On Demand

Amazon OpenSearch Service 最新アップデート 2021 (+2022)

2022 年 1 月のアップデートも解説します！

Takayuki Enomoto
Solution Architect, Analytics
Amazon Web Services Japan G.K.

AWS RE:INVENT RE:CAP

自己紹介

榎本 貴之 (Enomoto, Takayuki)

所属
技術統括本部レディネスソリューション本部
アナリティクスソリューション部

略歴
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 -> **Analytics Specialist SA @AWS**

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

Agenda

Part 1
Amazon OpenSearch Service 概要 & Amazon OpenSearch Service への名称変更について

Part 2
検索, 分析, 可視化関連のアップデート

Part 3
パフォーマンス, スケーラビリティ,運用, セキュリティ関連のアップデート

Agenda

Part 1
Amazon OpenSearch Service 概要 & Amazon OpenSearch Service への名称変更について

Part 2
検索, 分析, 可視化関連のアップデート

Part 3
パフォーマンス, スケーラビリティ,運用, セキュリティ関連のアップデート

Amazon OpenSearch Service 概要

Amazon OpenSearch Service

SUCCESSOR TO
AMAZON ELASTICSEARCH SERVICE

Fully managed

Log and search analytics

Cost effective

AWS RE:INVENT
RE:CAP

Amazon OpenSearch Service の特徴

フルマネージド

API とコンソール経由で,
数分でクラスターを
デプロイして利用可能

柔軟性

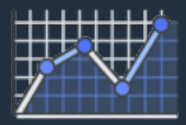
データの検索や
ログの分析を実行可能
AWS およびオープンソースの
データ収集ツールに対応

コスト効率

使った分だけの従量課金
運用コストを削減可能
ワークロードに応じたインスタンス
スタイプ, リザーブドインスタンス
の提供

高い可用性

マルチ AZ への対応
定期的な自動スナップショット取得
障害調査にかかせない
メトリクス, ログ収集の自動化



**スケーラブルで
高いパフォーマンス**

最大 200 ノードまでスケール
最大 3 PiB のデータを格納可能
3 つのストレージティアを提供
自動チューニング

セキュリティと認証

Amazon VPC 対応
ダッシュボードログイン時の認証機能
FISMA, SOC, PCI, FedRamp 取得
マルチテナント機能, 監査ログ

Amazon OpenSearch Service を活用しているお客様

Software and Internet

Adobe
IAC
AUTODESK

Education Technology

McGraw Hill Education
INSTRUCTURE
Blackboard

BioTech and Pharma

MONSANTO
Bristol-Myers Squibb

Financial Services

THOMSON REUTERS
stripe
KICKSTARTER

Media and Entertainment

mlbam
NETFLIX
FOX

Social Media

cookpad
ancestry
Nextdoor

Telecommunications

Jio
COMCAST
T-Mobile

Travel and Transportation

lyft
Expedia
UBER

Real Estate

Zillow
move

Logistics and Operations

here
elementum
infor

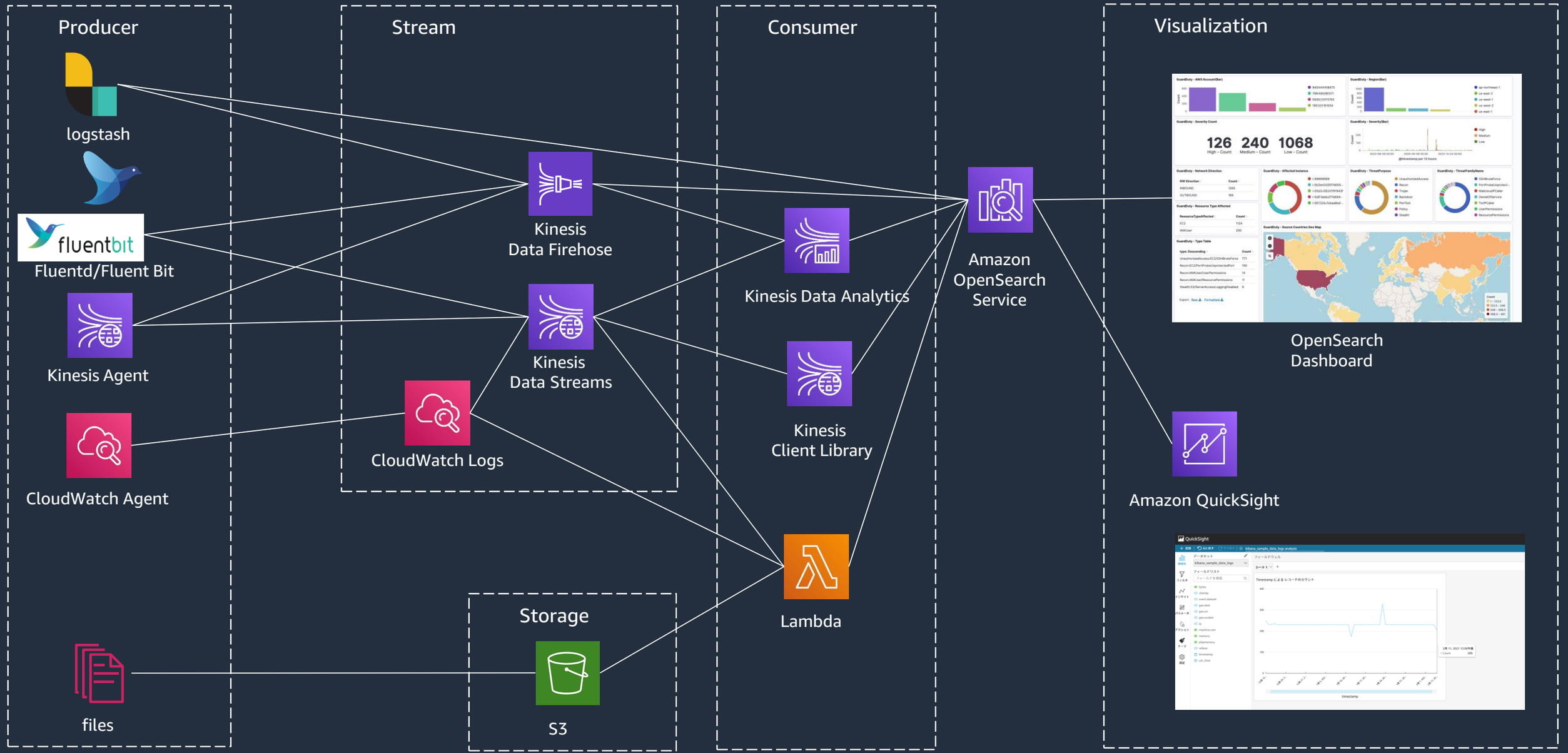
Publishing

FT FINANCIAL TIMES
ELSEVIER
The Washington Post

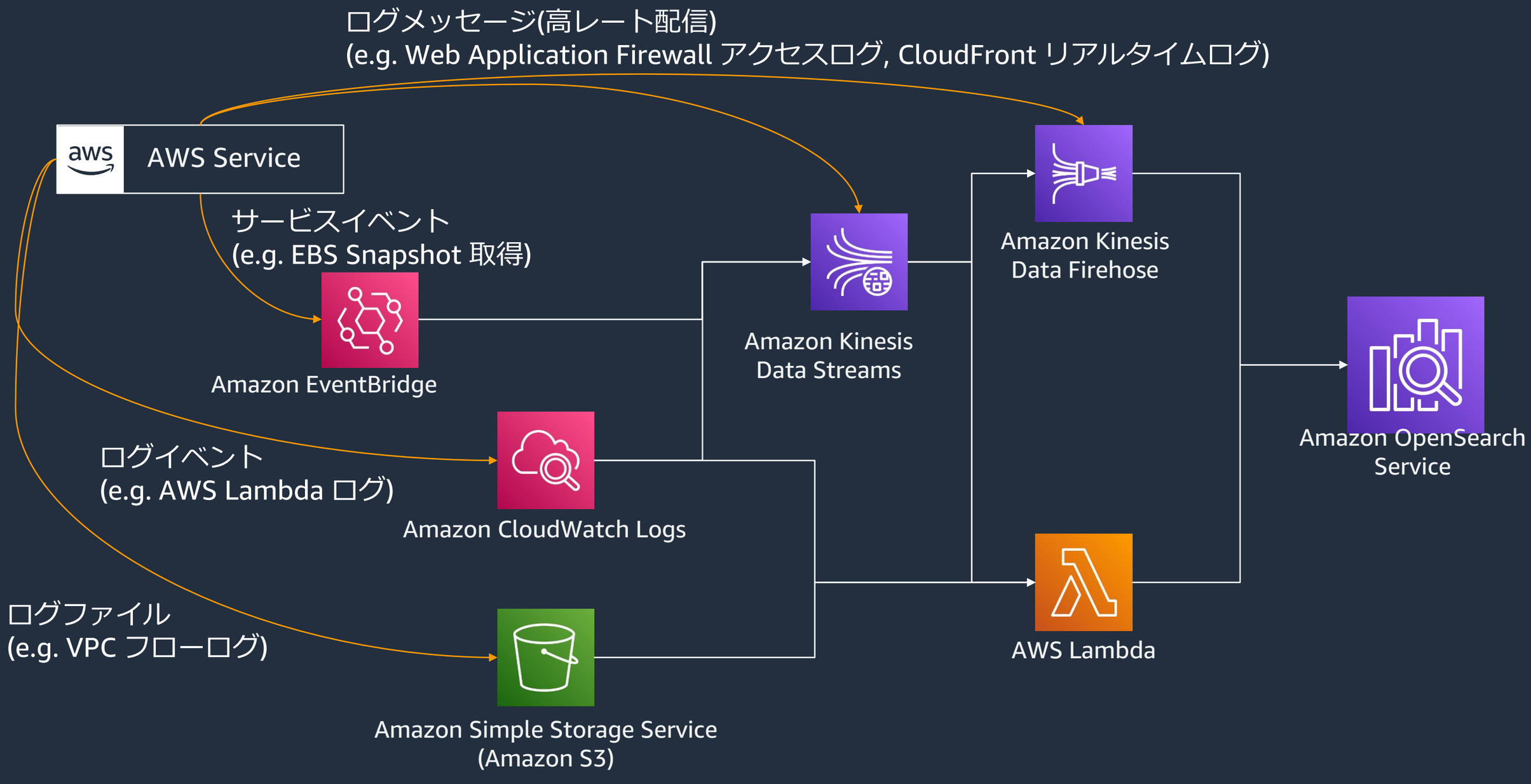
Other

Canon
SAMSUNG
British Gas

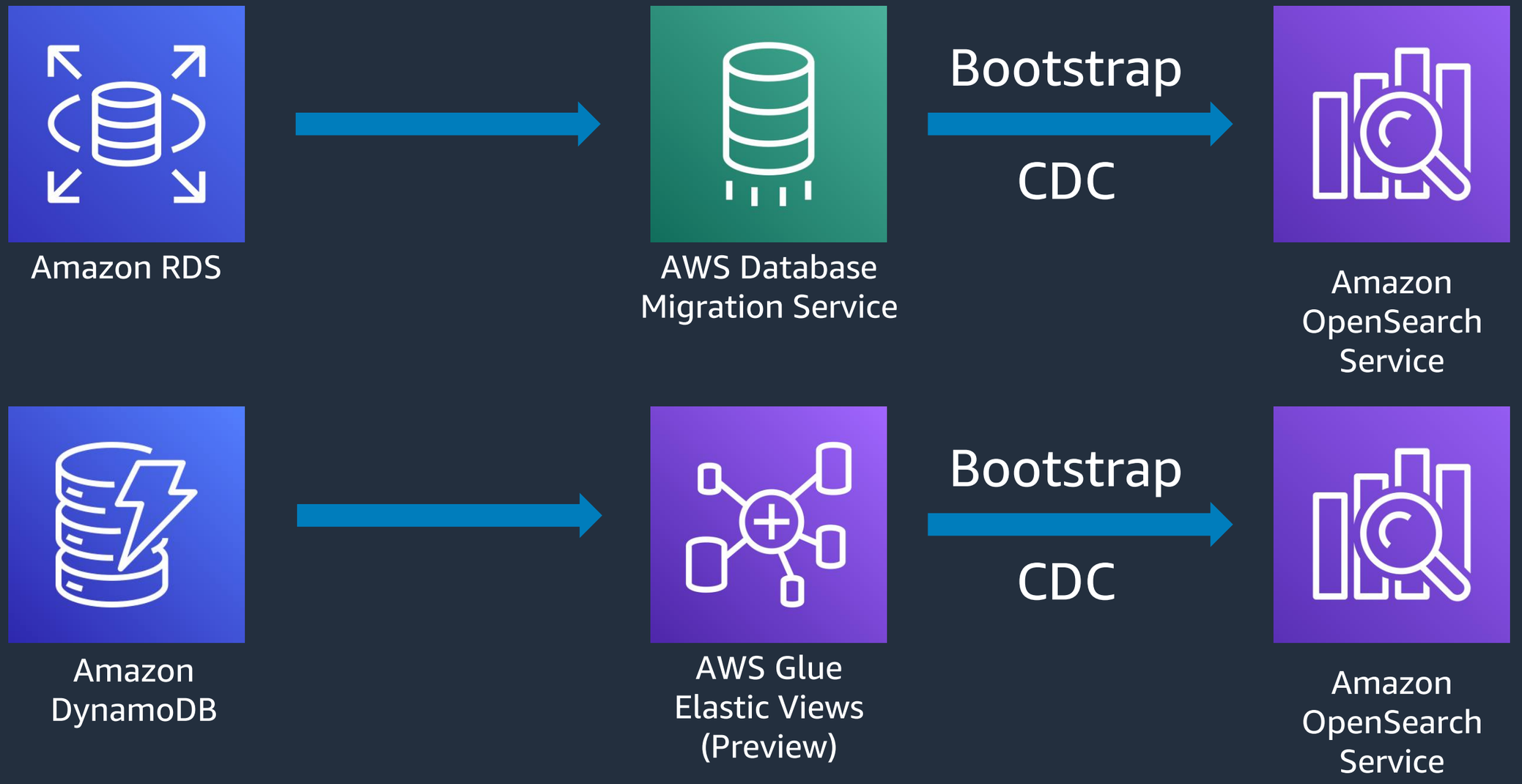
アプリケーションログの取り込み



AWS サービスのログ, イベント取り込み

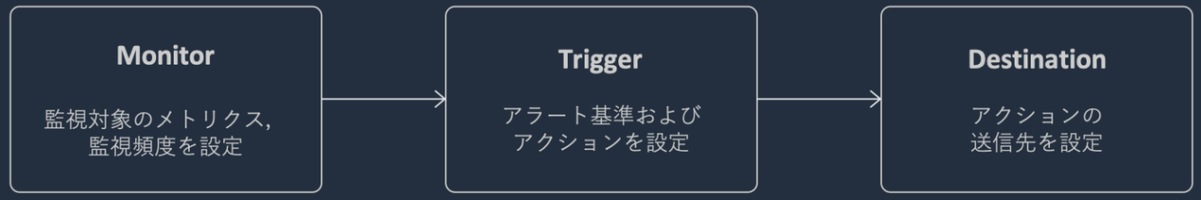


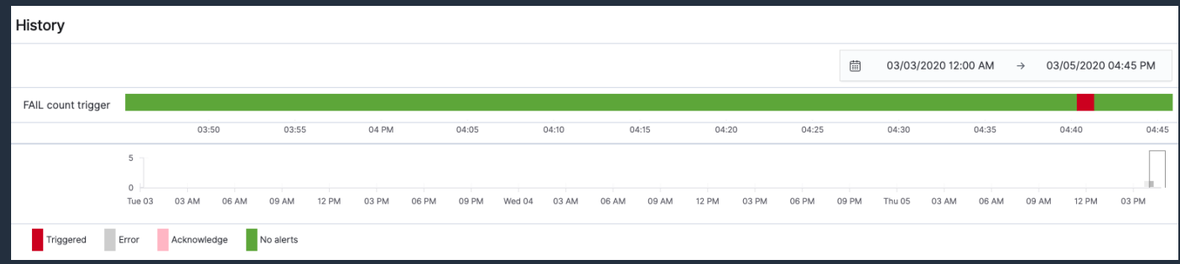
データベースに対する全文検索



OpenSearch Dashboards によるリアルタイム分析

- 蓄積したストリーミングデータを OpenSearch Dashboards で可視化
- GUI ベースでダッシュボードの作成，管理を行い，詳細な権限管理で複数部署が共同利用
- 基準を超えるような数値が出たら 自動で通知を送るような連携も可能



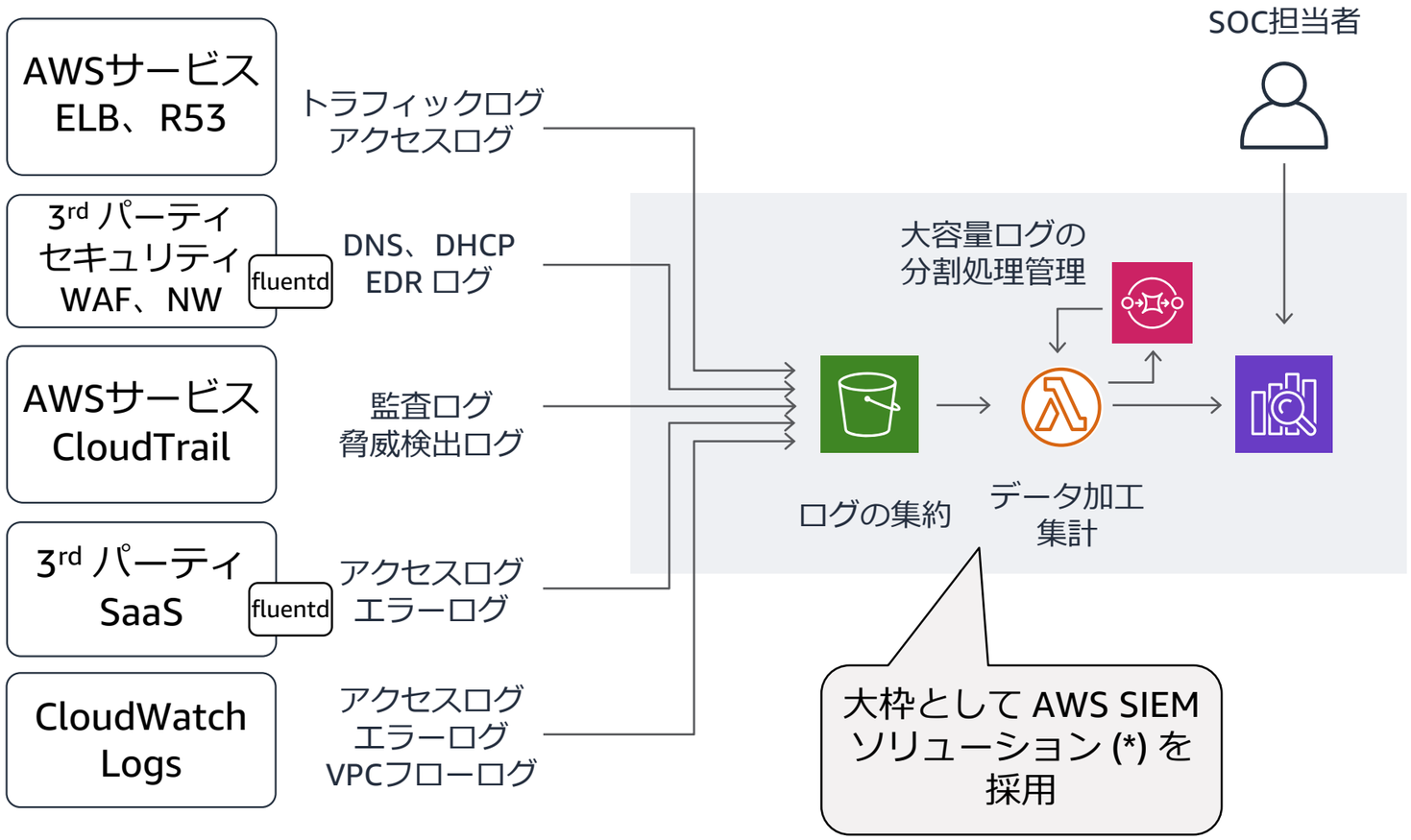


リアルタイムダッシュボードの利用シーン

- OpenSearch Dashboards を用いることでよりインタラクティブな形で分析を実施可能
- ビジネスユーザーも使うが，アナリストや開発者がメインターゲット
- SIEM(Security Information and Event Management) のように，セキュリティ問題の詳細な調査を行う
- カスタマーサポートで特定のログを検索する，全文検索を含めた調査を行う

高生産性　マネージド 業務注力　コスト最適化

お客様事例 - Sansan様 統合セキュリティ監視（SIEM）



1TB/Day のログ処理と可視化

課題

- サービスプロバイダとしての セキュリティ担保の責任
- 対象ログデータは常に増加傾向
- 運用工数にも大きく影響

効果

- 短期実装: 構想から **2ケ月**で最初のリリース。以降、対象ログを拡張。
- コスト最適化: 商用SIEMと比べてライセンス - **80% 以上**削減
- オペレーション最適化
  - インフラ管理タスク – **ほぼ自動化**（サーバーレス化）

* https://aws.amazon.com/jp/blogs/news/siem-on-amazon-elasticsearch-service/

2019 年から 2021, 2022 年にかけてのアップデート

Search & Analysis

Supported version

- Elasticsearch 6.4, 6.5, 6.6, 6.7, 6.8, 7.1, 7.4, 7.7, 7.8, 7.9, 7.10
- OpenSearch 1.0, 1.1

Remote Reindex

Custom dictionary

Cross-cluster search

Async Search

OpenSearch

- Alerting
- Anomaly detection
- SQL, PPL
- k-NN search
- Dynamic dictionary updates
- Index Rollups
- Index Transform

Visualization

Map Service

OpenSearch

- Notebook
- Reports
- Gantt Charts
- Trace Analytics

Performance & Scalability

Scale Cluster

- up-to 200-nodes
- up-to 3 PB storage

New Instance Type

- M5, C5, R5, T3
- M6g, C6g, R6g, R6gd

UltraWarm

Cold Storage

Auto-Tune

Gzip Compression

OpenSearch

- Index State Management
- Index State Management Template
- Data Streams

Security

Enforce HTTPS

Require TLS 1.2

Encryption for existing domains

Tag-based access control

Compliance

- SOC2
- FedRAMP
- HIPPA

OpenSearch

- Fine-grained access control
- Audit logs
- SAML Auth
- Multi-tenancy

Availability

3-AZ support

Hourly snapshots

In-place instance count update

Precheck for blue/green deployment

Cross-cluster Replication

Custom Endpoint

Event Notification

Metrics

- Shard level metrics

OpenSearch

- Dynamic dictionary updates

2019 年から 2021, 2022 年にかけてのアップデート

Search & Analysis

Supported version

- Elasticsearch 6.4, 6.5, 6.6, 6.7, 6.8, 7.1, 7.4, 7.7, 7.8, 7.9, 7.10
- OpenSearch 1.0, 1.1

Remote Reindex

Custom dictionary

Cross-cluster search

Async Search

OpenSearch

- Alerting
- Anomaly detection
- SQL, PPL
- k-NN search
- Dynamic dictionary updates
- Index Rollups
- Index Transform

2022 年 1 月 4 日 OpenSearch 1.1 をサポート

Visualization

Map Service

OpenSearch

- Notebook
- Reports
- Gantt Charts
- Trace Analytics

Performance & Scalability

Scale Cluster

- up-to 200-nodes
- up-to 3 PB storage

New Instance Type

- M5, C5, R5, T3
- M6g, C6g, R6g, R6gd

UltraWarm

Cold Storage

Auto-Tune

Gzip Compression

OpenSearch

- Index State Management
- Index State Management Template
- Data Streams

Security

Enforce HTTPS

Require TLS 1.2

Encryption for existing domains

Tag-based access control

Compliance

- SOC2
- FedRAMP
- HIPPA

OpenSearch

- Fine-grained access control
- Audit logs
- SAML Auth
- Multi-tenancy

Availability

3-AZ support

Hourly snapshots

In-place instance count update

Precheck for blue/green deployment

Cross-cluster Replication

Custom Endpoint

Event Notification

Metrics

- Shard level metrics

OpenSearch

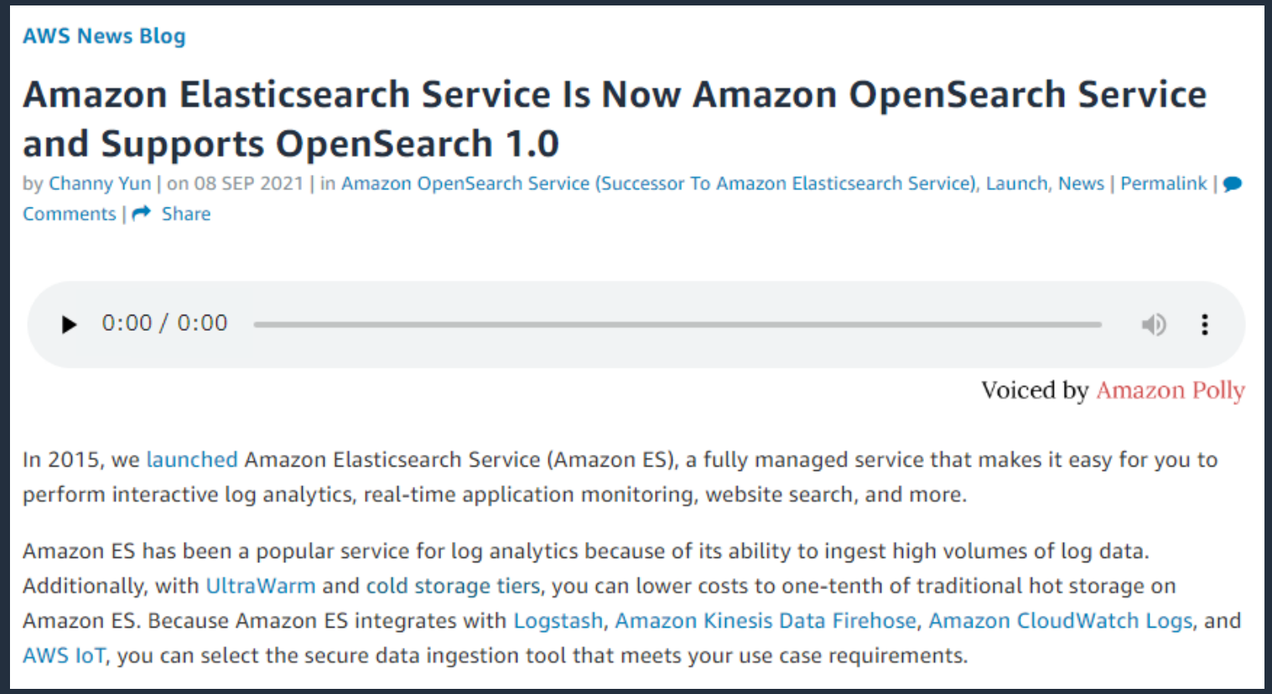
- Dynamic dictionary updates

Amazon Elasticsearch Service は Amazon OpenSearch Service へ

Amazon OpenSearch Service への名称変更

- 2021 年 9 月 8 日に Amazon Elasticsearch Service は Amazon OpenSearch Service へリネーム. 同時に OpenSearch 1.0 エンジンのサポートを開始

- 2022 年 1 月 4 日現在, OpenSearch 1.0, 1.1 バージョンを提供



AWS News Blog

Amazon Elasticsearch Service Is Now Amazon OpenSearch Service and Supports OpenSearch 1.0

by Channy Yun | on 08 SEP 2021 | in Amazon OpenSearch Service (Successor To Amazon Elasticsearch Service), Launch, News | Permalink | Comments | Share

0:00 / 0:00

Voiced by Amazon Polly

In 2015, we launched Amazon Elasticsearch Service (Amazon ES), a fully managed service that makes it easy for you to perform interactive log analytics, real-time application monitoring, website search, and more.

