oneoff...		65	30% ▲		10%	400
Product.comparision...		43	10% ▼		10%	100
Purchase.buynow...		28	10% ▼		10%	1,100

Rows per page: 10 >

- 類似したトレースを
トレースグループに集約
- サービスとオペレーション名に
基づき、トレースグループごとの
パフォーマンスとエラーレートを
測定
 - ログイントレース、
チェックアウトトレースなど
- P90/P95 レイテンシー、
エラーレート傾向等、
統計分析を用いて異常を検知

Observability > Trace Analytics > Trace span details

- マイクロサービスにおける単一のリクエストの詳細(レイテンシ、エラー)を分析



Observability > Trace Analytics > Trace span details

- Span の詳細を GUI または JSON 形式で確認可能

Span detail	
@hostname	659cfb-cjcz6
resource.attributes.service@instance@id	140477540492672
resource.attributes.service@name	database
resource.attributes telemetry@sdk@language	python
resource.attributes telemetry@sdk@name	opentelemetry
resource.attributes telemetry@sdk@version	1.9.1
span.attributes.db@name	APM
span.attributes.db@statement	SELECT * FROM Inventory_Items
span.attributes.db@system	mysql
span.attributes.db@user	root
span.attributes.net@peer@name	mysql.mysql.svc.cluster.local
span.attributes.net@peer@port	3306

```
Payload

[
  {
    "_index": "otel-v1-apm-span-000001",
    "_type": "_doc",
    "_id": "acabd443c66f3481",
    "_score": 2.330756,
    "_source": {
      "traceId": "1544956b6e14d1f5bf96f0a4dc75a1d6",
      "droppedLinksCount": 0,
      "kind": "SPAN_KIND_CLIENT",
      "droppedEventsCount": 0,
      "traceGroupFields": {
        "endTime": "2022-10-24T23:59:51.097254103Z",
        "durationInNanos": 188780628,
        "statusCode": 0
      },
      "traceGroup": "load_main_screen",
      "serviceName": "database",
      "parentSpanId": "e7d85af8819a1b99",
      "spanId": "acabd443c66f3481",
      "traceState": ""
    }
  }
]
```

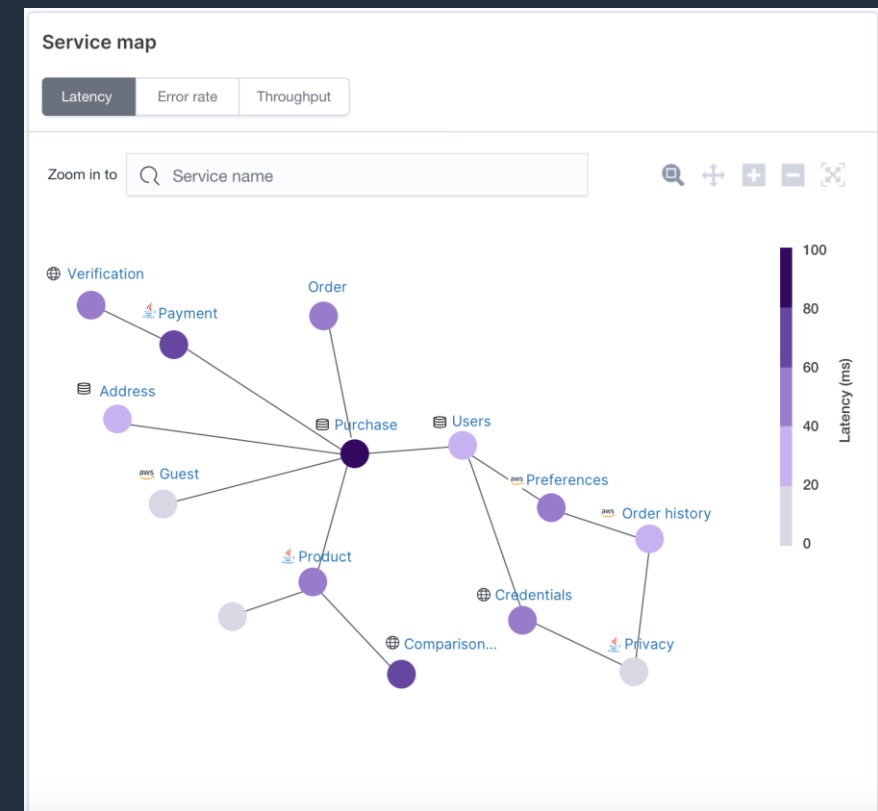
Observability > Trace Analytics > Services