Amazon ES has been a popular service for log analytics because of its ability to ingest high volumes of log data. Additionally, with UltraWarm and cold storage tiers, you can lower costs to one-tenth of traditional hot storage on Amazon ES. Because Amazon ES integrates with Logstash, Amazon Kinesis Data Firehose, Amazon CloudWatch Logs, and AWS IoT, you can select the secure data ingestion tool that meets your use case requirements.

https://aws.amazon.com/jp/blogs/aws/amazon-elasticsearch-service-is-now-amazon-opensearch-service-and-supports-opensearch-10/

Amazon OpenSearch Service 変更概要

- OpenSearch 1.0 エンジン, OpenSearch Dashboards の提供開始
  - OpenSearch 1.0 に付随する新機能も利用可能に
  - 2022 年 1 月現在は OpenSearch 1.1 も利用可能

- 既存の Elasticsearch エンジンを利用している環境には影響なし
  - 既存の Elasticsearch 7.10 およびそれ以前のバージョンの Elasticsearch エンジンの利用は今後も可能. 料金, サポートについても従来通り

- 変更の詳細についてはドキュメントにまとめられている
  - https://docs.aws.amazon.com/opensearch-service/latest/developerguide/rename.html

The OpenSearch Project

APACHE LICENSE 2.0 のもとリリースされた分散型のオープンソース検索，分析スイート

100%
オープンソース

エンタープライズ
グレード

コミュニティ
駆動

https://github.com/opensearch-project

OpenSearch が提供するエンタープライズグレードの機能

いずれもサブスクリプション無しで利用可能

Analysis
Anomaly Detection
Alert
Trace Analytics

Advanced Search
Asynchronous Search
k-NN
PPL
SQL

Analyzer
Performance Analyzer
Root Cause Analysis

Security
Audit Logs
Access Control

Index Management
Index State Management
Index Rollups
Refresh Search Analyzer
Data Streams
(New!!) Cross Cluster Replication

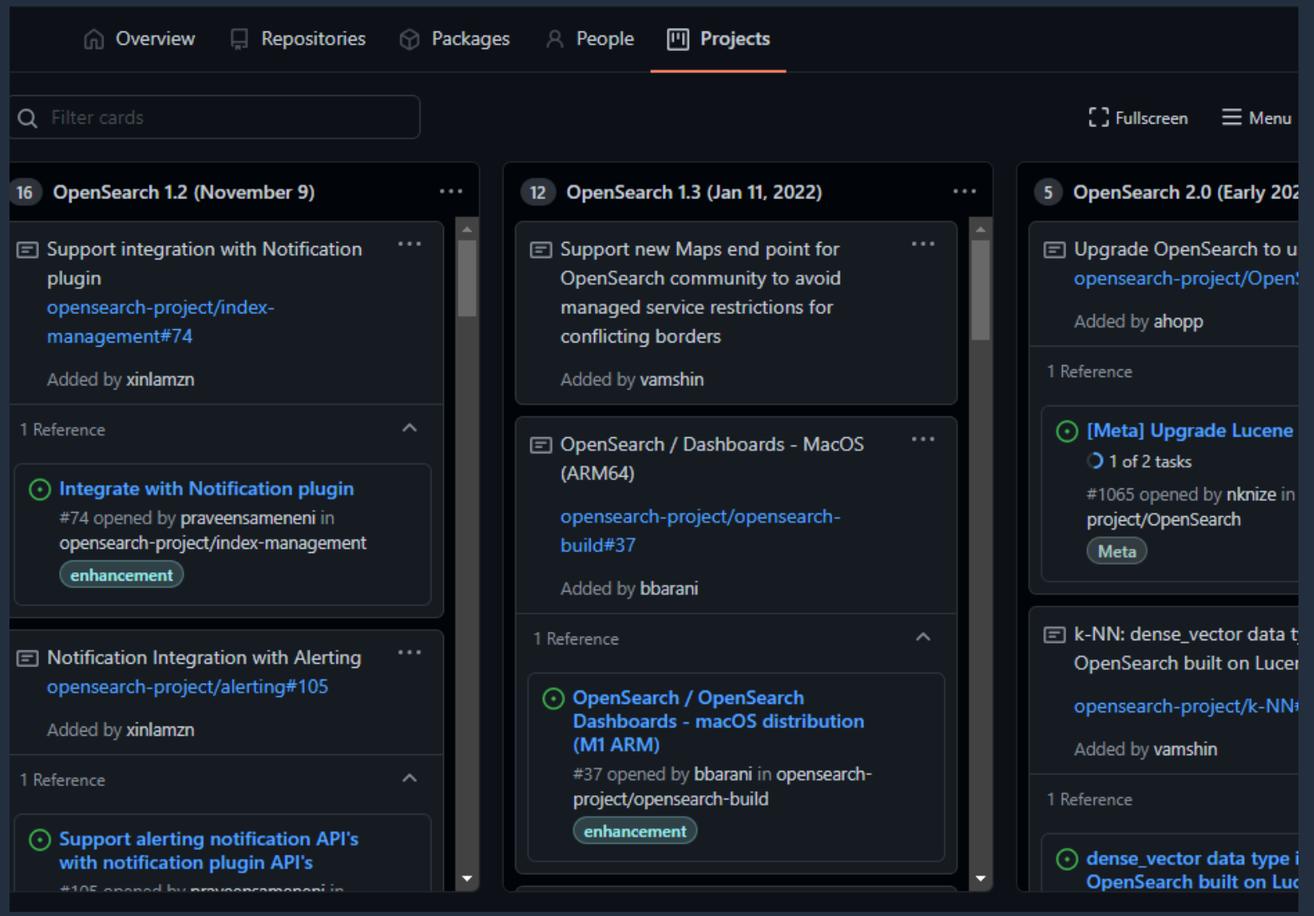
OpenSearch のロードマップ

OpenSearch 1.2(Released)
- App Analytics

OpenSearch 1.3(Jan, 2022)
- Point In Time Search
- Visualization Canvas

OpenSearch 1.4(March, 2022)
- Schema on Reads
- Threat Detection

OpenSearch 2.0(Early 2022)
- Upgrade Lucene to 9.0



https://github.com/orgs/opensearch-project/projects/1

OpenSearch と Elasticsearch の互換性

API 互換性

- インデクシング, 検索, 管理については Elasticsearch 7.10 と同様の REST API を提供. クエリ構文およびレスポンスデータの構造も同様

データ互換性

- OpenSearch では Elasticsearch バージョン 6.0 から 7.10 までに作成された Index との互換性がある. これらの Index を移行し, 利用することが可能

ソフトウェア互換性

クライアントライブラリ

- OpenSearch Project として Elastic から fork したライブラリを提供
- Java, Java high-level rest client, Python, Go, JavaScript, PHP をサポート
  - https://opensearch.org/docs/latest/clients/java-rest-high-level/
  - https://opensearch.org/docs/latest/clients/java/
  - https://opensearch.org/docs/latest/clients/python/
  - https://opensearch.org/docs/latest/clients/go/
  - https://opensearch.org/docs/latest/clients/javascript/
  - https://opensearch.org/docs/latest/clients/php/

ソフトウェア互換性

エージェント, その他のツール

エージェント

- Logstash については logstash-output-opensearchを利用可能
  - https://github.com/opensearch-project/logstash-output-opensearch
- OpenSearch Project としては Beats 互換のツール提供は現状無し. 旧バージョンの Beats を利用する必要あり
  - https://opensearch.org/docs/latest/clients/agents-and-ingestion-tools/index/

ベンチマークツール

- OpenSearch Benchmark を提供
  - https://github.com/opensearch-project/opensearch-benchmark

Compatibility Mode

クライアントとの互換性を保つために, エンジンのバージョン表記を設定で変更可能

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
}

GET /?filter_path=version
# result
{
  "version" : {
    "number" : "7.10.2",
    "build_type" : "tar",
    "build_hash" : "unknown",
    "build_date" : "2021-11-11T13:03:46.725100Z",
    "build_snapshot" : false,
    "lucene_version" : "8.8.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1“
  }
}
```

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : false
  }
}

GET /?filter_path=version
# result
{
  "version" : {
    "distribution" : "opensearch",
    "number" : "1.0.0",
    "build_type" : "tar",
    "build_hash" : "unknown",
    "build_date" : "2021-11-11T13:03:46.725100Z",
    "build_snapshot" : false,
    "lucene_version" : "8.8.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1“
  }
}
```

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/rename.html

Agenda

Part 1
Amazon OpenSearch Service 概要 & Amazon OpenSearch Service への名称変更について

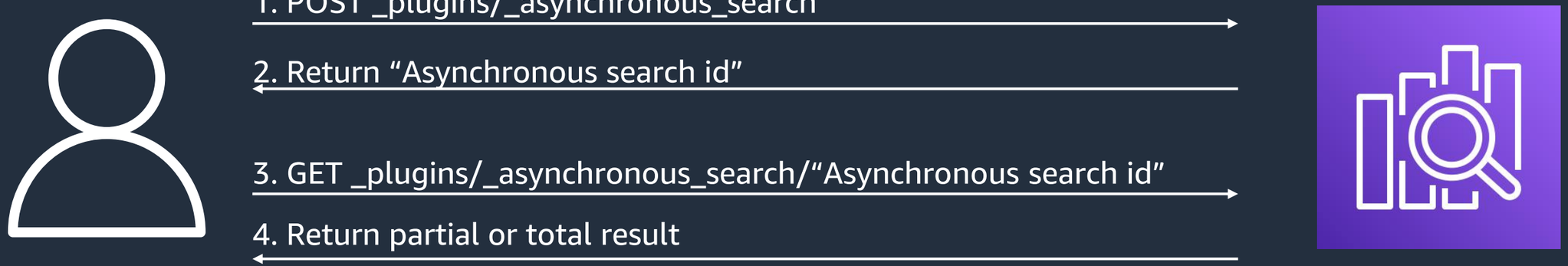
Part 2
検索, 分析, 可視化関連のアップデート

Part 3
パフォーマンス, スケーラビリティ,運用, セキュリティ関連のアップデート

非同期検索

Asynchronous Search

- 非同期な検索リクエストを発行する機能
- 大量データに対する検索や集計など, 時間がかかるクエリを実行する際のタイムアウトを回避することができる
- 検索処理はバックグラウンドで実行され, 非同期検索リクエスト実行時に発行された ID を使用することで結果を取得可能. 検索結果は任意の期間保存することが可能
- Elasticsearch 7.10 および OpenSearch 1.0 以降で利用可能



https://docs.aws.amazon.com/opensearch-service/latest/developerguide/asynchronous-search.html
https://opensearch.org/docs/latest/search-plugins/async/index/

Asynchronous Search – リクエスト発行

- <index-name>/_plugins/_asynchronous_search に対してリクエストを発行する
- ワイルドカードによる複数 Index へのクエリ, alias に対するクエリもサポート
- レスポンスには ID, クエリの有効期限が含まれる

```
POST nyc-taxi/_plugins/_asynchronous_search?pretty&wait_for_completion_timeout=1ms&keep_on_completion=true&size=0
{
  "size": 0,
  "aggs": {
    "date": {
      "date_histogram": {
        "field": "tpep_pickup_datetime",
        "calendar_interval": "day"
      },
      "aggs": {
        "passenger_count": {
          "sum": {
            "field": "passenger_count"
          }
        }
      }
    }
  }
}
```

```
{
  "id" :
"FjRqN3FrQ0lxUjYyNXpTbDc4eUR2MmcIMTE1NDkzMjAURlhiRC1YMEJyd2FKLVhWTkhGNmcBMw==",
  "state" : "RUNNING",
  "start_time_in_millis" : 1640572853408, #2021-12-27T02:40:53 UTC
  "expiration_time_in_millis" : 1640659253408, #2021-12-28T02:40:53 UTC
  "response" : {
    "took" : 0,
    "timed_out" : false,
    "num_reduce_phases" : 0,
    "_shards" : {
      "total" : 12,
      "successful" : 0,
      "skipped" : 0,
      "failed" : 0
    },
    "hits" : {
      "max_score" : null,
      "hits" : [ ]
    }
  }
}
```

Asynchronous Search – 結果の取得

- GET _plugins/_asynchronous_search/<ID> で結果を取得する
- クエリ実行中の場合, state: RUNNING と共に部分的な結果が返却される

```
GET
_plugins/_asynchronous_search/FjRqN3FrQ0lxUjYyNXpTbDc4eUR2MmcIMTE1NDkzMjAURlhiRC1YMEJyd2FKLVhWTkhGNmcBMw==?pretty
```


```
{
  "id" :
"FjRqN3FrQ0lxUjYyNXpTbDc4eUR2MmcIMTE1NDkzMjAURlhiRC1YMEJyd2FKLVhWTkhGNmcBMw==",
  "state" : "RUNNING",
  "start_time_in_millis" : 1640572853408,
  "expiration_time_in_millis" : 1640659253408,
  "response" : {
    "took" : 8605,
    "timed_out" : false,
    "_shards" : {
      "total" : 12,
      "successful" : 8,
      "skipped" : 0,
      "failed" : 0
    },
    "hits" : {
      "total" : {
        "value" : 10000,
        "relation" : "gte"
      },
      "max_score" : null,
      "hits" : [ ]
    },
    "aggregations" : {
      (...)
```

Asynchronous Search – 結果の取得

クエリの実行が完了している場合, 完全な結果が返却される

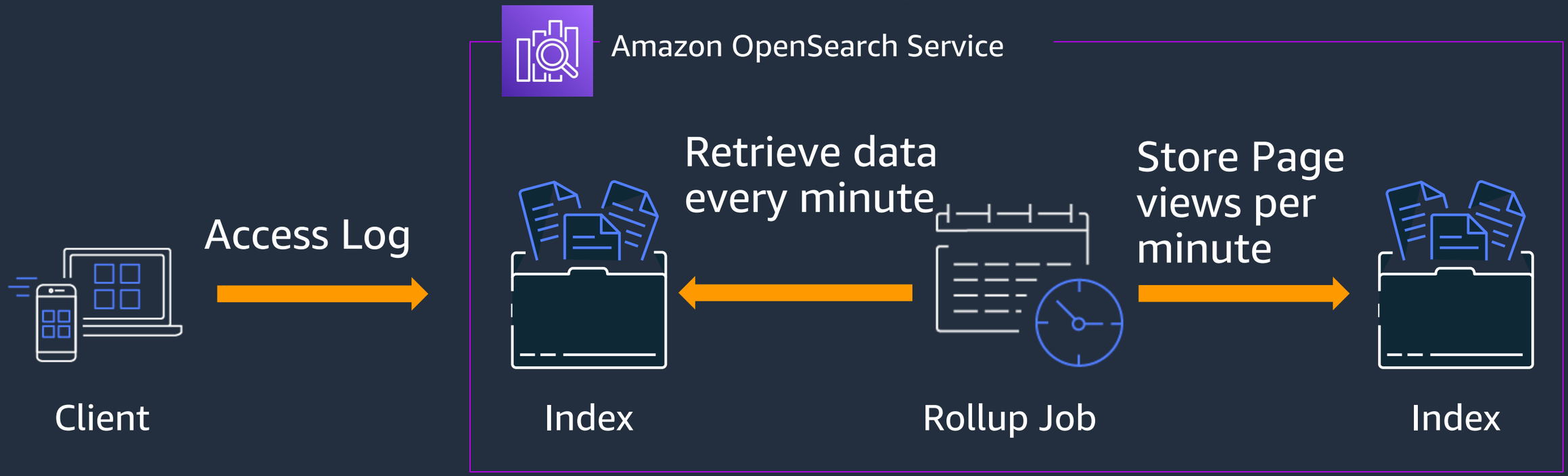
```
GET
_plugins/_asynchronous_search/FjRqN3FrQ0lxUjYyNXpTbDc4eUR2MmcIMTE1NDkzMjAURlhiRC1YMEJyd2FKLVhWTkhGNmcBMw==?pretty
```


```
{
  "id" :
"FjRqN3FrQ0lxUjYyNXpTbDc4eUR2MmcIMTE1NDkzMjAURlhiRC1YMEJyd2FKLVhWTkhGNmcBMw==",
  "state" : "STORE_RESIDENT",
  "start_time_in_millis" : 1640572853408,
  "expiration_time_in_millis" : 1640659253408,
  "response" : {
    "took" : 22135,
    "timed_out" : false,
    "num_reduce_phases" : 3,
    "_shards" : {
      "total" : 12,
      "successful" : 12,
      "skipped" : 0,
      "failed" : 0
    },
    "hits" : {
      "total" : {
        "value" : 10000,
        "relation" : "gte"
      },
      "max_score" : null,
      "hits" : [ ]
    },
    "aggregations" : {
      (...)
```

Index Rollups

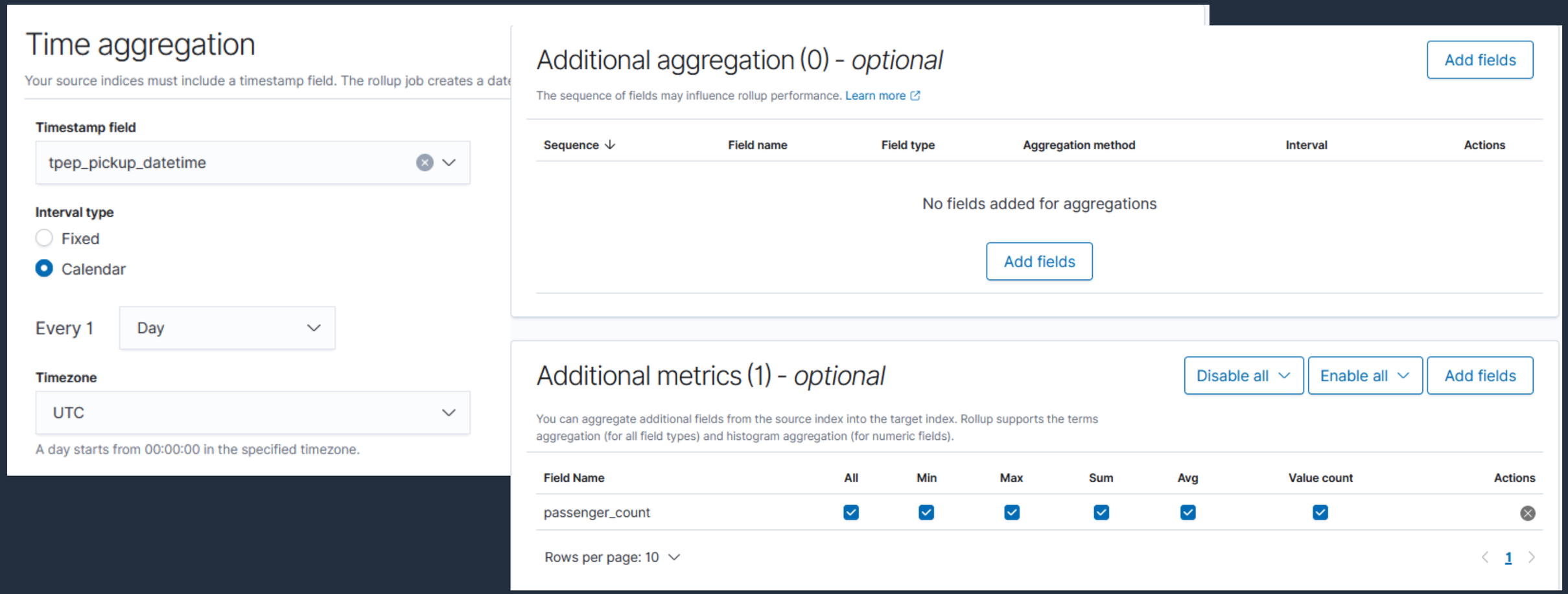
Index Rollups

- 時系列データのサマリを作成する機能
- サマライズされた結果は別の Index に保存可能
  - Index に対して Aggregation を行った結果がそのまま保存される
- 集計結果の可視化を行う際の負荷軽減, 高速化を実現