- 全分散トレースを集約
- トレースデータから抽出したレイテンシ、エラー、スループットから、サービスホットスポットを特定
- Service map による アプリケーション環境の end-to-end の可視化を提供

Services (8)						
Name ↑	Average latency (ms)	Error rate	Throughput	No. of connected services	Connected services	Traces
analytics-service	44.07	0%	17	5	authentication, inventory, order, payment, reco...	11
authentication	432.45	0%	3	3	analytics-service, frontend-client, recommendation	3
database	17.62	5.88%	17	2	inventory, order	13
frontend-client	199.57	18.18%	11	3	authentication, order, payment	11
inventory	340.32	0%	3	3	analytics-service, database, recommendation	3
order	87.26	0%	6	3	analytics-service, database, frontend-client	6
payment	42.34	100%	2	2	analytics-service, frontend-client	2
recommendation	387.83	0%	3	3	analytics-service, authentication, inventory	3

Rows per page: 10 ▾

< 1 >



Observability > Event Analytics

- **Piped Processing Language (PPL)** ベースのログ検索機能。データ加工も可能
- Live Tail 機能によるログのリアルタイム更新表示に対応

Observability / Event analytics / Explorer

[Logs] Max and a... × [Logs] Show all l... × [Logs] Show erro... × + Add new

```
source=opensearch_dashboards_sample_data_logs | where response='503' or response='404' | PPL
stats count() as ip_count, sum(bytes) as sum_bytes by host, response | rename response
as resp_code | sort - ip_count, + sum_bytes | eval per_ip_bytes=sum_bytes/ip_count
```

Year to date Show dates Refresh Live Save

Events Visualizations

Search field names

Query fields

- host
- ip_count
- per_ip_bytes
- resp_code
- sum_bytes

Selected Fields

Available Fields

- agent

host	ip_count	per_ip_bytes	resp_code	sum_bytes
> artifacts.opensearch.org	56	6256	404	350368
> artifacts.opensearch.org	31	0	503	0
> www.opensearch.org	28	6054	404	169516
> www.opensearch.org	23	0	503	0
> cdn.opensearch-opensearch-opensearch.org	15	5635	404	84528
> cdn.opensearch-opensearch-opensearch.org	11	0	503	0
> opensearch-opensearch-opensearch.org	3	1454	404	4364

PPL (Piped Processing Language)

- PPL とは、パイプ | でコマンドを繋いで処理を記述する言語
- 検索だけでなく、フィールドの値をパースし複数のフィールドに分割するなど複雑な操作も可能

```
search source=accounts | eval doubleAge = age * 2 | fields age, doubleAge;
```

age	doubleAge
32	64
36	72
28	56
33	66

```
os> source=accounts | parse email '.*@(<host>.*)' | fields email, host ;  
fetched rows / total rows = 4/4
```

email	host
amberduke@pyrami.com	pyrami.com
hattiebond@netagy.com	netagy.com
null	null
daleadams@boink.com	boink.com



PPL による高度な処理

ML Commons Plugin により、PPL でランダムカットフォレストや k-means によるデータ処理も可能となっている

ad command (RCF)

```
os> source=nyc_taxi | fields value,  
timestamp | AD time_field='timestamp' |  
where value=10844.0
```

value	timestamp	score	anomaly_grade
10844.0	1404172800000	0.0	0.0

kmeans command (k-means)

```
os> source=iris_data | fields  
sepal_length_in_cm, sepal_width_in_cm,  
petal_length_in_cm, petal_width_in_cm |  
kmeans 3
```

sepal_length_in_cm	sepal_width_in_cm	petal_length_in_cm	petal_width_in_cm	ClusterID
5.1	3.5	1.4	0.2	1
5.6	3.0	4.1	1.3	0
6.7	2.5	5.8	1.8	2