Rollup Job の作成

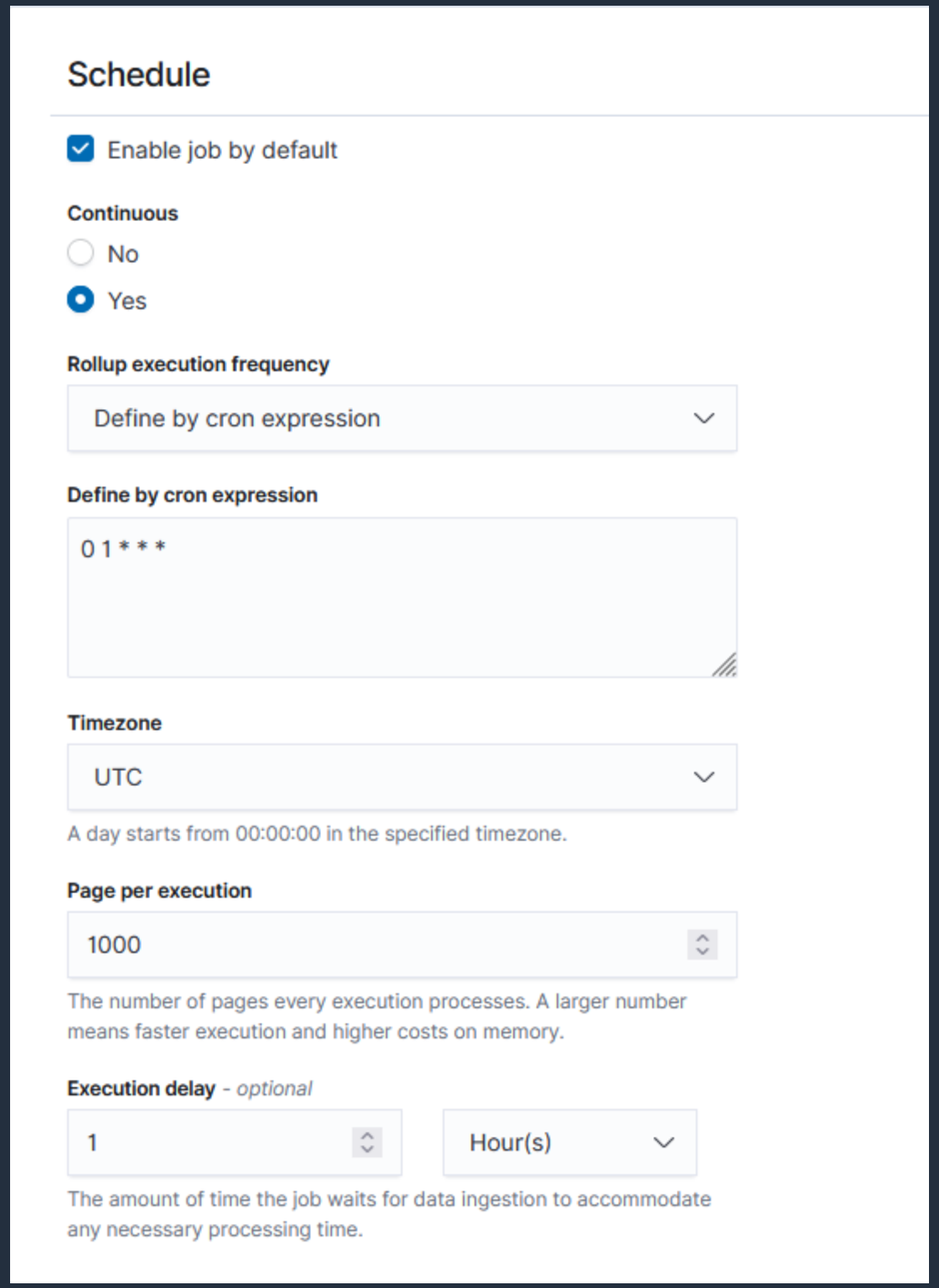
Timestamp フィールド, 集計対象のフィールドを指定
集計時にバケット(集計軸) を指定することも可能



Rollup Job の作成

- Rollup Job は定期実行が可能. また前回処理した地点からの増分実行をサポート

- 遅延設定により, 実行時間と集計対象の時間をずらすことも可能
  - 実行タイミングを毎日 1 時, 遅延を 1 時間に設定することで, 1:00 に前日の 0:00 から翌日の 0:00 までの集計が実行される
  - ストリームデータなど, 実際にイベントが発生してから OpenSearch に取り込まれるまでにタイムラグが発生するようなケースで有用



Index Rollups – 活用例

要件

- タクシー乗降データから日次の乗降客数を集計し, 可視化する

- 集計対象期間は 2009 年から 2020 年まで

Index Rollups – 活用例

課題

- 対象のデータサイズが大きく, 全期間のデータに対して集計を行うと, (特に初回アクセスにおいて)集計処理に時間がかかってしまう

対象 Index

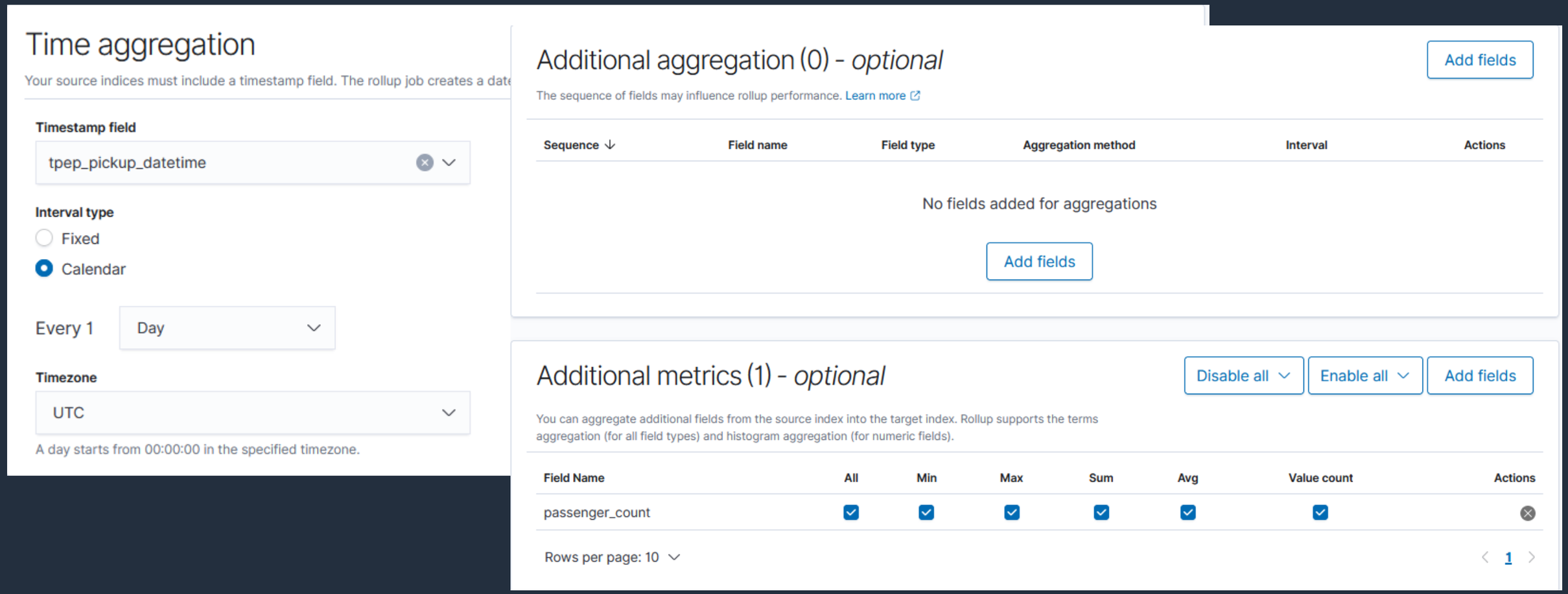
index	pri.store.size
fragmented-taxi-2009	26.7gb
fragmented-taxi-2010	27.8gb
fragmented-taxi-2011	27.6gb
fragmented-taxi-2012	28.7gb
fragmented-taxi-2013	28.4gb
fragmented-taxi-2014	24.1gb
fragmented-taxi-2015	23.1gb
fragmented-taxi-2016	22gb
fragmented-taxi-2017	16.4gb
fragmented-taxi-2018	14.6gb
fragmented-taxi-2019	13.2gb
fragmented-taxi-2020	3.8gb

集計所要時間(ミリ秒)
i3.16xlarge.search x 3 node 構成

Index Rollups – 活用例

解決策

- Index Rollups で日次の乗降客数を事前集計する



Index Rollups – 活用例

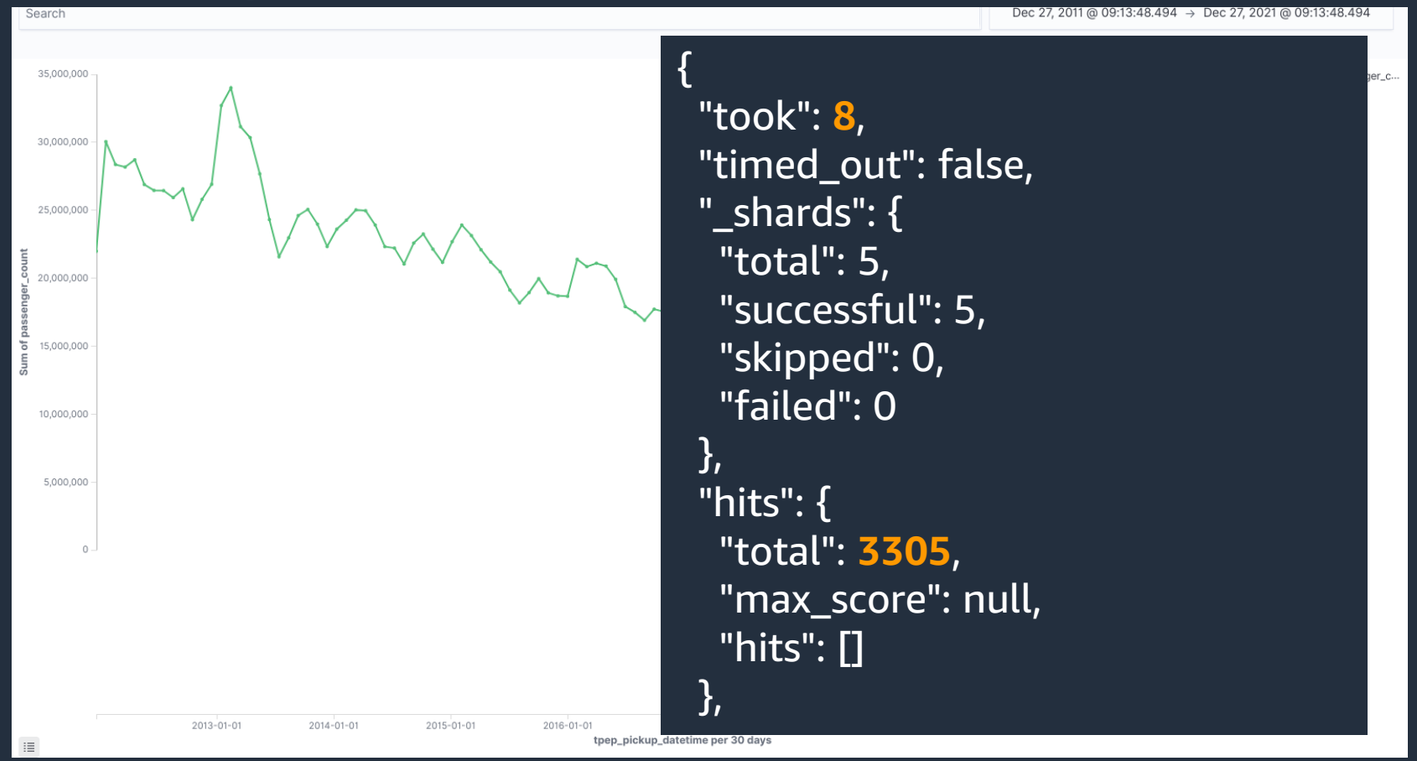
結果

- 集計結果を軽量なインデックスに保存することで, ダッシュボードの表示速度が大幅に改善された

対象 Index

index	pri.store.size
daily_passenger_count	870.2kb

集計所要時間(ミリ秒)
i3.16xlarge.search x 3 node 構成



Index Rollups – 制限

- Rollup Job により作成された Index に対するリクエストには size = 0 の指定が必須
  - つまり, 集計クエリ以外の発行は不可

- Rollup Job により作成された Index に対する Composite Aggregation は未サポート
  - Index Rollups により作成された Index を Index Rollups の Source として使用することはできない
  - Index Transforms の Source として使用することはできない

Index Transforms

Index Transforms

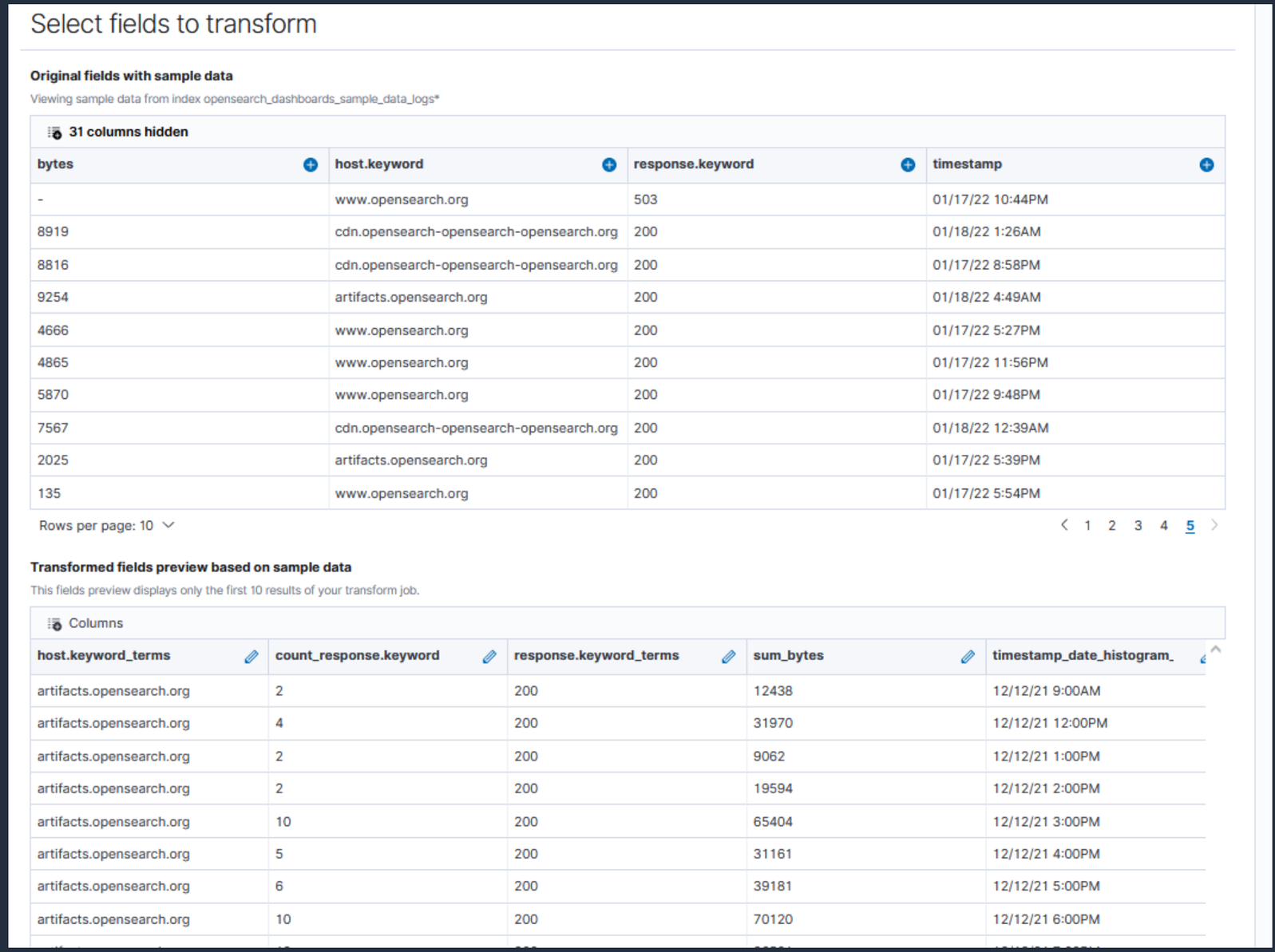
- ある Index に対する集計結果を別の Index に保存する機能
- 複数のフィールドに対するピボット集計を行った結果を可視化に用いたいケースなどで有用
- 時系列データ, 非時系列データのいずれも集計可能

Transform Job の作成

Index フィールドから集計対象のフィールドを選択する

時系列データについては時間ごとの集計が可能

キーワードフィールドに対するバケッティング(集計軸としての利用)も可能



Select fields to transform

Original fields with sample data

Viewing sample data from index opensearch_dashboards_sample_data_logs*

31 columns hidden

bytes	host.keyword	response.keyword	timestamp
-	www.opensearch.org	503	01/17/22 10:44PM
8919	cdn.opensearch-opensearch-opensearch.org	200	01/18/22 1:26AM
8816	cdn.opensearch-opensearch-opensearch.org	200	01/17/22 8:58PM
9254	artifacts.opensearch.org	200	01/18/22 4:49AM
4666	www.opensearch.org	200	01/17/22 5:27PM
4865	www.opensearch.org	200	01/17/22 11:56PM
5870	www.opensearch.org	200	01/17/22 9:48PM
7567	cdn.opensearch-opensearch-opensearch.org	200	01/18/22 12:39AM
2025	artifacts.opensearch.org	200	01/17/22 5:39PM
135	www.opensearch.org	200	01/17/22 5:54PM

Rows per page: 10

< 1 2 3 4 5 >

Transformed fields preview based on sample data

This fields preview displays only the first 10 results of your transform job.

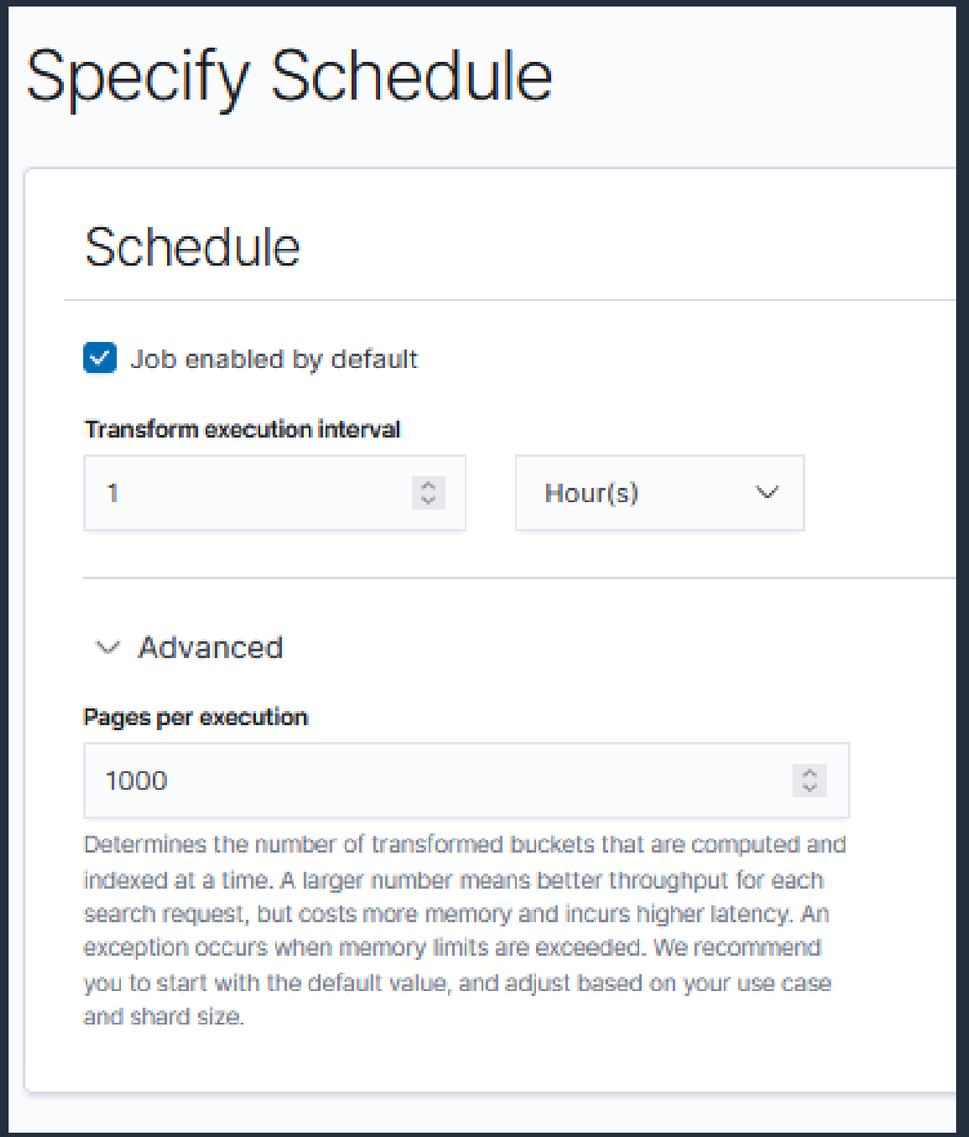
Columns

host.keyword_terms	count_response.keyword	response.keyword_terms	sum_bytes	timestamp_date_histogram_
artifacts.opensearch.org	2	200	12438	12/12/21 9:00AM
artifacts.opensearch.org	4	200	31970	12/12/21 12:00PM
artifacts.opensearch.org	2	200	9062	12/12/21 1:00PM
artifacts.opensearch.org	2	200	19594	12/12/21 2:00PM
artifacts.opensearch.org	10	200	65404	12/12/21 3:00PM
artifacts.opensearch.org	5	200	31161	12/12/21 4:00PM
artifacts.opensearch.org	6	200	39181	12/12/21 5:00PM
artifacts.opensearch.org	10	200	70120	12/12/21 6:00PM

Transform Job の作成

- 指定した間隔でジョブを実行することが可能

- Transform Job は複数回に分けてクエリを実行することで占有メモリを最小限に抑えている. Pages per execution を変更することでスループットを向上させることができるが, その分消費リソースが増加する. 基本的には, デフォルトの 1000 のまま実行することを推奨



Index Transforms – 活用例

要件

- ショッピングサイトの購買履歴から, ユーザーごとの月額売り上げ合計を算出したい
- 算出した月額売り上げ金額を元に, ユニークユーザーごとの月額購入額の分布を作成したい
  - 月額購入額1000円未満のユーザー数
  - 1000 円以上 10000 円未満のユーザー数
  - 10000円以上購入したユーザー数

課題

- ユーザーごとの月額購入額の合計は Aggregation で集計することができるが, 月額購入数に基づく分布を作成することができない

サンプルデータ

```
GET opensearch_dashboards_sample_data_ecommerce/_search?filter_path=hits.hits.fields{  "size": 1,   "fields": ["order_date", "customer_id", "taxless_total_price"],  "_source": false}

{
  "hits" : {
    "hits" : [
      {
        "fields" : {
          "order_date" : [
            "2022-01-10T09:28:48.000Z"
          ],
          "taxless_total_price" : [
            36.98
          ],
          "customer_id" : [
            "38"
          ]
        }
      }
    ]
  }
}
```

Index Transforms – 活用例

ユーザーごとの月額購入額の合計を集計することはできるが, 合計金額ごとの分類を作成することが困難

```
GET opensearch_dashboards_sample_data_ecommerce/_search?filter_path=aggregations.histogram.buckets
{
  "size": 0,
  "aggs": {
    "histogram": {
      "date_histogram": {
        "field": "order_date",
        "calendar_interval": "month"
      },
      "aggs": {
        "customer_id": {
          "terms": {
            "field": "customer_id"
          },
          "aggs": {
            "taxless_total_price": {
              "sum": {
                "field": "taxless_total_price"
              }
            }
(…)
```

```
{
  "aggregations" : {
    "histogram" : {
      "buckets" : [
        {
          "key_as_string" : "2021-12-01T00:00:00.000Z",
          "key" : 1638316800000,
          "doc_count" : 2363,
          "customer_id" : {
            "doc_count_error_upper_bound" : 0,
            "sum_other_doc_count" : 1498,
            "buckets" : [
              {
                "key" : "27",
                "doc_count" : 176,
                "taxless_total_price" : {
                  "value" : 15412.671875
                }
              },
              {
                "key" : "52",
                "doc_count" : 99,
                "taxless_total_price" : {
                  "value" : 8656.953125
                }
              },
```

Index Transforms – 活用例

対策: Index Transform を使用しユーザーごとの月次購入額の合計を事前集計

Select fields to transform

Original fields with sample data

Viewing sample data from index opensearch_dashboards_sample_data_ecommerce*

52 columns hidden

customer_id	order_date	taxless_total_price
38	01/10/22 6:28PM	36.98
20	01/10/22 6:59AM	53.98
26	01/10/22 7:32AM	199.98
22	01/10/22 7:58AM	174.98
38	01/03/22 12:48PM	80.98
22	01/03/22 6:44AM	71.98
7	12/27/21 6:27PM	45.98
52	01/10/22 11:19AM	138.96
17	01/02/22 9:59AM	88.96
5	01/10/22 12:41PM	171.96

Rows per page: 10

1 2 3 4 5

Transformed fields preview based on sample data

This fields preview displays only the first 10 results of your transform job.

Columns

order_date_date_histogram_month	customer_id_terms	sum_taxless_total_price
12/01/21 9:00AM	10	1977.3515625
12/01/21 9:00AM	11	2485.4453125
12/01/21 9:00AM	12	5052.0625
12/01/21 9:00AM	13	5170.12890625
12/01/21 9:00AM	14	1926.640625
12/01/21 9:00AM	15	4901.3125

Index Transforms – 活用例

Index Transform による個々の集計結果は document として格納されるため, aggregation による再集計が可能

```
GET transform_opensearch_dashboards_sample_data_ecommerce/_search?filter_path=hits.hits._source

{
  "hits" : {
    "hits" : [
      {
        "_source" : {
          "transform._id" : "opensearch_dashboards_sample_data_ecommerce",
          "transform._doc_count" : 32,
          "order_date_date_histogram_month" : 1638316800000,
          "customer_id_terms" : "10",
          "sum_taxless_total_price" : 1977.3515625
        }
      },
      {
        "_source" : {
          "transform._id" : "opensearch_dashboards_sample_data_ecommerce",
          "transform._doc_count" : 67,
          "order_date_date_histogram_month" : 1638316800000,
          "customer_id_terms" : "18",
          "sum_taxless_total_price" : 4331.796875
        }
      },
      (...)
```

Index Transforms – 活用例

結果: 事前集計結果を利用した分類が可能に

```
GET
transform_opensearch_dashboards_sample_data_ecommerce/_search?filter_path=aggregations.order_date_date_histogram_month.buckets
{
  "size": 0,
  "aggs": {
    "order_date_date_histogram_month": {
      "date_histogram": {
        "field": "order_date_date_histogram_month",
        "interval": "month"
      },
      "aggs": {
        "sum_taxless_total_price": {
          "range": {
            "field": "sum_taxless_total_price",
            "ranges": [
              { "from": 0, "to": 1000 },
              { "from": 1000, "to": 10000 },
              { "from": 10000}
            ]
(...)
```

```
{
  "aggregations" : {
    "order_date_date_histogram_month" : {
      "buckets" : [
        {
          "key" : 1638316800000,
          "doc_count" : 46,
          "sum_taxless_total_price" : {
            "buckets" : [
              {
                "key" : "0.0-1000.0",
                "from" : 0.0, "to" : 1000.0,
                "doc_count" : 0
              },
              {
                "key" : "1000.0-10000.0",
                "from" : 1000.0, "to" : 10000.0,
                "doc_count" : 45
              },
              {
                "key" : "10000.0-*",
                "from" : 10000.0,
                "doc_count" : 1
              }
            ]
          }
        },
```

Index Transforms – 制限と考慮事項

Index Rollups とは異なり増分実行には非対応

- 同じ軸での集計結果は上書きされるため, 集計結果の重複は発生しない
- 実行対象の Index に含まれるデータは実行の都度すべて再集計されるため, ソースの Index Pattern にはワイルドカードを用いないことを推奨. 時系列 Index については個別の Index ごとに Transform Job を実行すること

https://aws.amazon.com/jp/blogs/big-data/view-summarized-data-with-amazon-opensearch-service-index-transforms/

Index Rollups と Index Transforms の使い分け

Index Rollups を検討するパターン

- OpenSearch Dashboards などから, 集計された時系列データを日常的に参照しており, データ取得のパフォーマンスを改善したい
- 時系列データのサマライズをニアリアルタイムに行いたい
- 集計されたデータを再集計する要件は無い

Index Transforms を検討するパターン

- 集計結果を元にさらに別の集計を行いたい
- 非時系列データに対する集計を行いたい
- 集計はニアリアルタイムで行う必要は無い

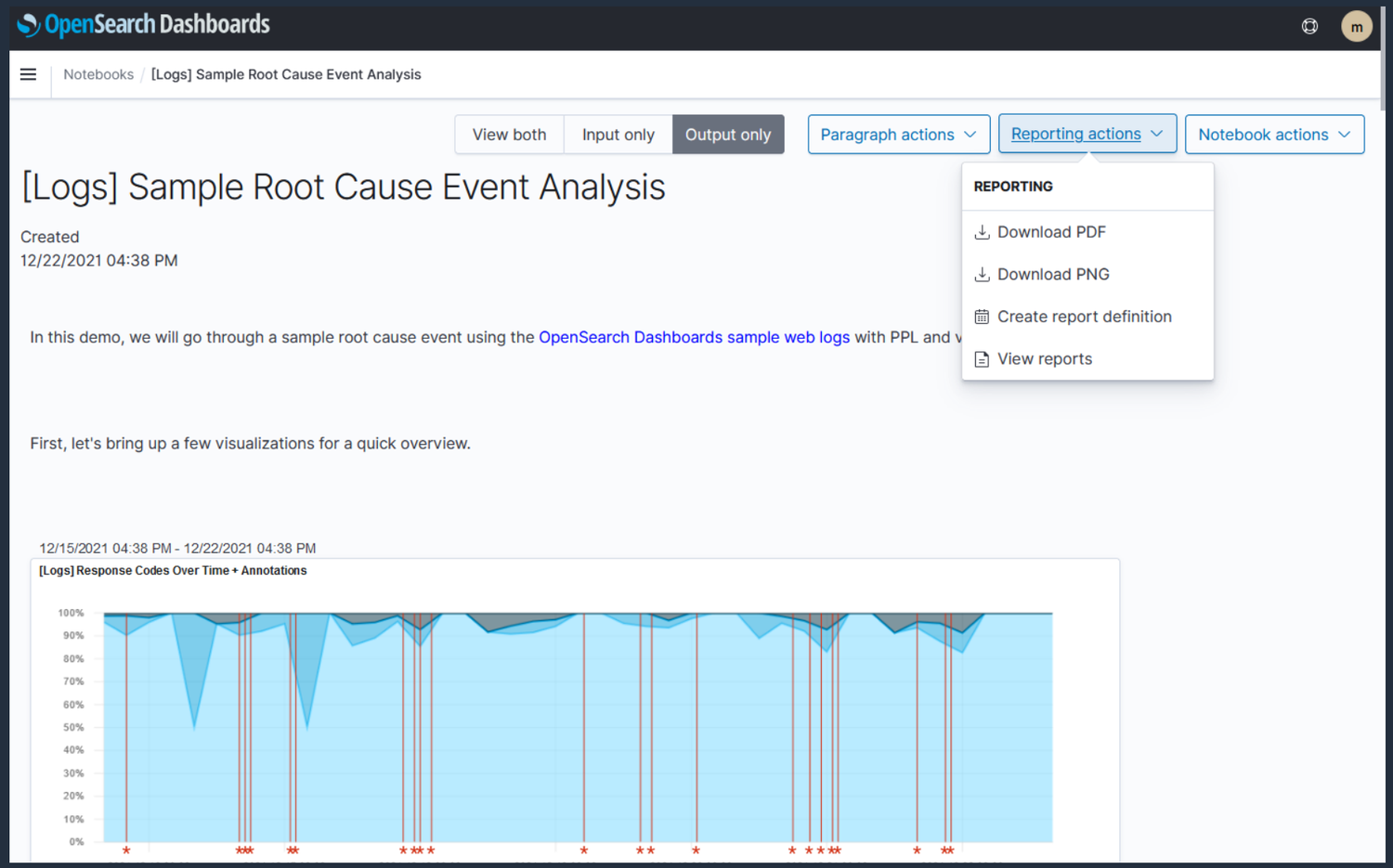
Reporting

Reporting

- Notebook, Dashboard, Visual を PDF, PNG 形式でエクスポート

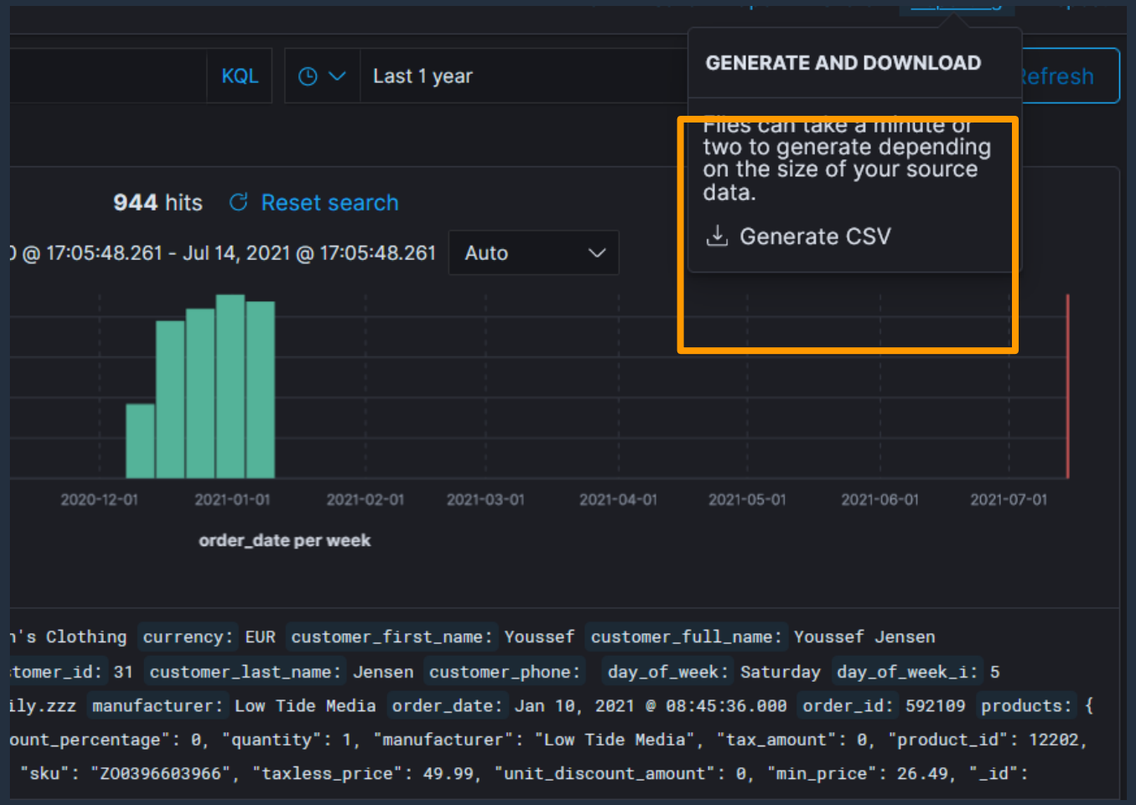
- Discover 上で検索したログを CSV 形式でダウンロード

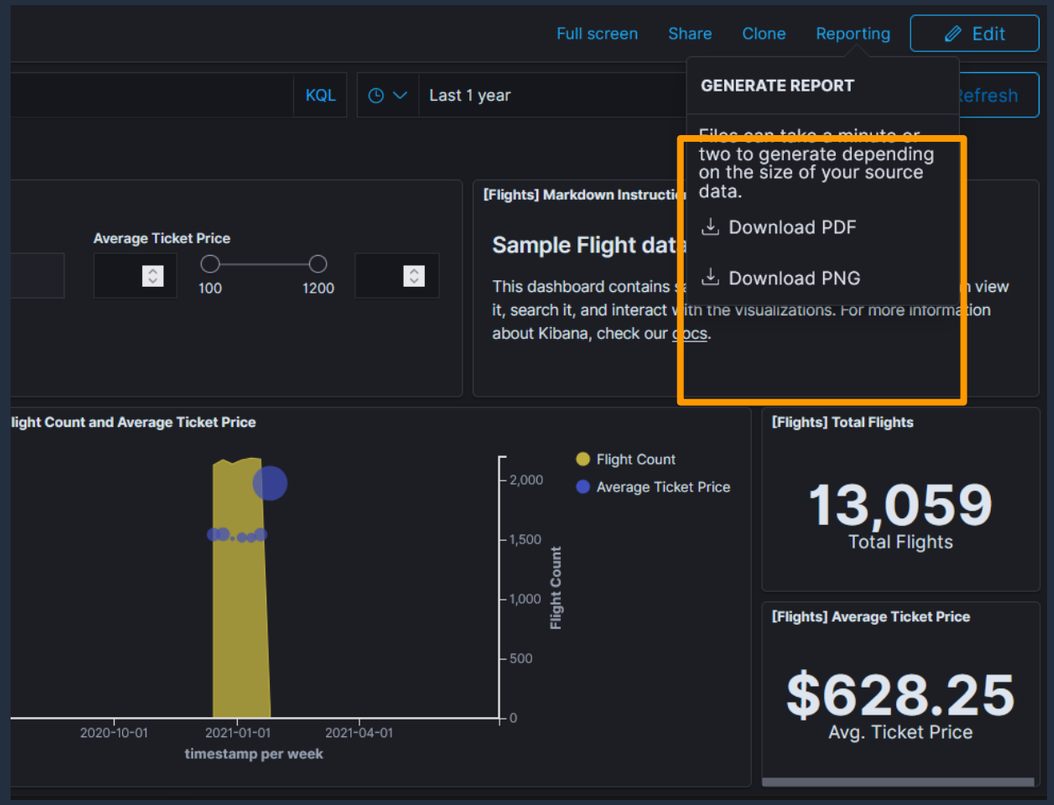
- レポートはオンデマンドもしくはスケジュールベースの生成が可能



Reporting – オンデマンドレポート

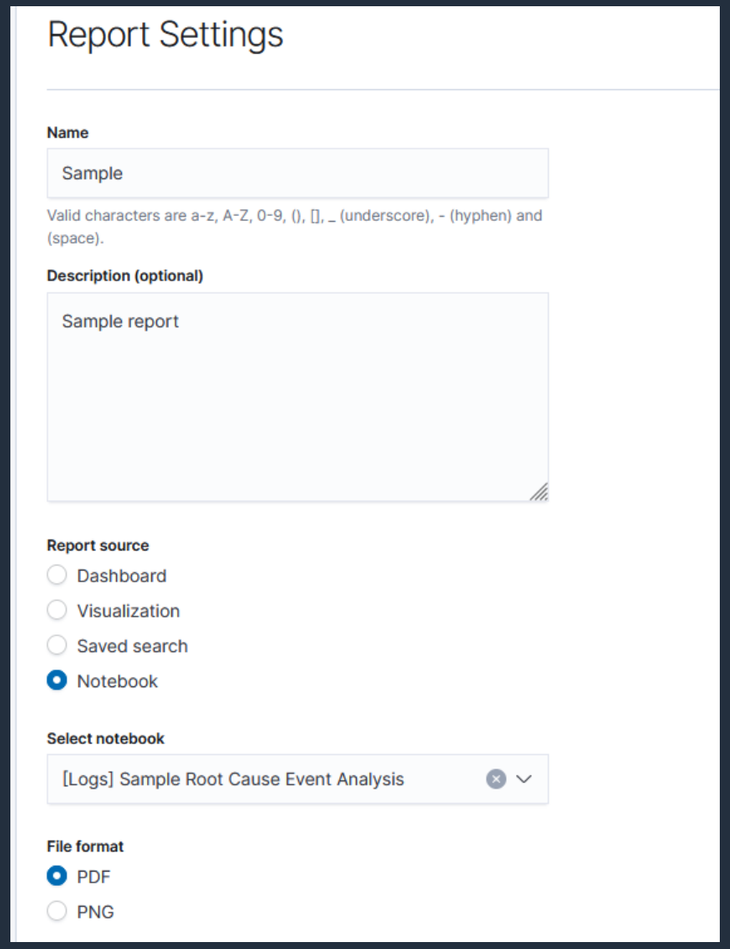
各画面から Generate CSV(PDF, PNG) を選択することで, オンデマンドレポートの生成, ダウンロードが可能

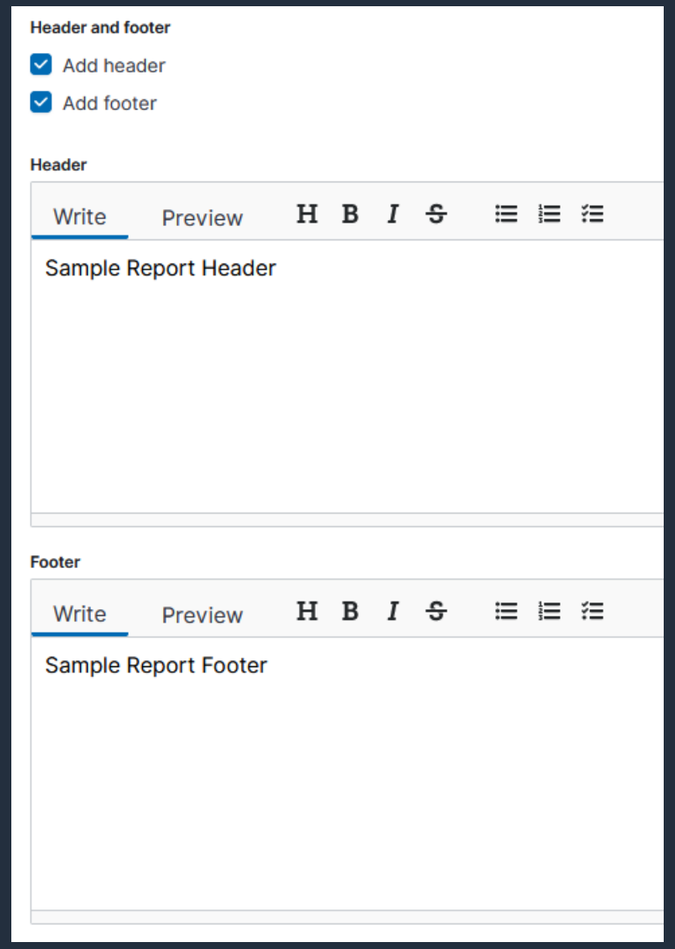


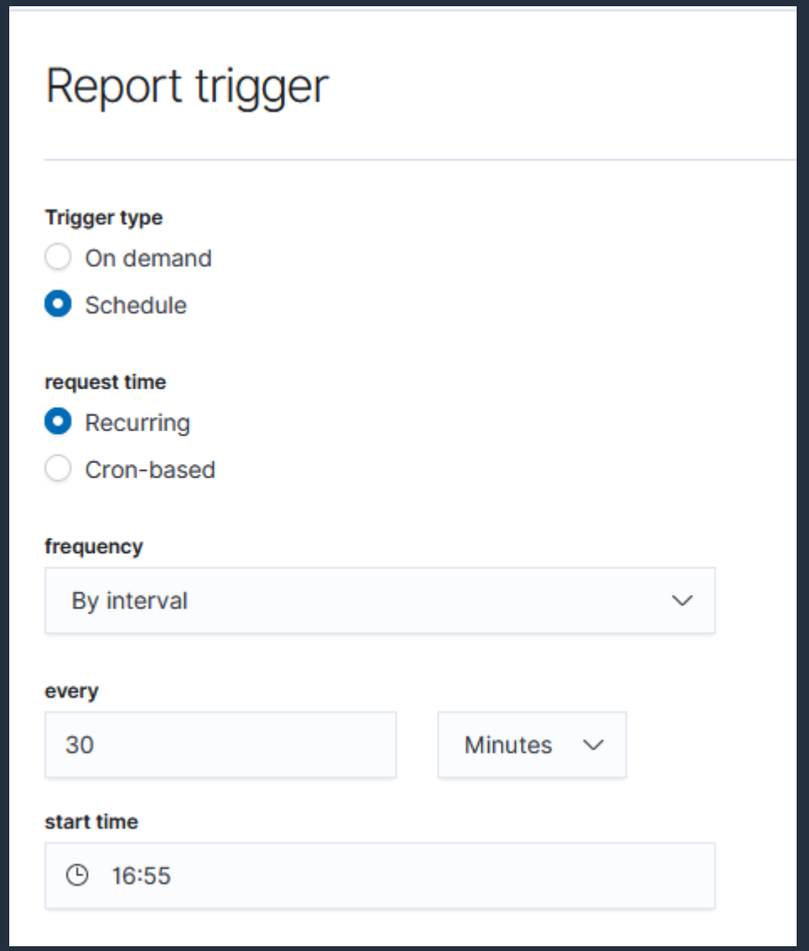


Reporting – Job によるレポートの作成

- レポートの作成時にヘッダ, フッタの指定が可能
- スケジュールベースのレポート作成をサポート







Reporting – レポートの取得

レポートは一覧画面からダウンロード可能

Reporting

Reports (1)

Refresh

Search...

Type

State

Name	Source	Type	Creation time	State	Generate
Sample	Notebook	Schedule	Wed Dec 22 2021 @ 16:56:08	Created	PDF

Rows per page: 10

1

Report definitions (1)

Refresh

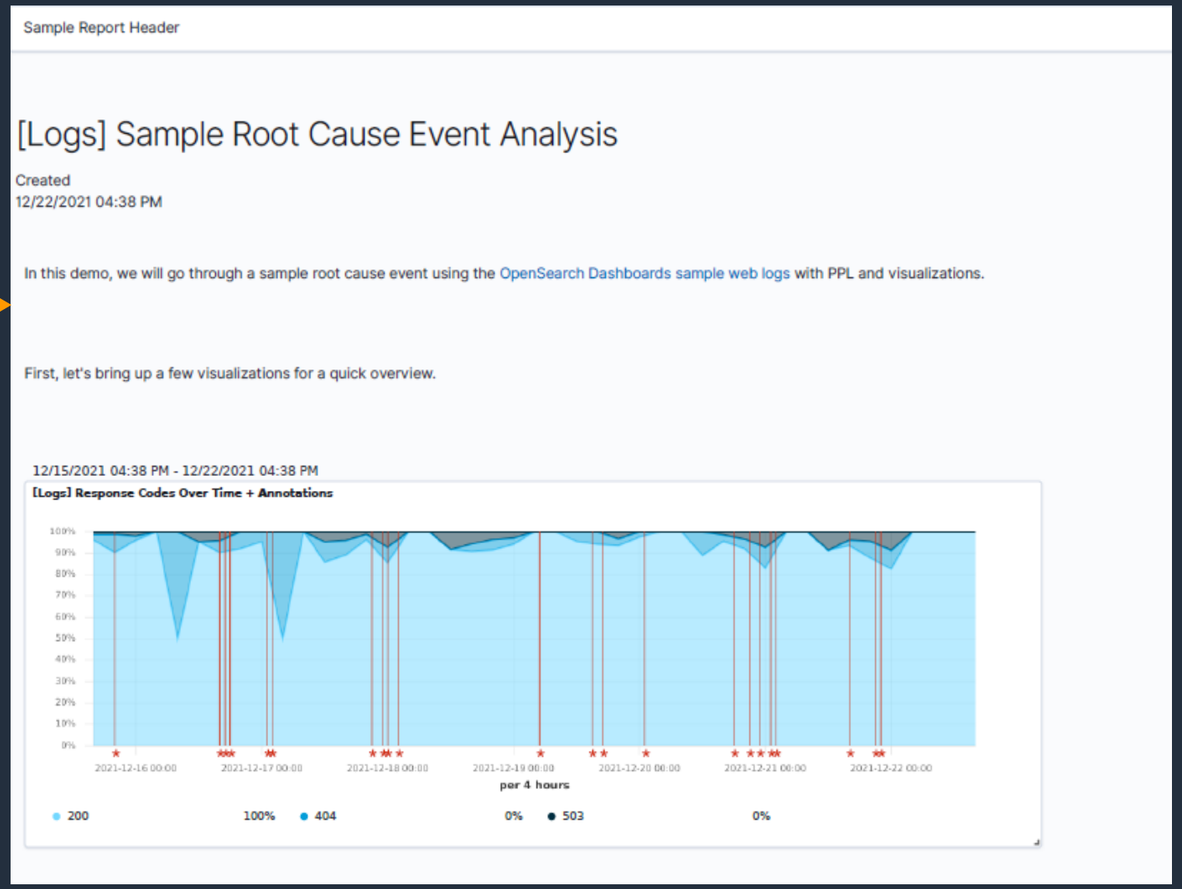
Create

Search...