ML Commons Plugin

- OpenSearch 上で機械学習モデルのトレーニングと推論を行う機能
- 以下のアルゴリズムをサポート
 - K-means (1.3 以降)
 - Linear regression (1.3 以降)
 - Random Cut Forrest (1.3 以降)
 - Random Cut Forrest Summarize (2.2 以降)
 - Localization (1.3 以降)
 - Logistic regression (2.2 以降)
- OpenSearch 上で動作する機械学習を使用した機能のベースとして使われている

```
POST /_plugins/_ml/_train/kmeans
{
  "parameters": {
    "centroids": 3,
    "iterations": 10,
    "distance_type": "COSINE"
  },
  "input_query": {
    "_source": ["petal_length_in_cm", "petal_width_in_cm"],
    "size": 10000
  },
  "input_index": [
    "iris_data"
  ]
}
```

```
POST /_plugins/_ml/_predict/kmeans/<model-id>
{
  "input_query": {
    "_source": ["petal_length_in_cm", "petal_width_in_cm"],
    "size": 10000
  },
  "input_index": [
    "iris_data"
  ]
}
```

Observability > Event Analytics > Visual

- Event Analytics で検索したログからグラフを作成する機能
- 作成したグラフは **Operational Analytics Panel** ダッシュボードに追加可能

The screenshot displays the OpenSearch Event Analytics interface. At the top, there are several tabs for different log views. The main query area contains the following query: `source = opensearch_dashboards_sample_data_logs | where geo.src='US' | where geo.dest='JP' or geo.dest='CN' or geo.dest='IN' | stats count() by geo.dest`. The visualization is a bar chart showing the count of requests by destination. The y-axis represents the count, ranging from 0 to 30. The x-axis represents the destination. The bars are colored blue and purple. A legend on the right indicates that the blue bar represents 'count()'. A modal window titled 'Custom operational dashboards/application' is open, showing a dropdown menu with the following options: '[Logs] Web traffic Panel', 'sample', and '[Logs] Count requests from US to CN, IN :'. The modal also has a 'Name for your savings' field and 'Cancel' and 'Save' buttons.