Name	Source	Type	Schedule details	Last Updated	Status
Sample	Notebook	Schedule	Recurring	Wed Dec 22 2021 @ 16:55:41	Active

Rows per page: 10

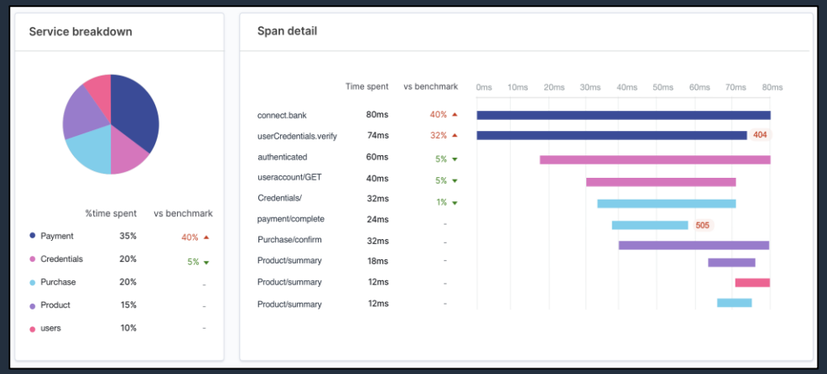
1

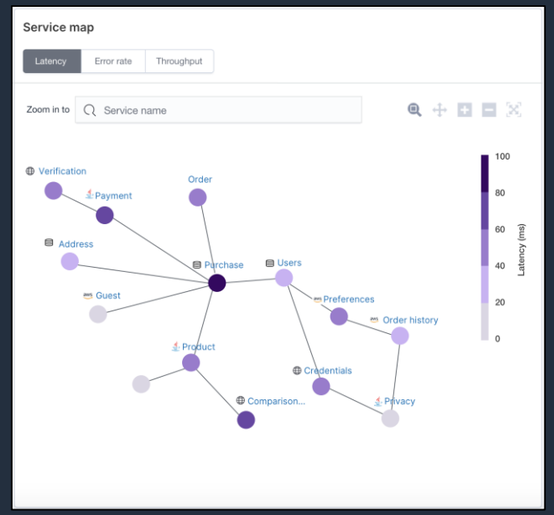


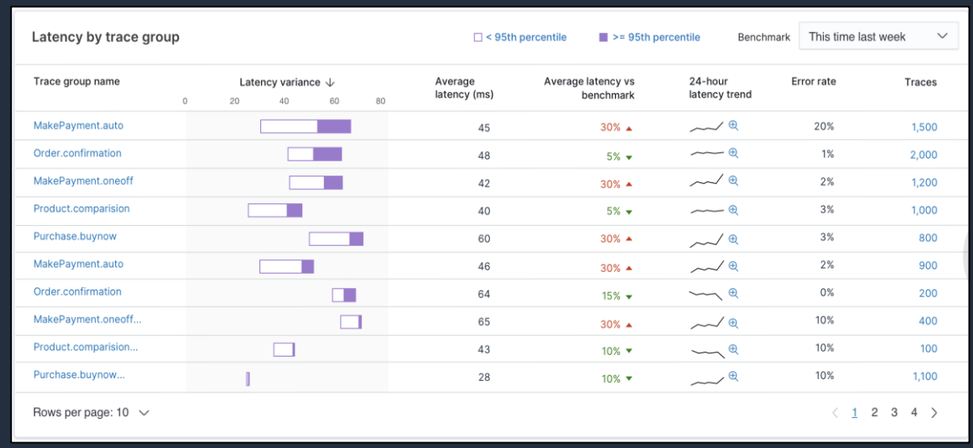
Trace Analysis

Trace Analysis

- 分散型アプリケーションのパフォーマンスや可用性上の問題を分析するためのダッシュボードを提供
- Cloud Native Computing Foundation(CNCF) プロジェクトの OpenTelemetry がサポートされる







Trace-Span Details

- Single request performance
- Diagnose root cause

Service Maps

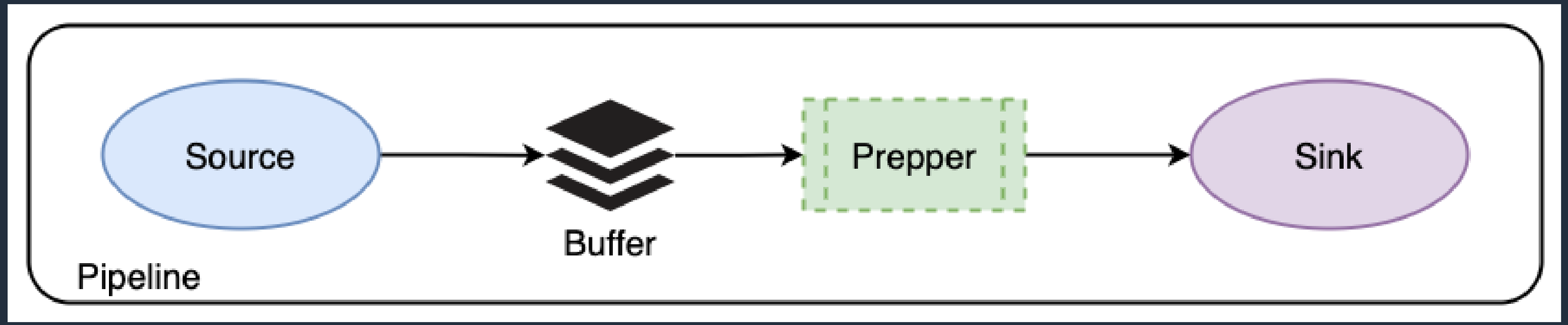
- End-to-end view
- Isolate issues to services

Trace Groups

- Monitor performance
- Identify issues early

Trace Analysis

- OpenTelemetry Collector と互換性のあるライブラリ(OpenTelemetry SDKS, X-Ray SDKs, Jaeger, zipkin, AWS Distro for OpenTelemetry 等)と統合されている
- OpenSearch プロジェクトにより提供される Data Prepper と連携することで, フィルタリングや変換などの中間処理を実施することも可能



https://opensearch.org/docs/latest/observability/data-prepper/pipelines/

Alerting 機能のアップデート

Alerting – Bucket Level Monitor

- 単一モニターで複数のモニタリング対象を一括監視
- アラート通知はモニタリング対象毎に発行される
- OpenSearch 1.1 以降で利用可能

Query Level Monitor

- 監視対象の数にかかわらず,モニター 1 つに対して通知は 1 つのみ
- 監視対象毎に個別に通知を発行する場合は, 監視対象数分のモニターが必要

Bucket Level Monitor (New!)

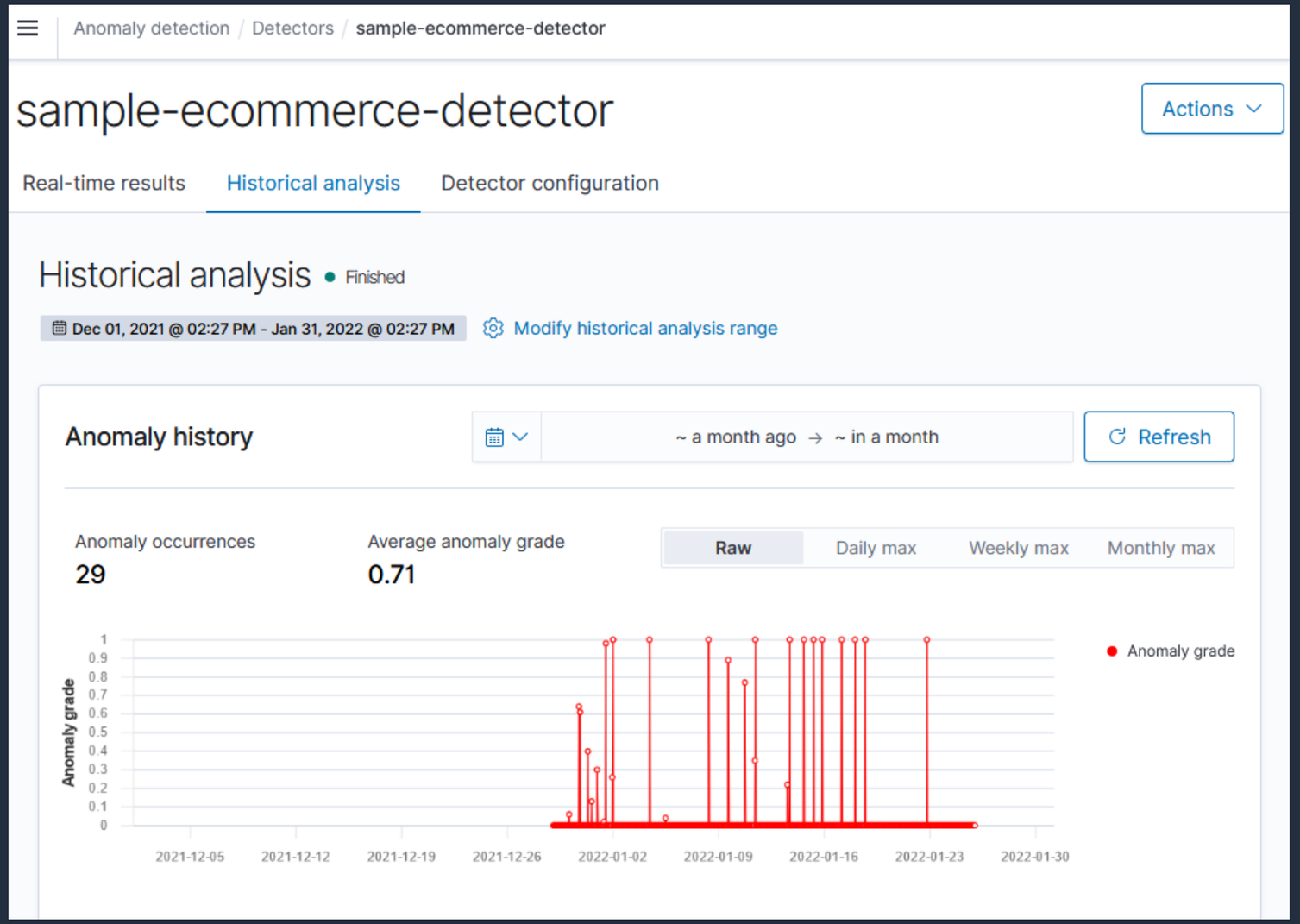
- 監視対象毎に個別に通知を発行することが可能
- 単位時間あたりの通知数に制限を設けることも可能

異常検知機能のアップデート

AWS RE:INVENT
RE:CAP

Anomaly Detection for Historical Data

- 過去データに対する異常検知をサポート
- 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. 数週間, 数か月分の分析も可能
- 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, モデルチューニングの要否判断に役立てることができる
- OpenSearch 1.1 以降で利用可能



クラスター間連携のアップデート

Cross Cluster Search

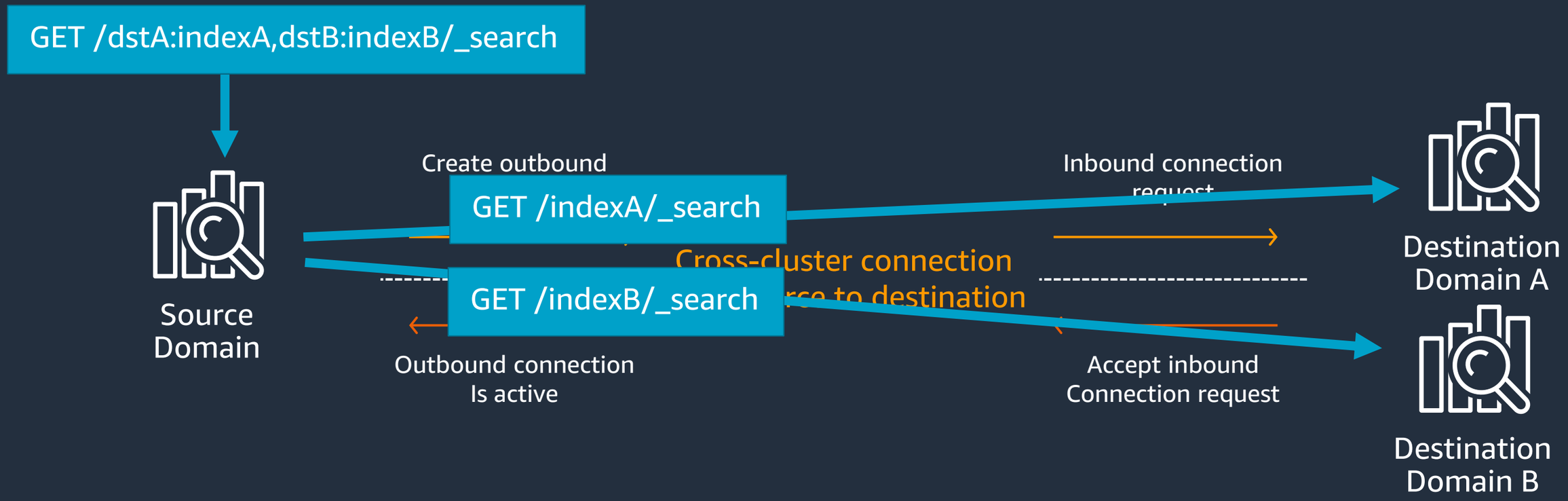
ワークロードを分離することでスケーラビリティ, リソース効率, 可用性を強化

スケーラビリティ: OpenSearch Dashboards から複数クラスターに格納されたデータを横断的に検索, 可視化

リソース利用効率の改善: 格納データ, ワークロードをドメイン毎に分離することで, 適切なリソースの割り当てが可能に

可用性の向上: 特定のワークロードによって発生する問題を隔離

セキュリティ: Fine Grained Access Control Policy によるアクセス制御が利用可能

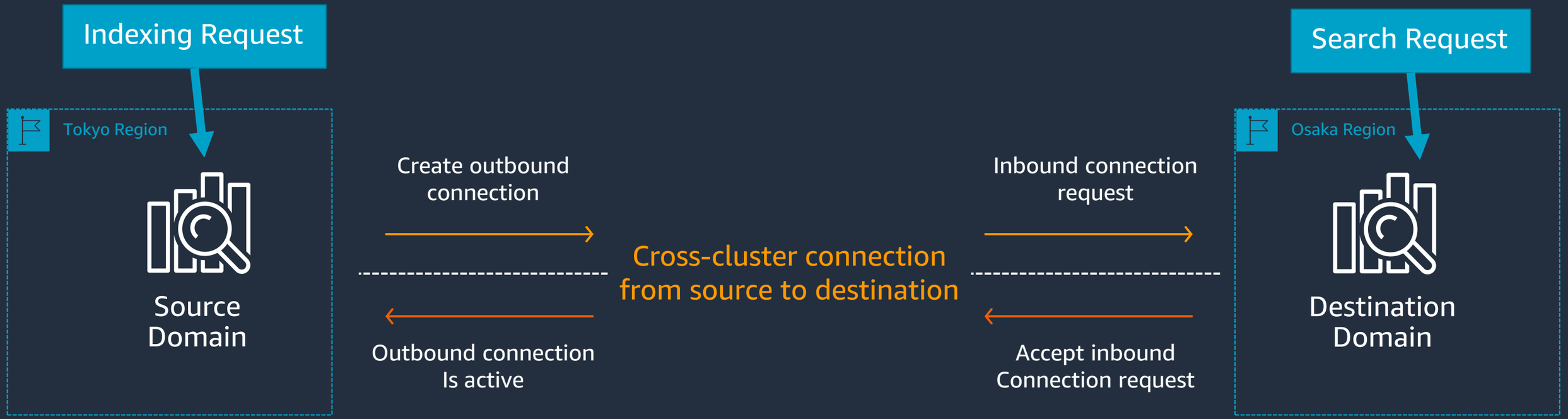


Cross Cluster Replication (New!)

Index の論理レプリケーションによるワークロードの分離, データ耐久性の向上

リソース利用効率: クラスター間でインデクシング, 検索ワークロードを分離することで, 適切なリソースの割り当てが可能に

可用性: 異なるリージョン間でレプリケーションを構築することが可能. データの継続レプリケーションもサポート



Agenda

Part 1
Amazon OpenSearch Service 概要 & Amazon OpenSearch Service への名称変更について

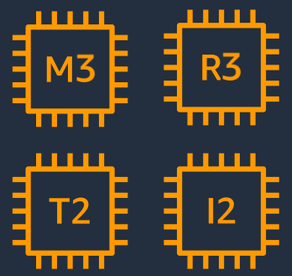
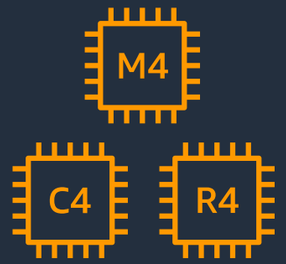
Part 2
検索, 分析, 可視化関連のアップデート

Part 3
パフォーマンス, スケーラビリティ,運用, セキュリティ関連のアップデート

パフォーマンス, スケーラビリティ関連のアップデート
- Graviton2 インスタンスサポート -

Amazon OpenSearch Service スケーラビリティの歴史

最大で 200 nodes, 3.0 PiB のスケーラビリティを提供可能

2015.10	2016.05	2017.02	2017.04	2017.12	2019.01
10 nodes 5TiB	**20 nodes** **10 TiB**	20 nodes **30 TiB**	**100 nodes** **150 TiB**	100 nodes **1.5 PiB**	**200 nodes** **3.0 PiB**
					

https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/supported-instance-types.html
https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/limits.htm

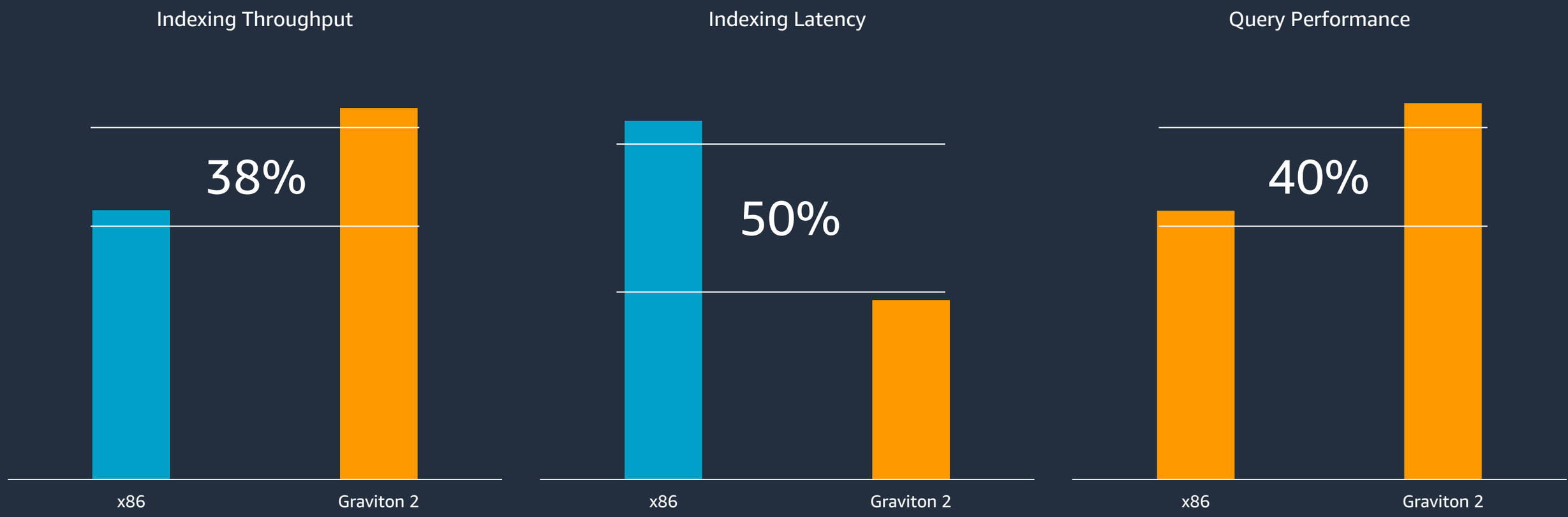
Amazon OpenSearch Service スケーラビリティの歴史

新しいインスタンスタイプについても順次対応を行っている

2019.04	2020.05	2020.11	2021.03
200 nodes 3.0 PiB	200 nodes 3.0 PiB	200 nodes 3.0 PiB	200 nodes 3.0 PiB
M5 C5 R5	ultrawarm1.medium.elasticsearch ultrawarm1.large.elasticsearch	T3	M6g R6g C6g R6gd

https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/supported-instance-types.html
https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/limits.html

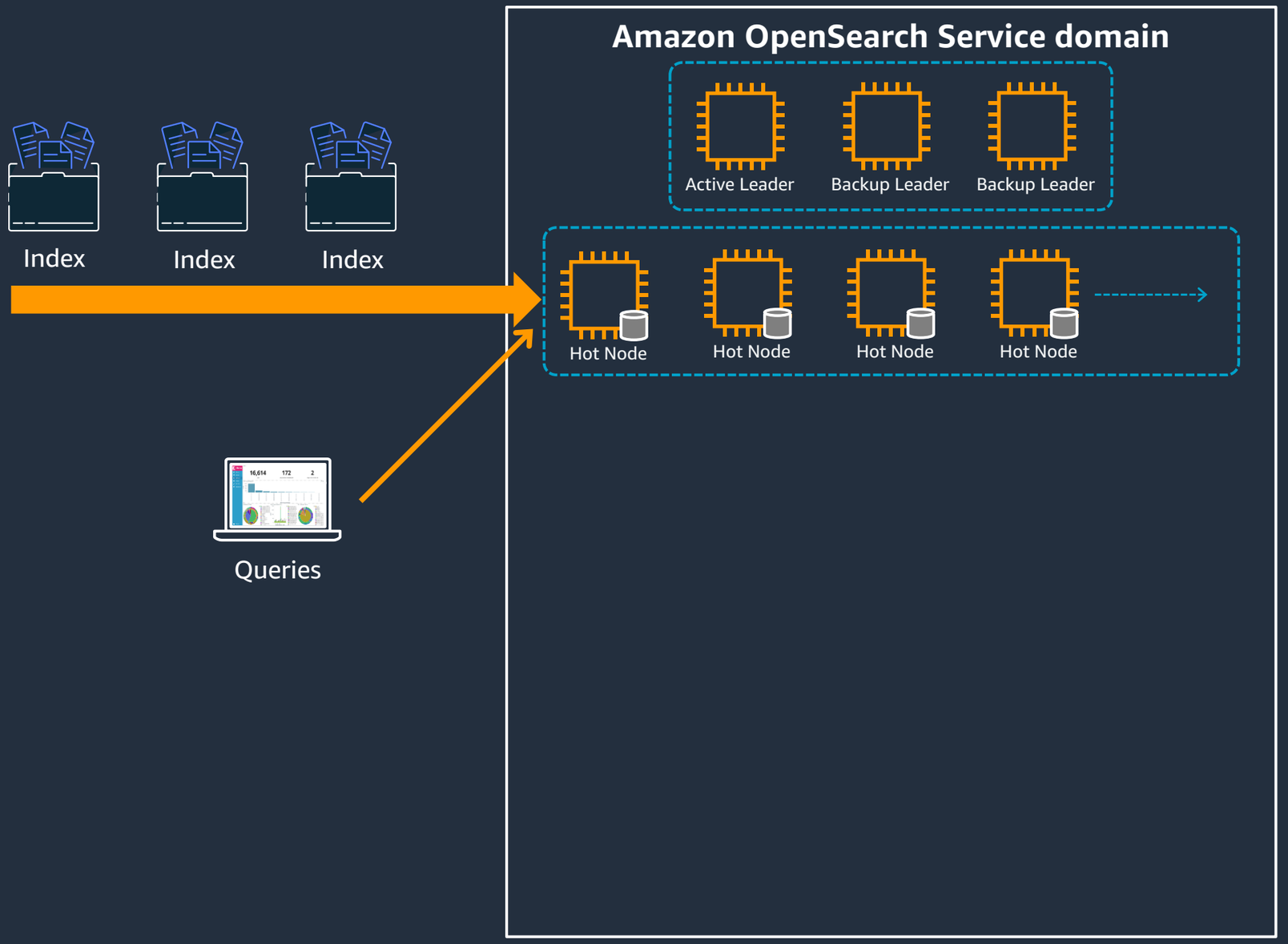
Graviton 2 搭載インスタンス



Graviton 2 搭載インスタンスは, 第五世代のインスタンスと比較して
優れたコストパフォーマンスを提供

パフォーマンス, スケーラビリティ関連のアップデート
- Cold Storage -

Amazon OpenSearch Service の階層ストレージ



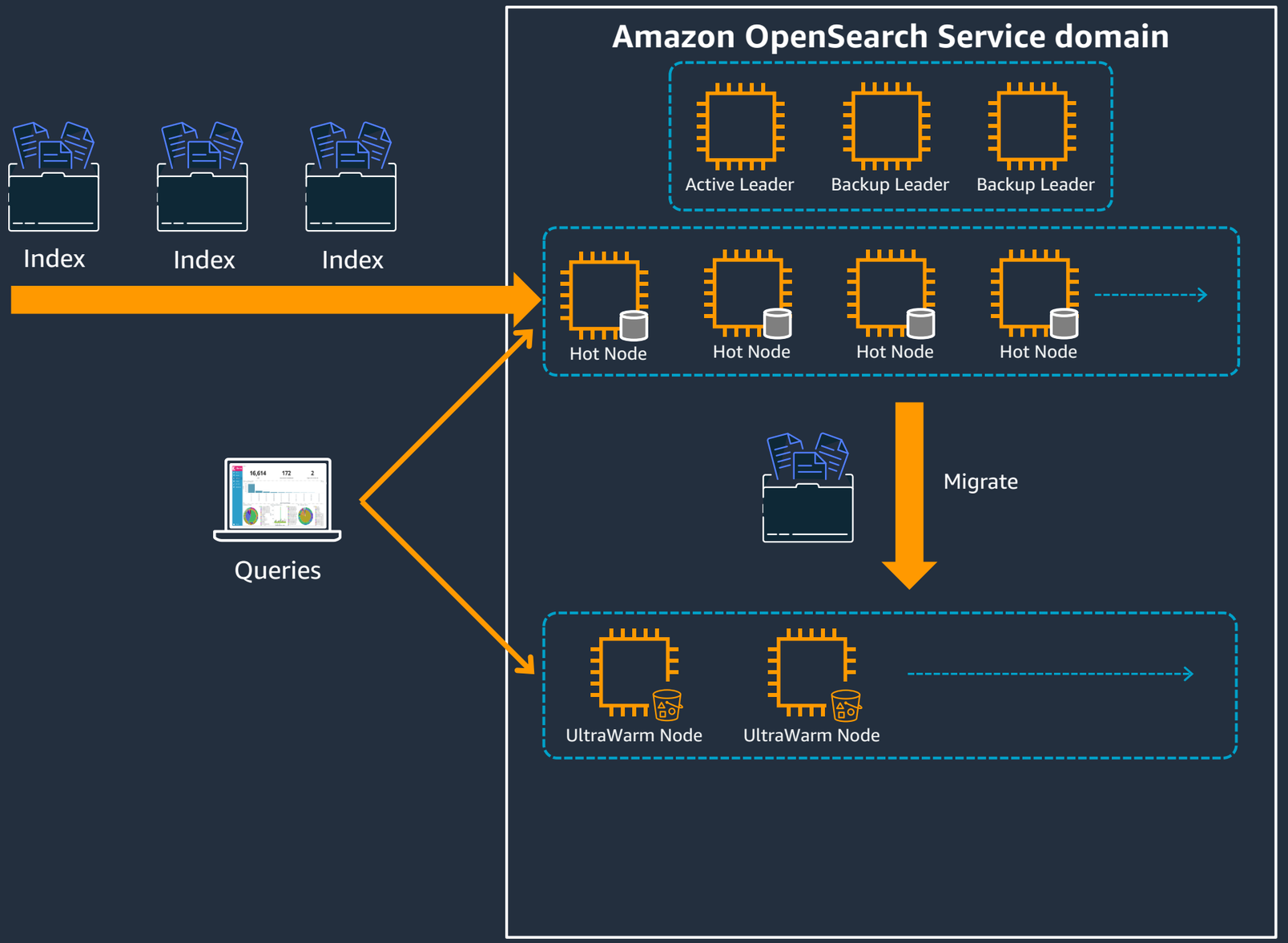
Hot Node

IOPS, レイテンシ要件に応じて EBS(gp2, io1, standard) およびインスタンスストアからストレージを選択可能

クラスターあたり最大 3 PB のストレージを割り当て可能

低レイテンシ, 高頻度なランダムアクセスが必要な用途向き

Amazon OpenSearch Service の階層ストレージ



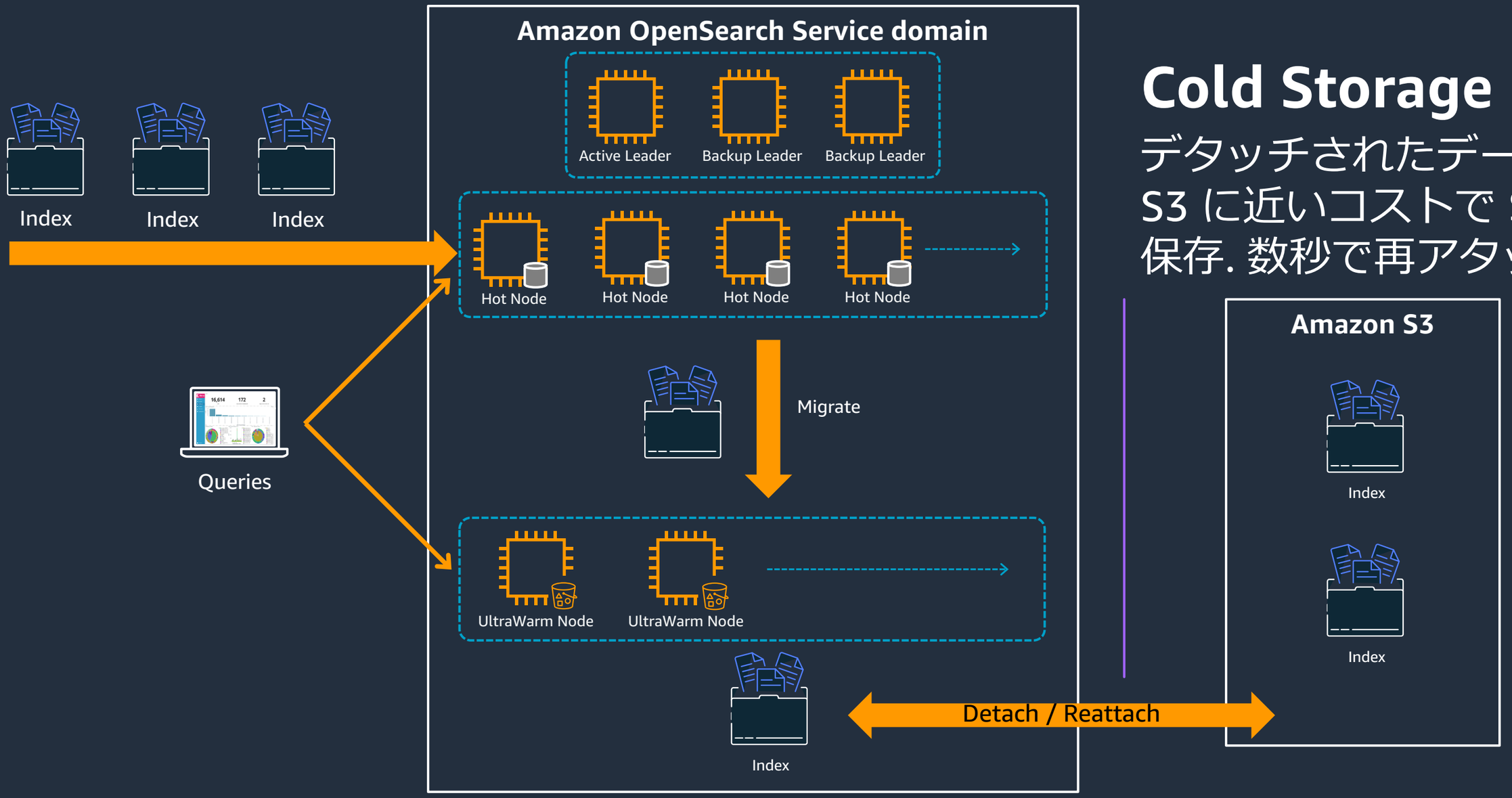
UltraWarm

全てのデータをホットストレージに格納する場合と比較して, **最大 90%** のコスト削減

データは高耐久の S3 に格納. レプリカ, ストレージオーバーヘッドを削減し, データの収容効率を向上

インタラクティブなログ分析, 可視化に利用可能

Amazon OpenSearch Service の階層ストレージ



Cold Storage

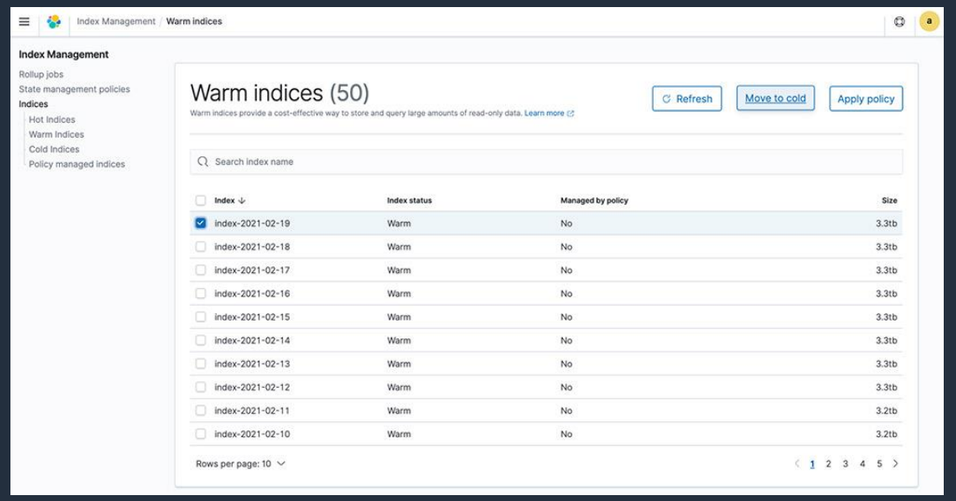
デタッチされたデータを S3 に近いコストで S3 に保存. 数秒で再アタッチ

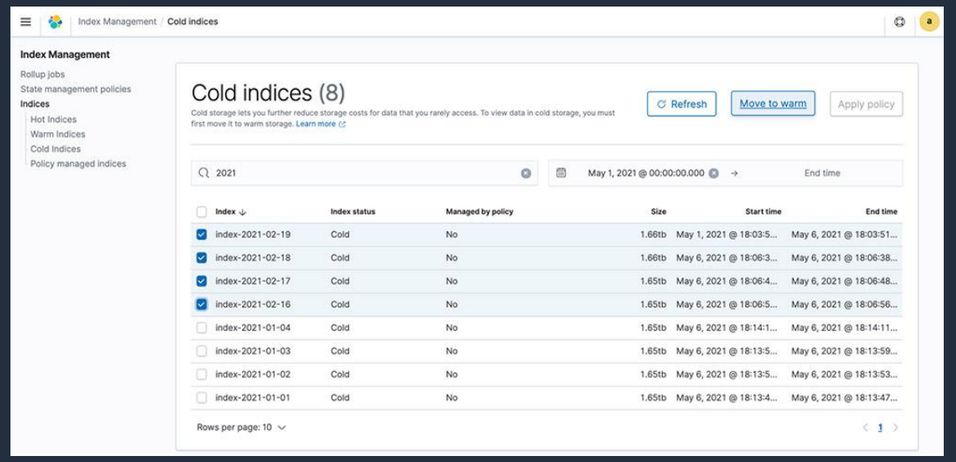
UltraWarm から Cold Storage への移動

- OpenSearch Dashboards または API による移動が可能

- ISM(Index State Management) との併用で, スケジュールベースで Cold Storage へ移動することも可能

- Cold Storage 上の Index もダッシュボードまたは API により UltraWarm へ戻すことが可能



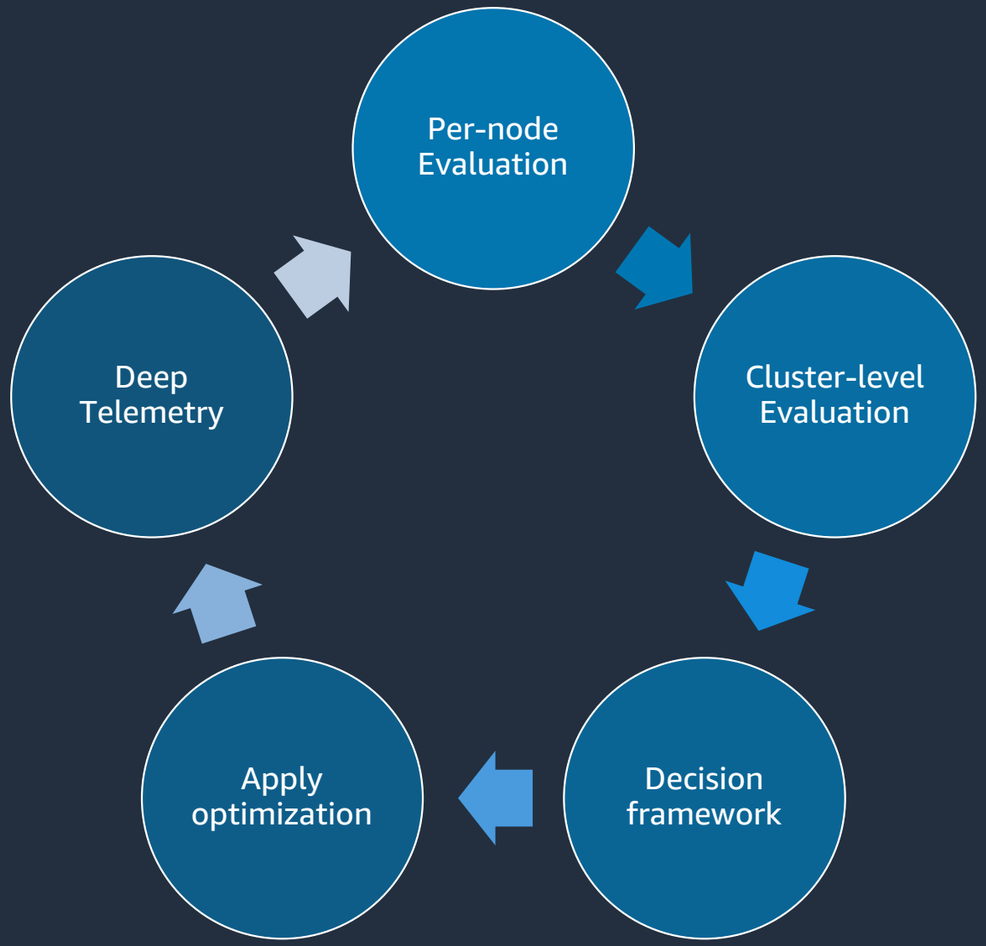


https://aws.amazon.com/blogs/big-data/introducing-cold-storage-for-amazon-elasticsearch-service/

パフォーマンス, スケーラビリティ関連のアップデート
- Auto-Tune -

Auto-Tune

OpenSearch の Performance Analyzer をベースとした自動チューニング機能



メンテナンスウィンドウで Blue/Green デプロイにより反映

JVM Settings

- ヒープサイズ(最大 128 GiB まで増加)
- GC (CMS から G1GC への変更 *1)
- Young 領域のサイズ

オンラインで即時反映

Cache (即時反映)

- キャッシュクリア
- Field data cache サイズ
- Shard request cache サイズ

Queue (即時反映)

- Search queue
- Write queue

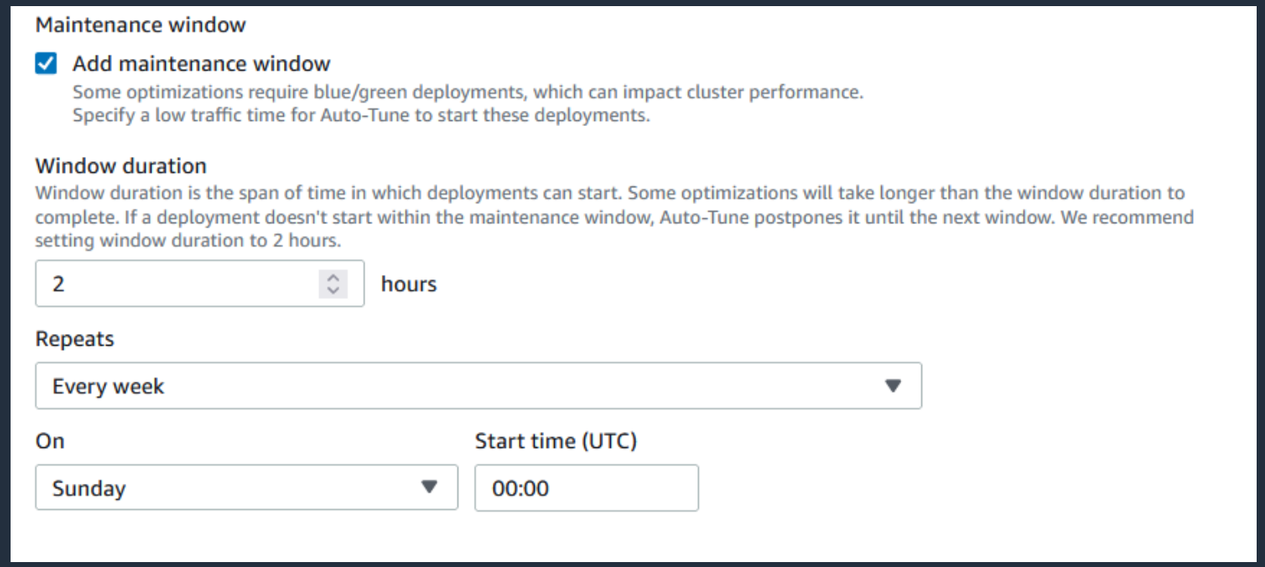
*1 Graviton2 搭載インスタンスはデフォルトで G1GC

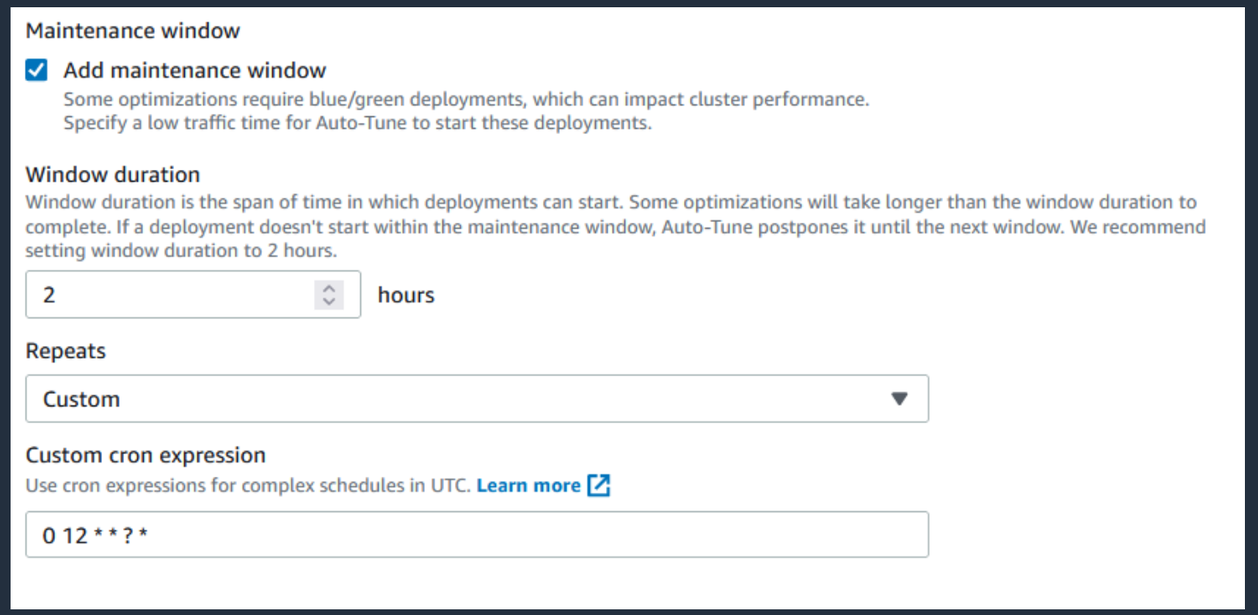
Auto-Tune – メンテナンスウィンドウ

- JVM Settings のチューニングを有効化するにはメンテナンスウィンドウを設定する必要あり

- ウィンドウは曜日と時間ベース, cron ベースの 2 通りをサポート. タイムゾーンは UTC

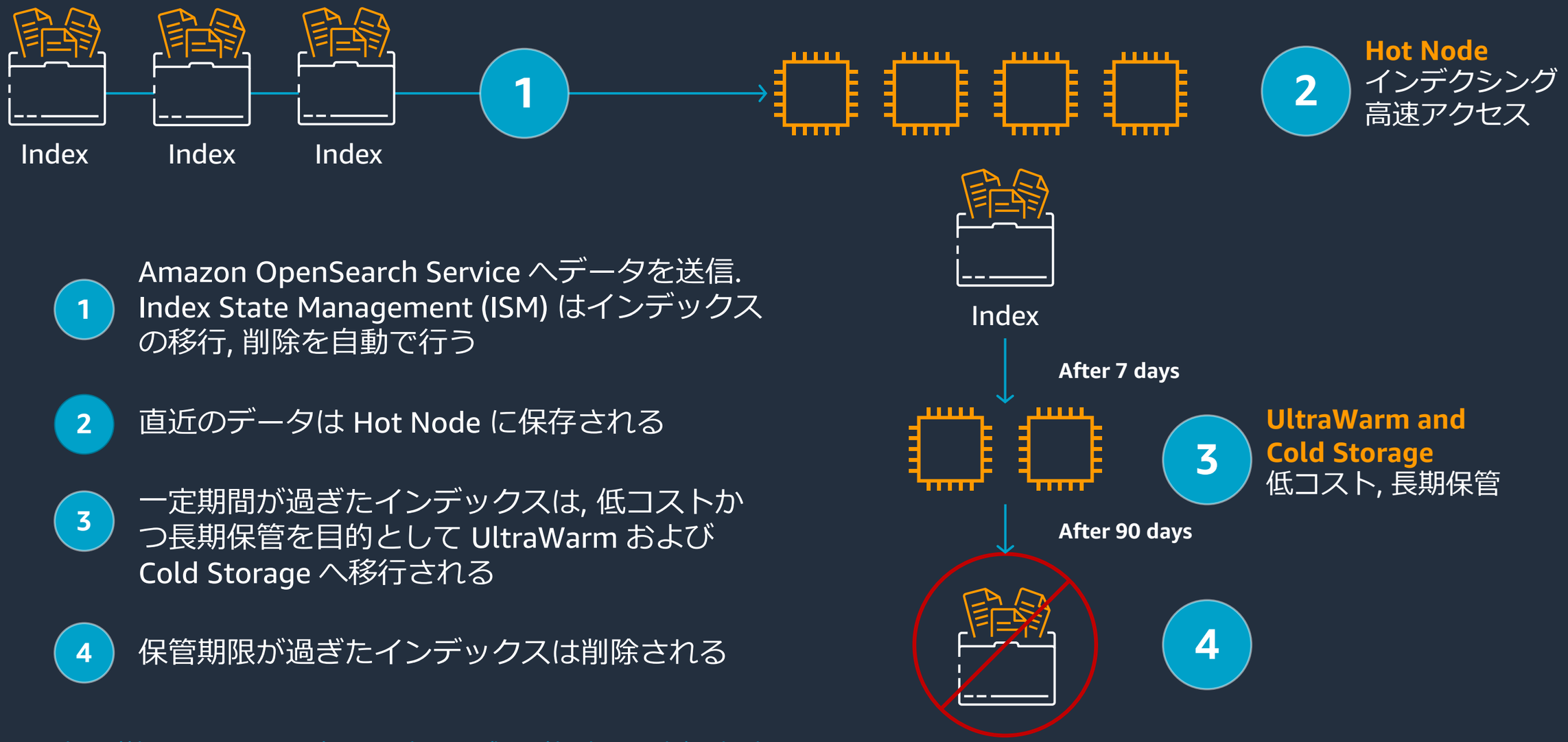
- メンテナンスウィンドウ中に Blue/Green デプロイが実行される. オンラインで処理されるためクラスターの停止は発生しない





運用関連のアップデート
- Index State Management Policy -

Index State Management によるライフサイクル管理



1. Amazon OpenSearch Service へデータを送信. Index State Management (ISM) はインデックスの移行, 削除を自動で行う
2. 直近のデータは Hot Node に保存される
3. 一定期間が過ぎたインデックスは, 低コストかつ長期保管を目的として UltraWarm および Cold Storage へ移行される
4. 保管期限が過ぎたインデックスは削除される

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/ism.html

ISM ポリシー

- JSON 形式で記述

- ism_template 要素内に Index パターンを記載することで, 新規に作成される Index に自動的にポリシーを適用することが可能 (New!)