geo.dest	count()
JP	31
CN	28

Observability > Operational Panels

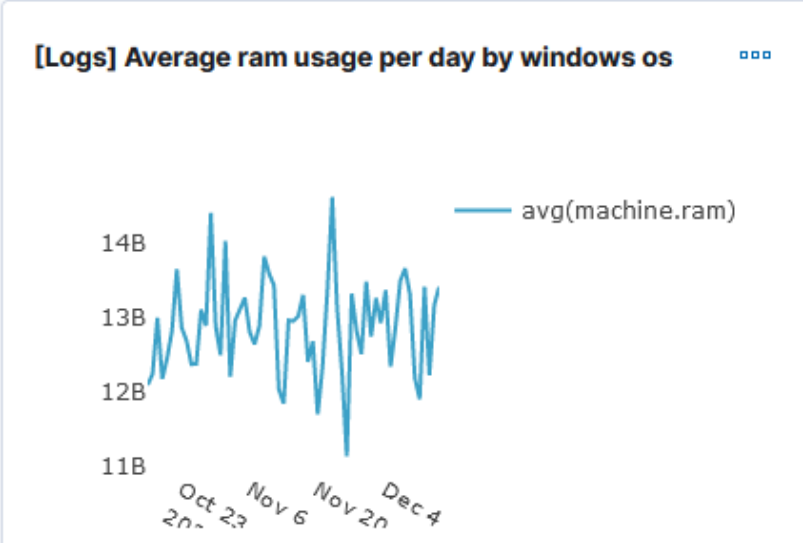
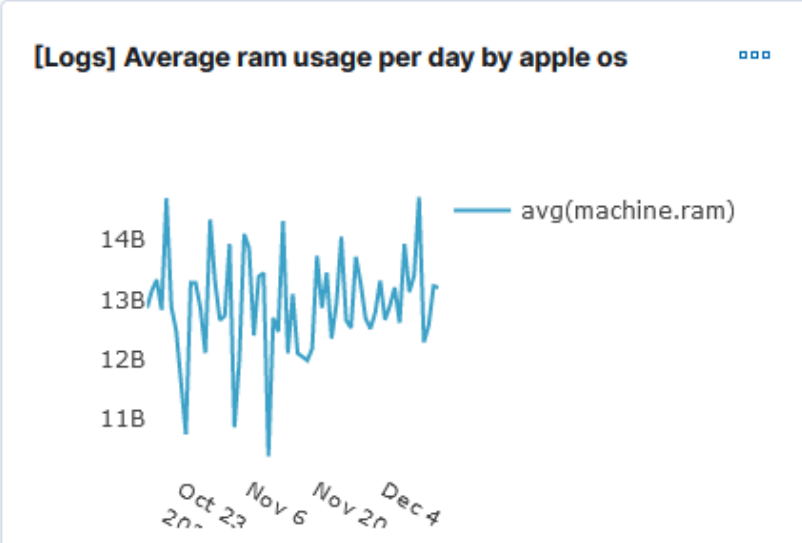
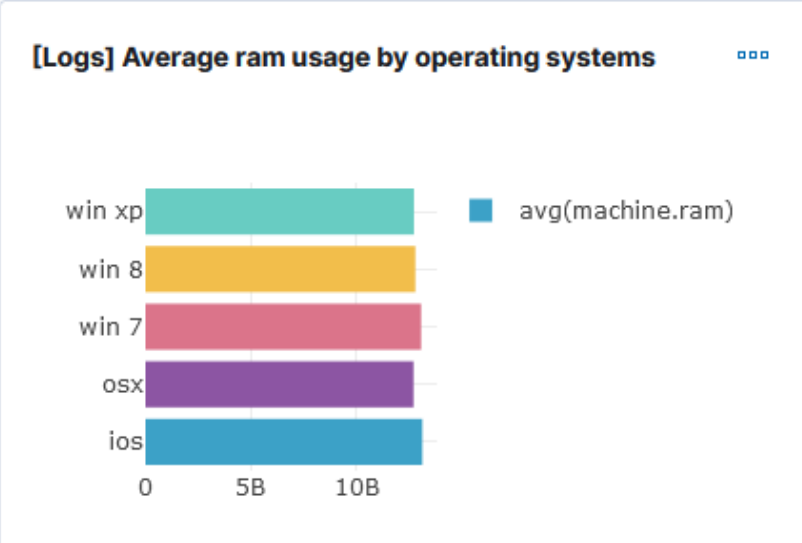
- Observability におけるダッシュボード機能
- Event Analytics で作成したビジュアルを配置可能

[Logs] Web traffic Panel

Created on 10/25/2022 11:47 AM

Edit
Panel actions
Add visualization

Use PPL 'where' clauses to add filters on all visualizations [where Carrier = 'Open
 PPL
▼
This year
Show dates
Refresh



Observability > Application Analytics

- Trace Analytics、Event Analytics、Operational Panels が統合されたアプリケーション分析環境。ログとトレースの横断分析、可視化を一つの画面で行う