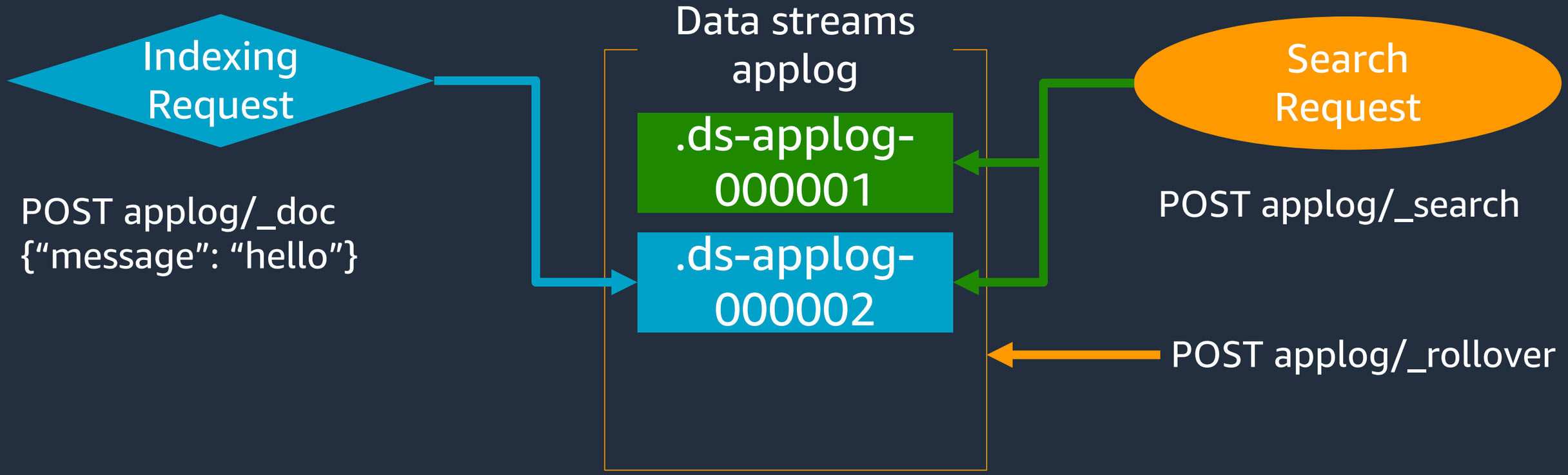
- Action では Storage Tier の移動の他, Snapshot の取得や Replica 数の変更, Rollover による Index のローテーションなど様々なオペレーションを指定可能

```
{
 "policy": {
  "description": "Demonstrate a hot-warm-cold-delete workflow.",
  "default_state": "hot",
  "schema_version": 1,
  "ism_template": { "index_patterns": ["log*"], "priority": 100 }
  "states": [ {
     "name": "hot",
     "actions": [],
     "transitions": [ { "state_name": "warm", "conditions": { "min_index_age": “7d" } } ]
   },
   {
     "name": "warm",
     "actions": [ { "warm_migration": {}, "retry": { "count": 5, "delay": "1h" } } ],
     "transitions": [ { "state_name": "cold", "conditions": { "min_index_age": “30d" } } ]
   },
   {
     "name": "cold",
     "actions": [{ "cold_migration":  { "timestamp_field": "@timestamp" } } ],
     "transitions": [ { "state_name": "delete", "conditions": { "min_index_age": “90d" } } ]
   },
   {
     "name": "delete",
     "actions": [ { "cold_delete": {} } ]
   }
 ] }
}
```

運用関連のアップデート
- Data Streams -

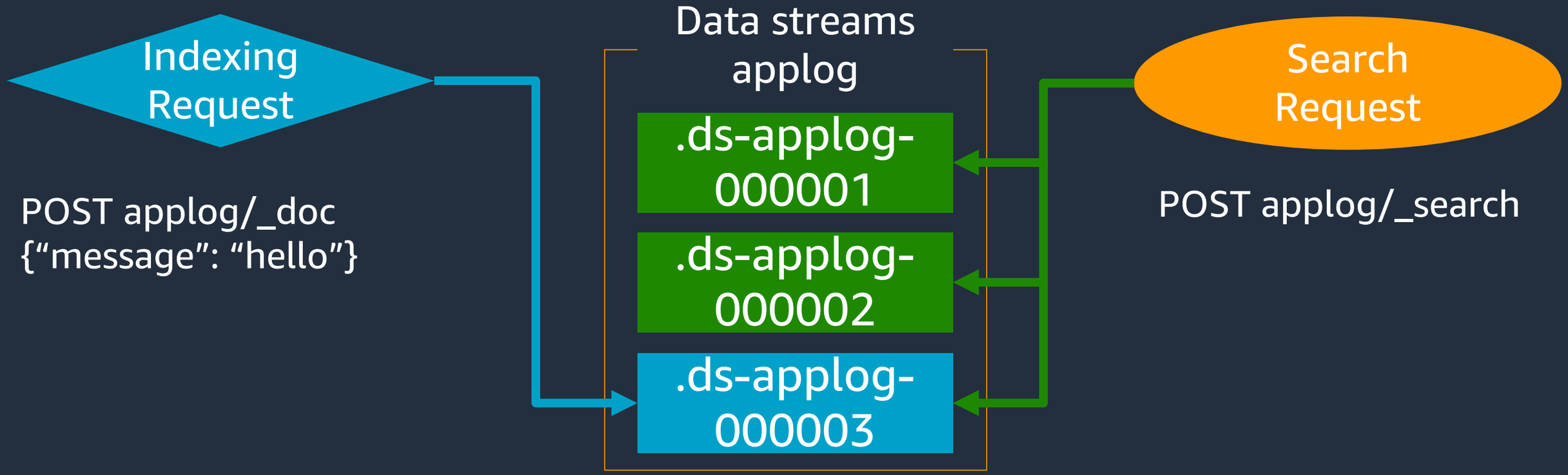
Data streams

- 複数の Index をあたかも一つの Index として見せることのできる機能
- Data stream は内部的に複数の Index で構成されており, 検索は全ての Index に対して, 書き込みは一つの Index に対して行われる
- 書き込み先の Index はローテーション可能であり, ログの蓄積による肥大化を防止する
- Index State Management 経由のローテーションもサポート



Data streams

- 複数の Index をあたかも一つの Index として見せることのできる機能
- Data stream は内部的に複数の Index で構成されており, 検索は全ての Index に対して, 書き込みは一つの Index に対して行われる
- 書き込み先の Index はローテーション可能であり, ログの蓄積による肥大化を防止する
- Index State Management 経由のローテーションもサポート

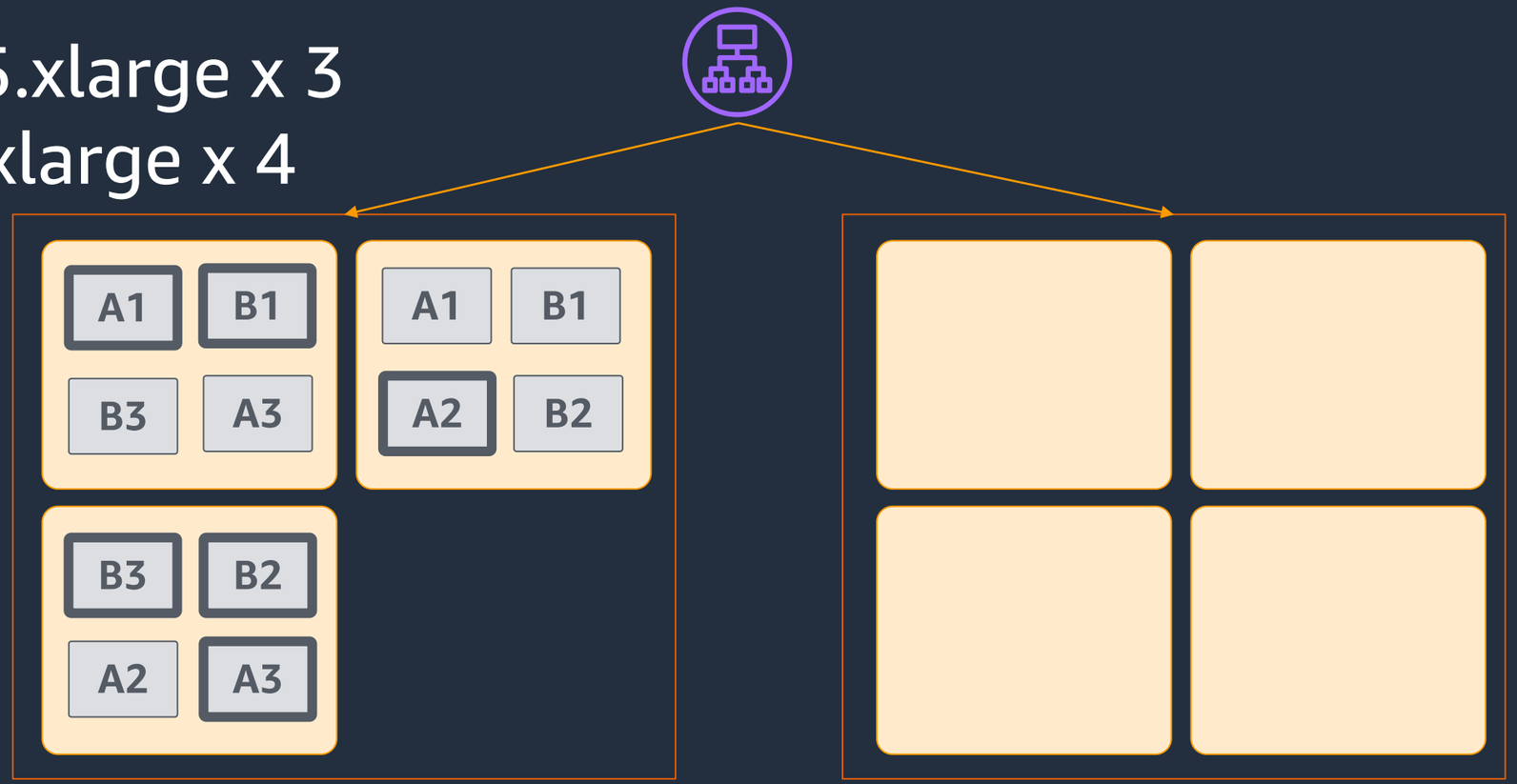


運用関連のアップデート
- 設定変更時の Dry Run -

構成変更, 設定変更時の挙動

- 設定変更, 構成変更はオンラインで行われる
- 構成変更が実行されると, ノード間でデータの移動が行われる. データの移動が完了するとトラフィックが切り替えられる (blue/green deployment)
- 移動はノード間で直接行われるため負荷がかかる. オフピーク帯での実行を推奨

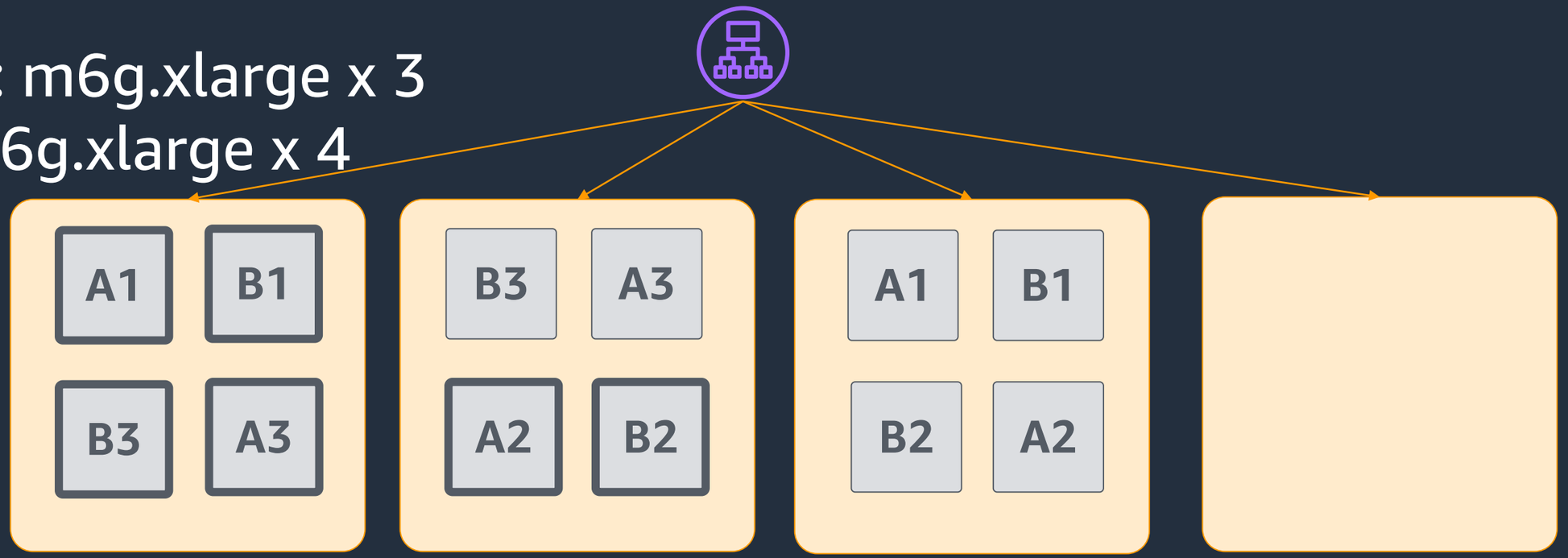
from: m5.xlarge x 3
to: m6g.xlarge x 4



構成変更, 設定変更時の挙動

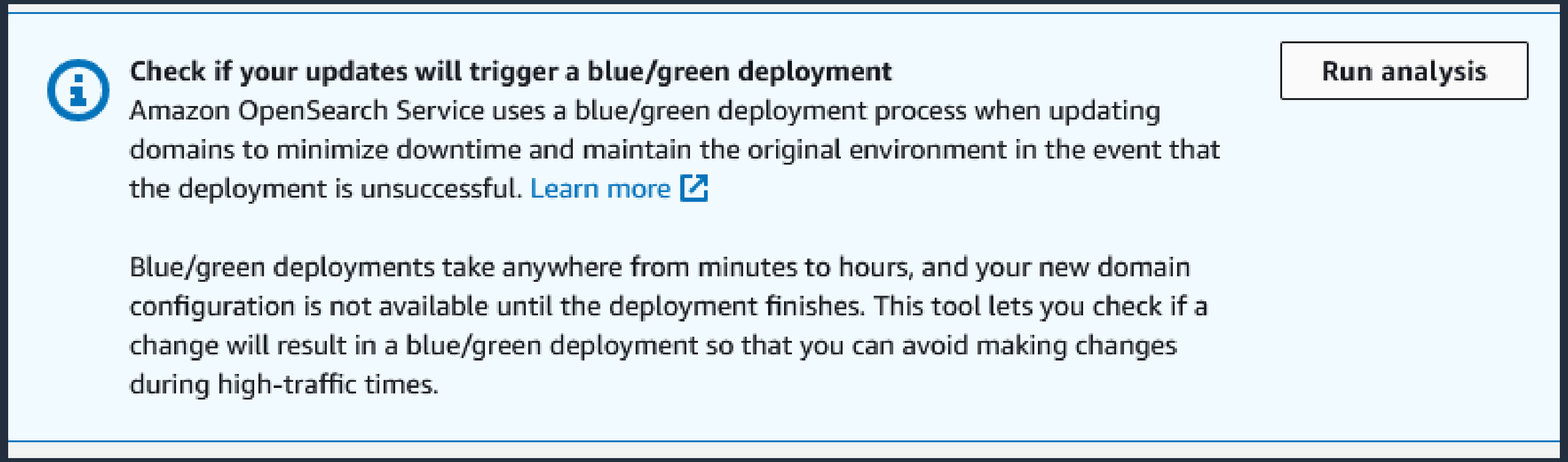
- 同一インスタンスタイプでデータノードおよび UltraWarm ノードの台数のみを変更する場合, blue/green deployment 無しでノードの増減が可能(専用マスターノードが存在することが前提)
- Blue/green deployment ほどの規模ではないが, ノード追加時のシャードリバランスは発生する

from: m6g.xlarge x 3
to: m6g.xlarge x 4



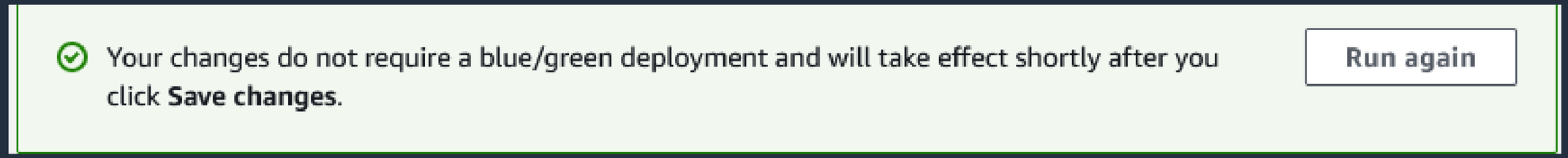
構成変更における DryRun 機能

- 2021 年 11 月より, コンソールおよび UpdateDomainConfig の DryRun オプションにて, blue/green deployment が発生するかを事前に検証可能になった
- Amazon OpenSearch Service では, 大半の設定変更によって blue/green deployment と呼ばれるノードの入れ替え処理が発生する
- DryRun オプションの追加により, 構成変更をオフピーク時間帯に実行するべきかの判断を行うことが可能になった



構成変更における DryRun 機能

blue/green deployment が発生しない場合のチェック結果例



blue/green deployment が発生する場合のチェック結果例

運用関連のアップデート
- Shard メトリクスの追加 -

メトリクス

CloudWatch と連携したモニタリング用メトリクスを提供. 大きく分けて 以下 3 レベルのメトリクスが提供されている

Cluster メトリクス

- Cluster 全体の状態, 傾向を把握するためのメトリクス

Node メトリクス

- CPU 使用率など, 個々のノードのパフォーマンスを把握するためのメトリクス

Shard メトリクス(New!)

- ノードごとの Shard 数など, 負荷の偏りなどのトラブル対応に利用可能なメトリクス

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-cloudwatchmetrics.html

シャード関連のメトリクス

- Node メトリクスにも Shard 数をカウントするメトリクスが追加されている. 現時点では, Shard メトリクスが提供する ShardCount より有用なものが多い

名称	説明	メトリクスタイプ
Shards.active	Active シャード数. ヒープ領域 1 GiB につき 20 – 25 シャードであることが推奨	Node
Shards.unassigned	Unassigned シャード数. マルチノード構成で 1 つ以上の Unassigned シャードが存在する場合は要調査・対応	Node
Shards.delayedUnassigned	割り当てが遅延しているシャードの数. 本メトリクスが継続的に 1 以上を記録している場合は要調査・対応	Node
Shards.activePrimary	Active シャードの中でも Primary シャードのみの数	Node
Shards.initializing	割り当て中のシャード数	Node
Shards.relocating	ノード間で移動されているシャードの数. 構成変更の所要時間計測などにも役立つ他, 構成変更処理がスタックしているように見える際の調査にも有用	Node
ShardCount	Primary, Replica の Shard 数を計測する際に利用する	Shard

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-cloudwatchmetrics.html

セキュリティ関連のアップデート
- 暗号化機能に関するアップデート -

暗号化

保管時のデータ暗号化

- ドメイン作成時に, 以下のデータに対する暗号化の有無を指定可能．有効化した場合，AWS KMS の暗号化キーが使用される
  - ノードに格納されているデータ(インデックス, ログ, スワップファイル,アプリケーションディレクトリのその他全てのデータ)
  - UltraWarm ストレージ上に格納されているインデックス
  - S3 上に格納されている**自動**スナップショット
- 以下のリソースは暗号化の対象外
  - S3 上に格納される**手動**スナップショット(S3 の Server Side Encryption で対応可能)
  - CloudWatch Logs に配信されるスローログ, エラーログ, 監査ログ (CloudWatch Logs の保管時データ暗号化機能で対応可能)
- **ドメイン作成後に, ノード間の通信暗号化を有効化することも可能**
  - **暗号化を有効から無効に変更することは不可**

2021 年のアップデートで対応

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/encryption-at-rest.html

暗号化

ノード間転送時のデータ暗号化

- ドメイン作成時に, ノード間の通信について暗号化の有無を指定可能
- ドメイン作成後に, ノード間の通信暗号化を有効化することも可能
  - 暗号化を有効から無効に変更することは不可

2021 年のアップデートで対応

クライアント – ドメイン間通信の暗号化

- ドメインへのアクセスにおいて HTTPS を必須とするか, HTTP も許可するかを指定可能
- 以下 2 つのポリシーを利用可能
  - Policy-Min-TLS-1-0-2019-07: TLS v1.0 およびそれ以降をサポート (デフォルト)
  - Policy-Min-TLS-1-2-2019-07: TLS v1.2 をサポート

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/ntn.html
https://docs.aws.amazon.com/opensearch-service/latest/developerguide/infrastructure-security.html

セキュリティ関連のアップデート
- Fine-Grained Access Control に関するアップデート -

Fine-Grained Access Control

ドメインアクセスに対する詳細なアクセス管理

- ドメイン作成時に，詳細なアクセス権限管理の有効 / 無効を設定可能
- ドメイン作成後に有効化することも可能
  - 有効化後の無効化は不可

2022 年のアップデートで対応

- ダッシュボードログイン時のユーザーディレクトリに下記 3 つのいずれかを指定可能
  - -内部ストア(ID+パスワード)
  - -Amazon Cognito 連携による IAM 制御
  - -SAML 認証に対応した ID プロバイダー

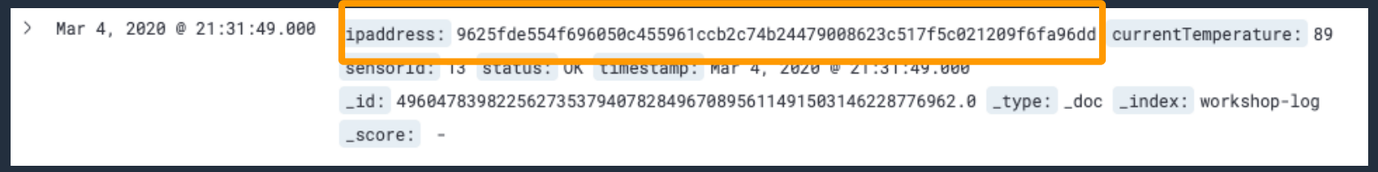
- Fine-Grained Access Control が有効化されている場合, アプリケーションから Direct API にアクセスする場合は IAM Role に対して権限を付与するか, ID+パスワードをリクエストに含める必要が有る

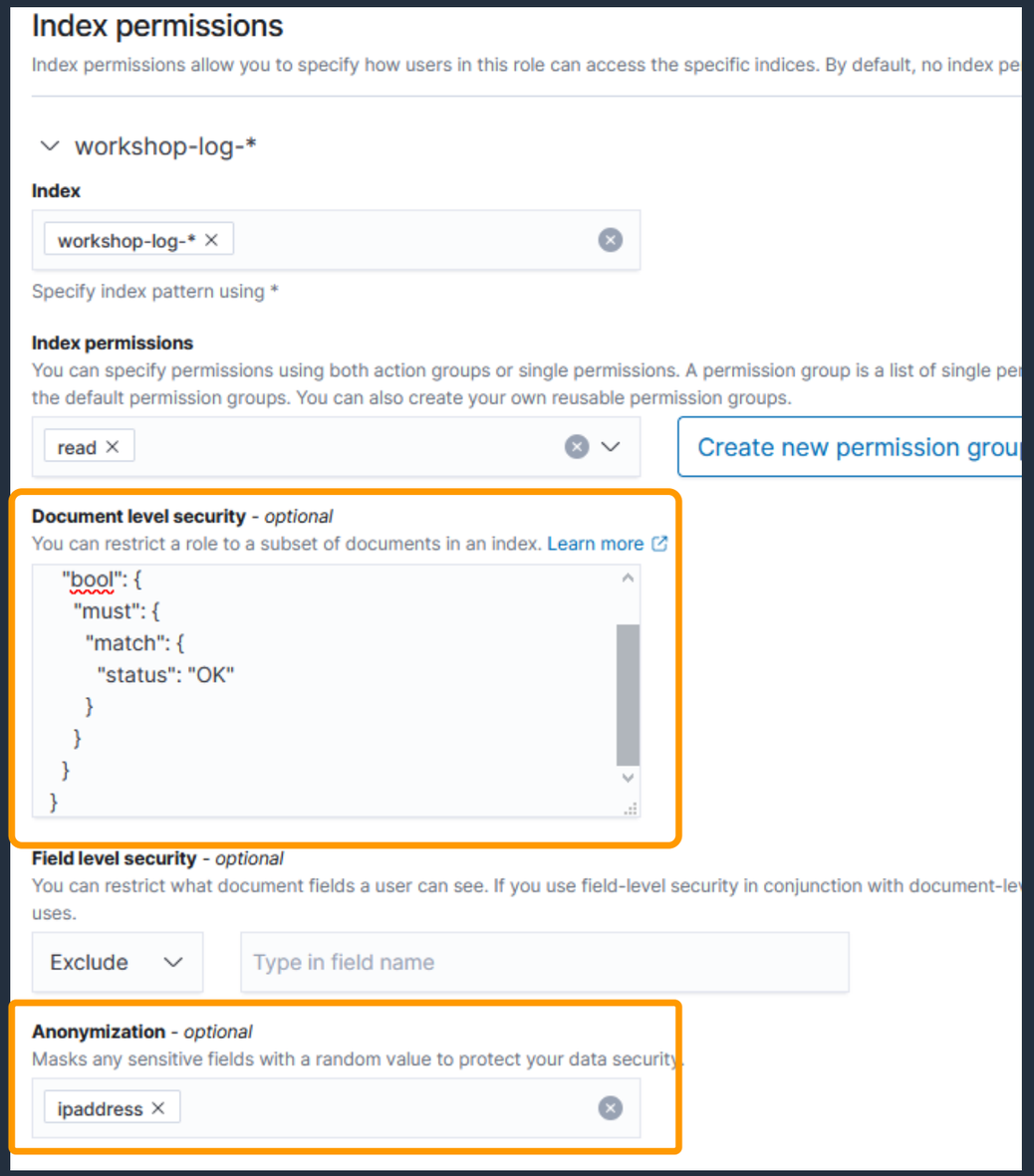
https://docs.aws.amazon.com/opensearch-service/latest/developerguide/fgac.html