Observability / Application analytics / Sample Application

Sample Application

Sample application for observability workshop

Overview Services Traces & Spans Log Events Panel Configuration

Trace ID, trace group name, service name Last 24 hours Show dates Refresh

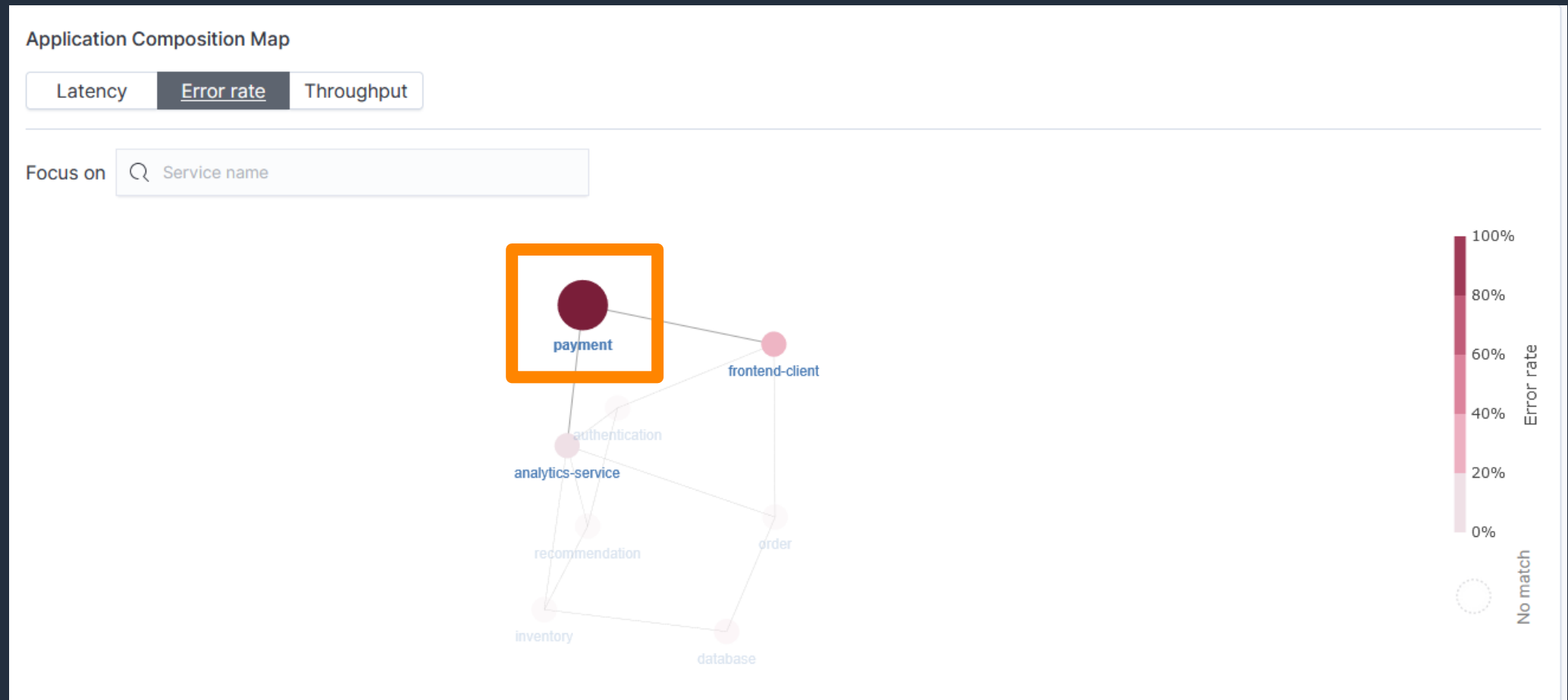
+ Add filter

Latency by trace group (7) < 95 percentile >= 95 percentile

Trace group name	Latency variance (ms)	Average latency (ms)	24-hour latency trend	Error rate	Traces
load_main_screen		465.91		0%	3
client_checkout		65.14		100%	2
client_create_order		163.29		0%	2
client_pay_order		89.56		0%	2
CREATE		15.14		0%	3
client_delivery_status		80.76		0%	2
USE		2.05		100%	1

Observability > Application Analytics > 分析の流れ

サービスマップからエラーレートの高いマイクロサービスを選択



Observability > Application Analytics > 分析の流れ

選択されたサービス内で、エラーとなっているトレースの ID をコピー

Sample Application

Sample application for observability workshop

Overview Services **Traces & Spans** Log Events Panel Configuration

Trace ID, trace group name, service name 📅 Last 24 hours Show dates Refresh

serviceName: payment × + Add filter

Traces (2)

Trace ID ↑	Trace group	Latency (ms)	Percentile in trace group	Errors	Last updated
246885d9210cf17f85dc9...	client_checkout	83.14	75th	Yes	10/24/2022 17:40:08
267b711a99c593d986120...	client_checkout	47.14	0th	Yes	10/25/2022 09:05:27

Rows per page: 10 ▾ < 1 >

Observability > Application Analytics > 分析の流れ

Log Events タブに移動し、トレース ID でログを検索、閲覧

The screenshot displays the AWS Observability console interface for 'Sample Application'. The 'Log Events' tab is selected. The 'Base Query' field contains the query `where traceId = '246885d9210cf17f85dc9fb18b5131b9'`, which is highlighted with an orange box. The search results show a single hit for the trace ID 'trace 0 1, 2022'. The visualization area shows a purple bar representing the event duration from 07:59:59.9996 to 08:00:00.0004. The left sidebar lists available fields such as 'date', 'kubernetes', 'log', 'serviceName', 'spanId', 'stream', 'time', and 'traceId'. The bottom of the console displays the log event details for the selected trace.

```
> 2022-10-24 17:40:08 date: 1666600830 kubernetes: {"container_name": "payment-service", "container_hash": "126221258167.dkr.ecr.us-east-2.amazonaws.com/payment-service@sha256:b1d0efe5bc0b82e8343c318071af552c7a4706b6a146e484b0855b04942479a0", "host": "ip-172-16-22-100.us-east-2.compute.internal", "annotations": {"kubernetes.io/psp": "eks.privileged"}, "docker_id": "ffb4a12d37639885a862a2424fcac65c3ad8593611557105d32993dce8302068", "pod_id": "4630c0a1-6707-4ecb-a235-e09898a8ab68", "container_image": "126221258167.dkr.ecr.us-east-2.amazonaws.com/payment-
```

Observability > Notebook

- PPL、SQL によるログ検索結果、グラフ、任意の注釈を記載可能
- 作成したノートブックはレポート機能と連携し、PDF または PNG 形式で出力可能
- 以下のようなユースケースで有用
 - 障害時の調査・対応手順書
 - 定常レポートの作成



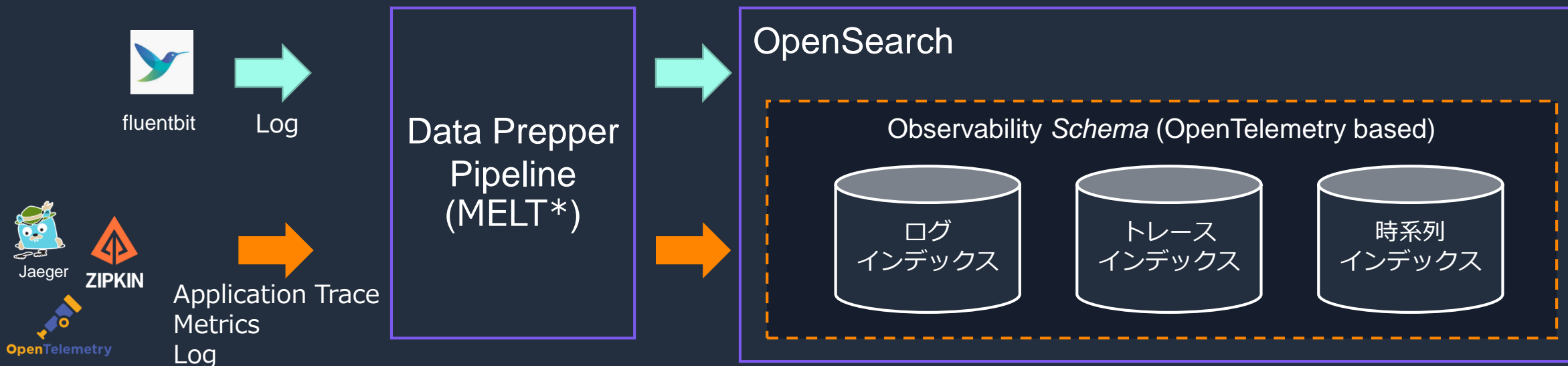
テレメトリデータの収集

- Data Prepper で各種エージェントからデータを収集し、OpenSearch に連携
- [Jaeger](#)、[Zipkin](#)、[X-Ray](#) SDKs および OpenTelemetry SDKs との統合によるアプリケーショントレースの迅速な開始をサポート

*MELT = Metrics, Events, Logs, Traces

オブザーバビリティ UI

Piped Query Language (PPL)



OpenTelemetry / AWS Distro for OpenTelemetry



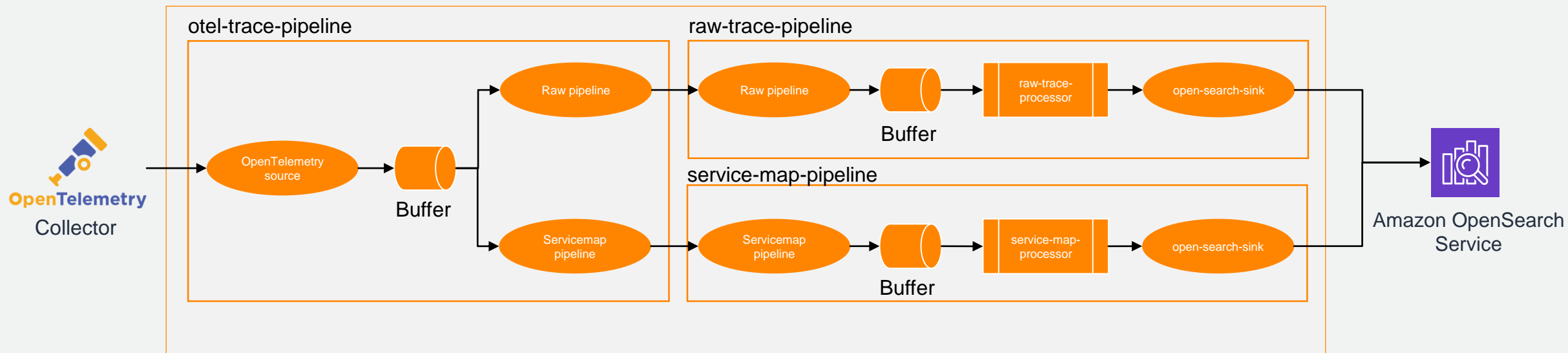
- OpenTelemetry (OTel)
 - クラウドネイティブな Computing Foundation (CNCF) プロジェクト
 - アプリケーションのモニタリング、管理、デバッグを統合するためのオープンソースオブザーバビリティのエージェント、ライブラリ、データプロトコルを提供
 - 全 3 種類のデータシグナルと 11 のプログラミング言語をサポート



- AWS Distro for OpenTelemetry (ADOT)
 - AWSによってサポートされている、セキュアで本番利用可能なオープンソースディストリビューション
 - OpenTelemetry プロジェクト内でコード開発が進行
 - AWS のセキュリティと予測性で認証済

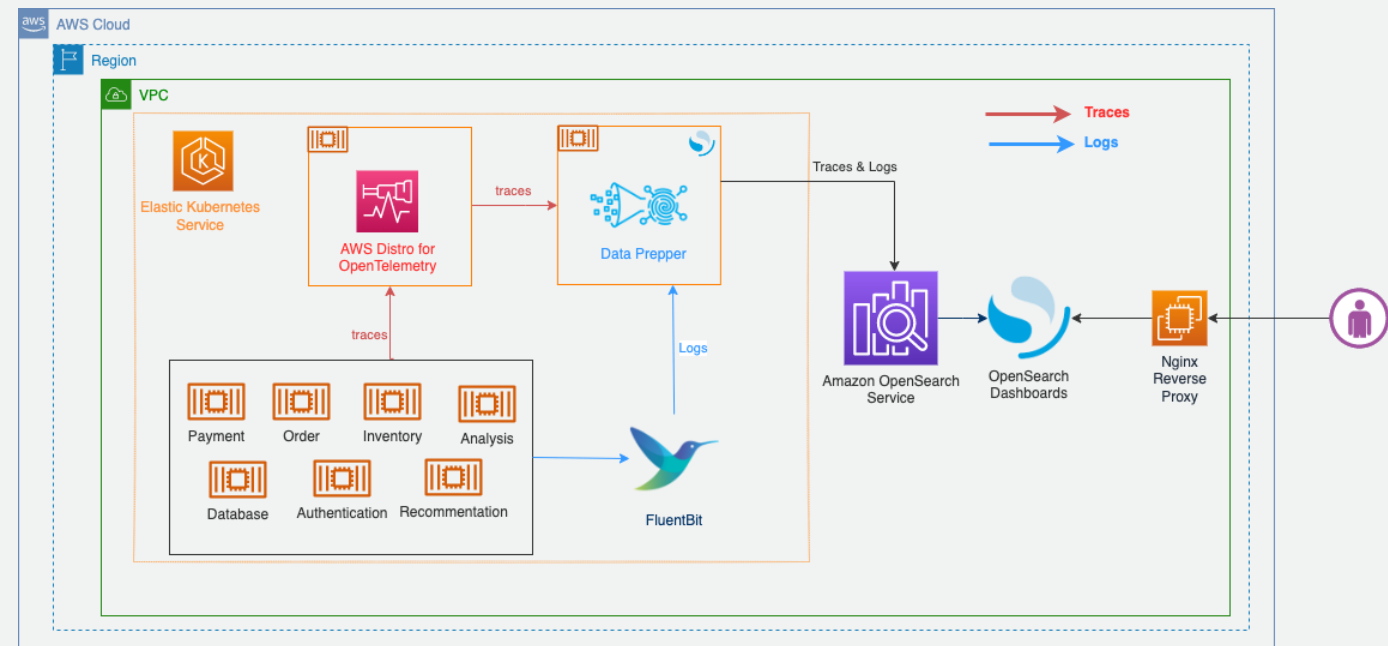
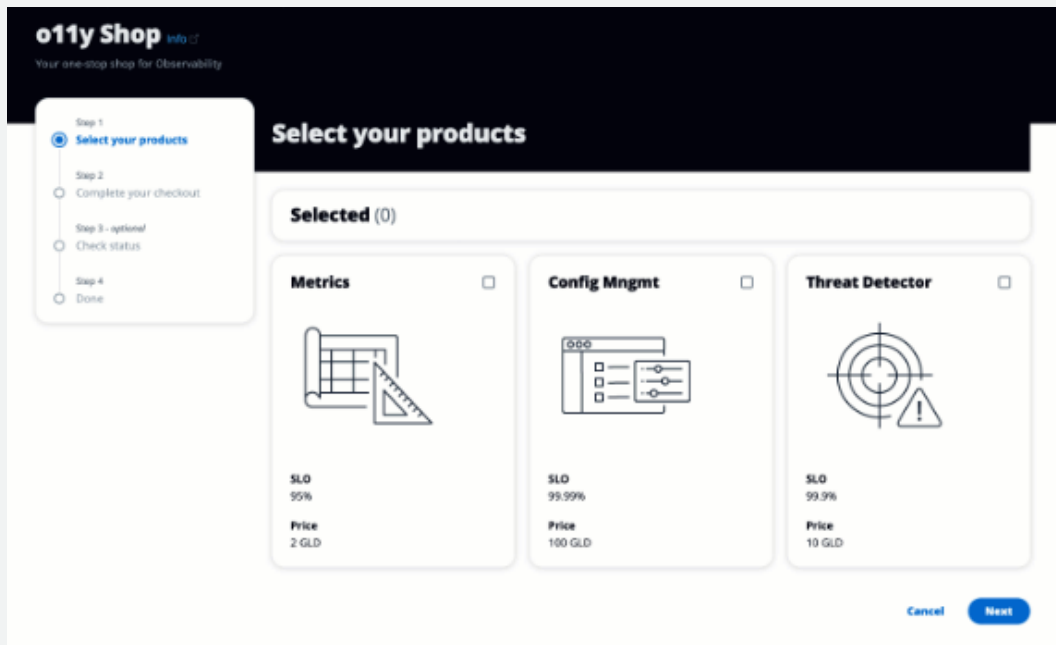
Data Prepper

- オブザーバビリティデータのパイプライン。フィルタリング、加工、情報付与、ルーティング機能を持つ
- Apache License v2.0 のオープンソース



Microservice Observability with Amazon OpenSearch Service Workshop

サンプルアプリケーションからトレースデータを生成し、OpenSearch の Observability 機能を使用したアプリケーションの問題検出から修正までを体験できるワークショップ



その他補足事項

リファレンス

よくある質問:

<https://aws.amazon.com/jp/opensearch-service/faqs/>

トラブルシューティング:

https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/handling-errors.html

ナレッジセンター:

https://aws.amazon.com/jp/premiumsupport/knowledge-center/#Amazon_OpenSearch_Service

料金:

<https://aws.amazon.com/jp/opensearch-service/pricing/>



本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください

<https://aws.amazon.com/jp/premiumsupport/>

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

<https://aws.amazon.com/jp/events/>

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!