Fine-Grained Access Control

ドメイン内リソースに対する詳細な権限管理

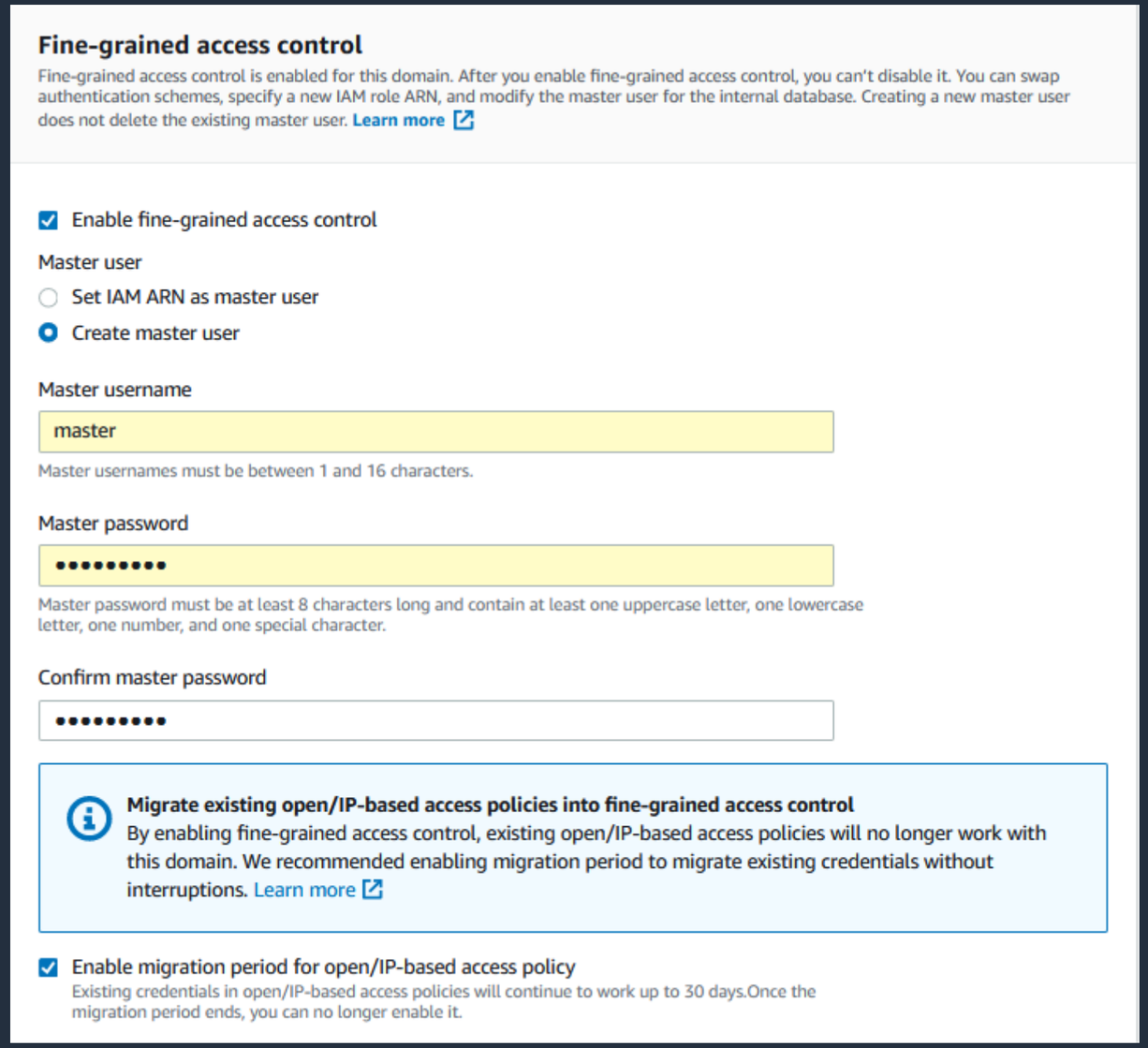
- 複数レベルでのアクセス権限管理が可能
  - -インデックスレベル
  - -ドキュメントレベル
  - -フィールドレベル
- プリセットの権限セットも多数
  - -cluster_monitor
  - -kibana_all_read
  - -manage_snapshots etc...
- フィールドのマスキングにも対応





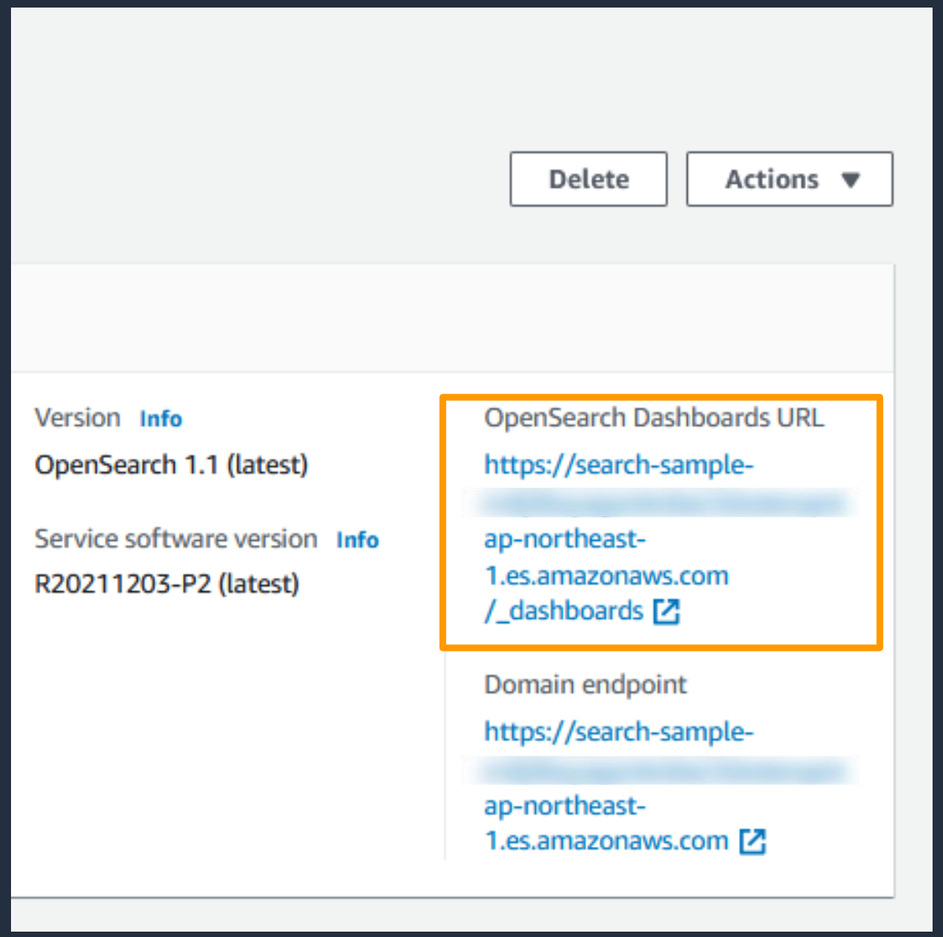
既存ドメインの FGAC 有効化 - 猶予期間

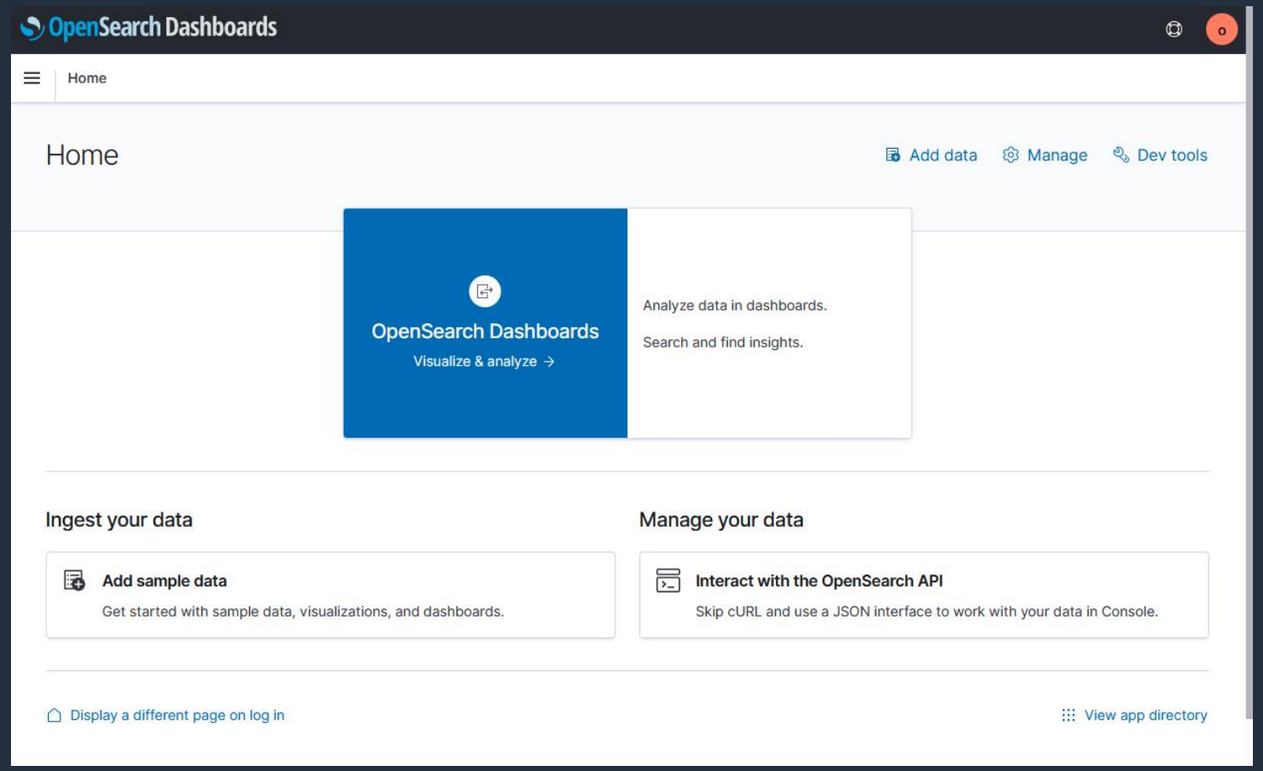
- 既存ドメインの FGAC を有効化する際, 猶予期間を設定可能
- 猶予期間中は, オープンアクセスポリシー(Public ドメインでの利用は非推奨) もしくは IP ベースのアクセスポリシーで許可された通信については認証がバイパスされる
- 利用者は猶予期間中に, FGAC 設定の追加やテストを行うことができる
- 猶予期間は 30 日間(固定). 猶予期間が満了すると, IP ベースのアクセスポリシーで許可されていた通信についても認証が要求されるようになる



既存ドメインの FGAC 有効化 – ダッシュボードアクセス

IP ベースのアクセスポリシーで許可された IP アドレスから OpenSearch Dashboards の URL へアクセスすると, 認証無しでダッシュボードが表示される

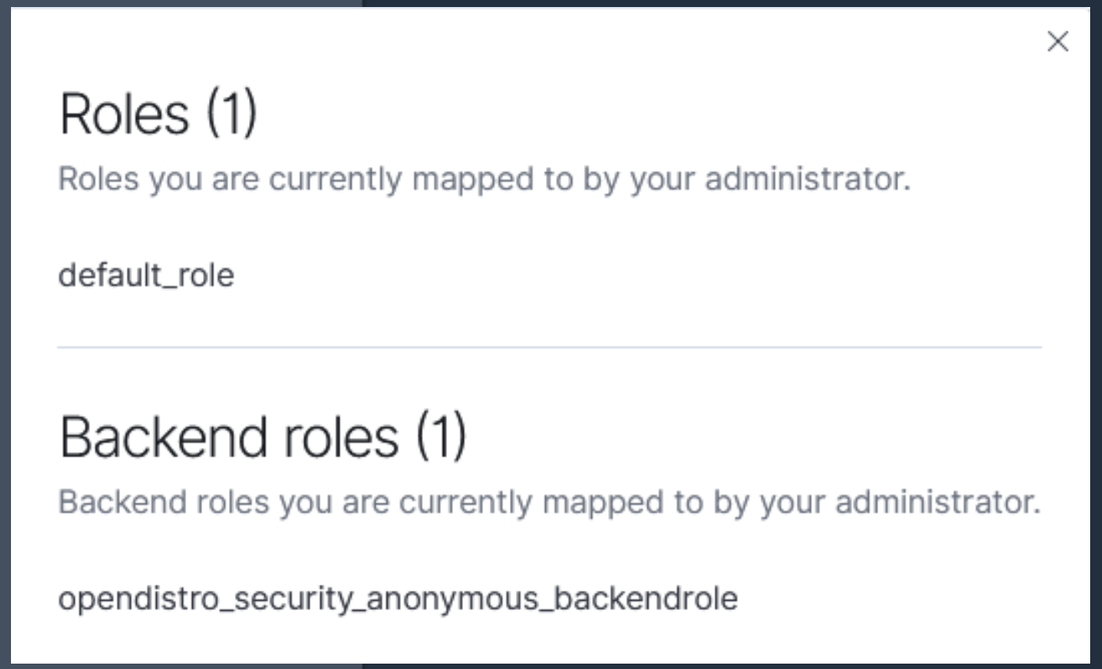




匿名ユーザーの権限

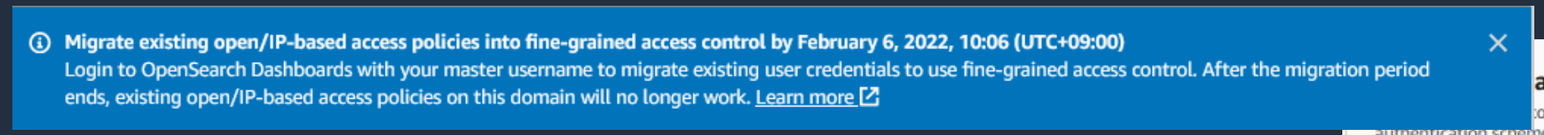
- 猶予期間内に認証無しでアクセスした場合, セッション上は匿名ユーザーとして認識される
- 匿名ユーザーは既存の全リソースへのアクセスが可能. またセキュリティ設定以外の全ての機能を利用可能

```
GET _plugins/_security/authinfo
{
  "user" : "User [name=opendistro_security_anonymous,
backend_roles=[opendistro_security_anonymous_backendrole], requestedTenant=null]",
  "user_name" : "opendistro_security_anonymous",
  "user_requested_tenant" : null,
  "remote_address" : "27.0.3.153:9200",
  "backend_roles" : [
    "opendistro_security_anonymous_backendrole"
  ],
  "custom_attribute_names" : [ ],
  "roles" : [
    "default_role"
  ],
  "tenants" : {
    "opendistro_security_anonymous" : true
  },
  "principal" : null,
  "peer_certificates" : "0",
  "sso_logout_url" : null
}
```

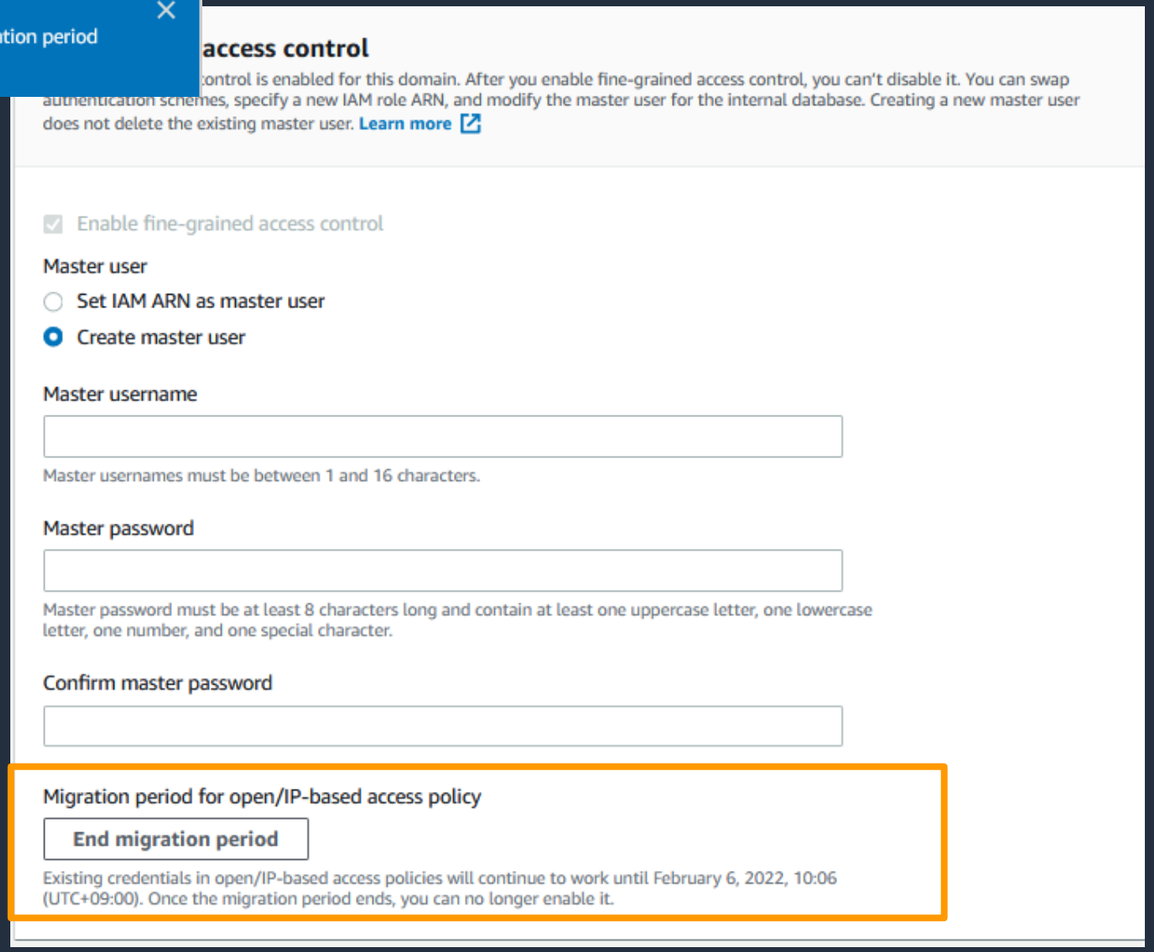


既存ドメインの FGAC 有効化 - 猶予期限の確認

- コンソール上のバナー, セキュリティ設定変更画面, API などから確認可能
- 猶予期間を前倒しで終了させることも可能

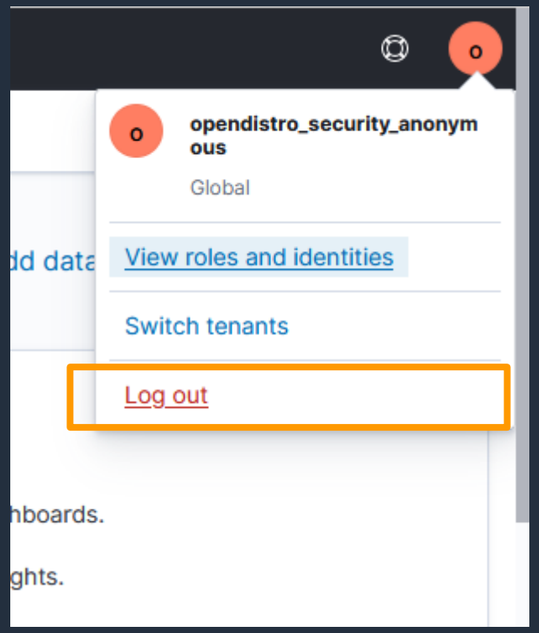


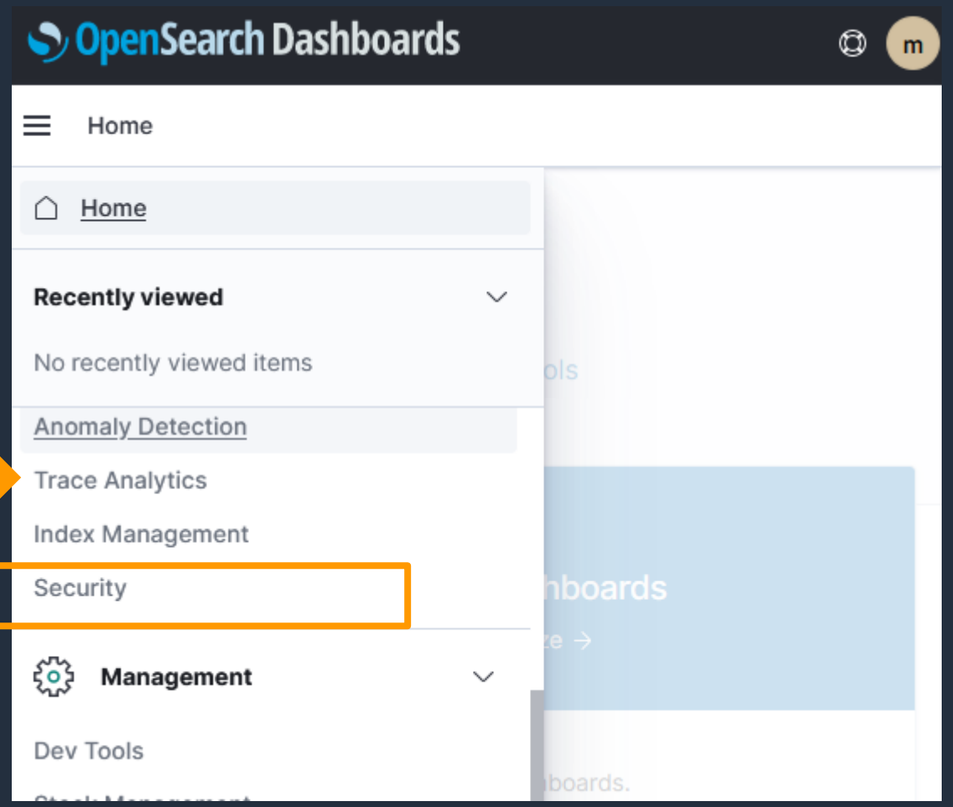

```
$ aws opensearch describe-domain-config --domain-name sample --query
DomainConfig.AdvancedSecurityOptions
{
    "Options": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "AnonymousAuthDisableDate": "2022-02-06T10:06:44.135000+09:00",
        "AnonymousAuthEnabled": true
    },
    "Status": {
        "CreationDate": "2022-01-07T08:42:59.064000+09:00",
        "UpdateDate": "2022-01-07T10:54:47.341000+09:00",
        "UpdateVersion": 25,
        "State": "Active",
        "PendingDeletion": false
    }
}
```



セキュリティ設定の変更

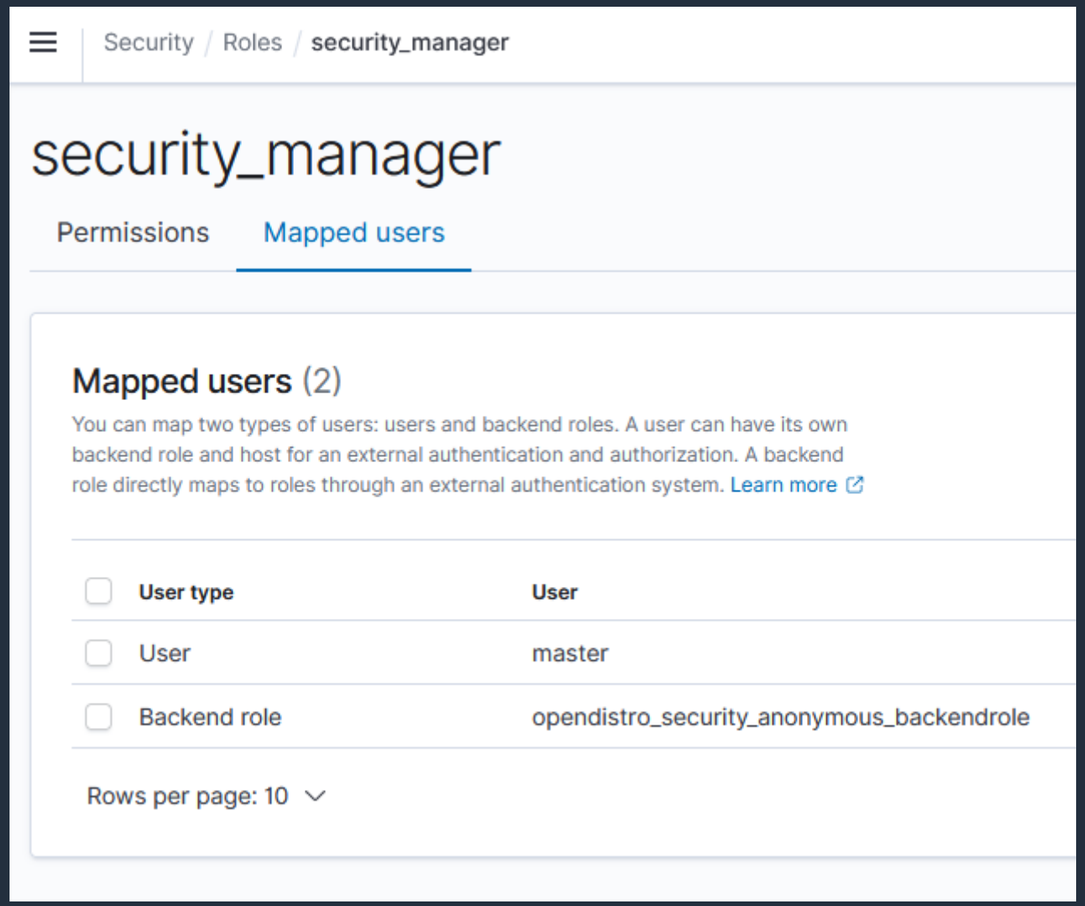
- 匿名ユーザーセッションからログアウトし, 管理者ユーザーでログインすることでセキュリティ設定の変更が可能
- 直接 _dashboards/app/login エンドポイントからログインすることも可能

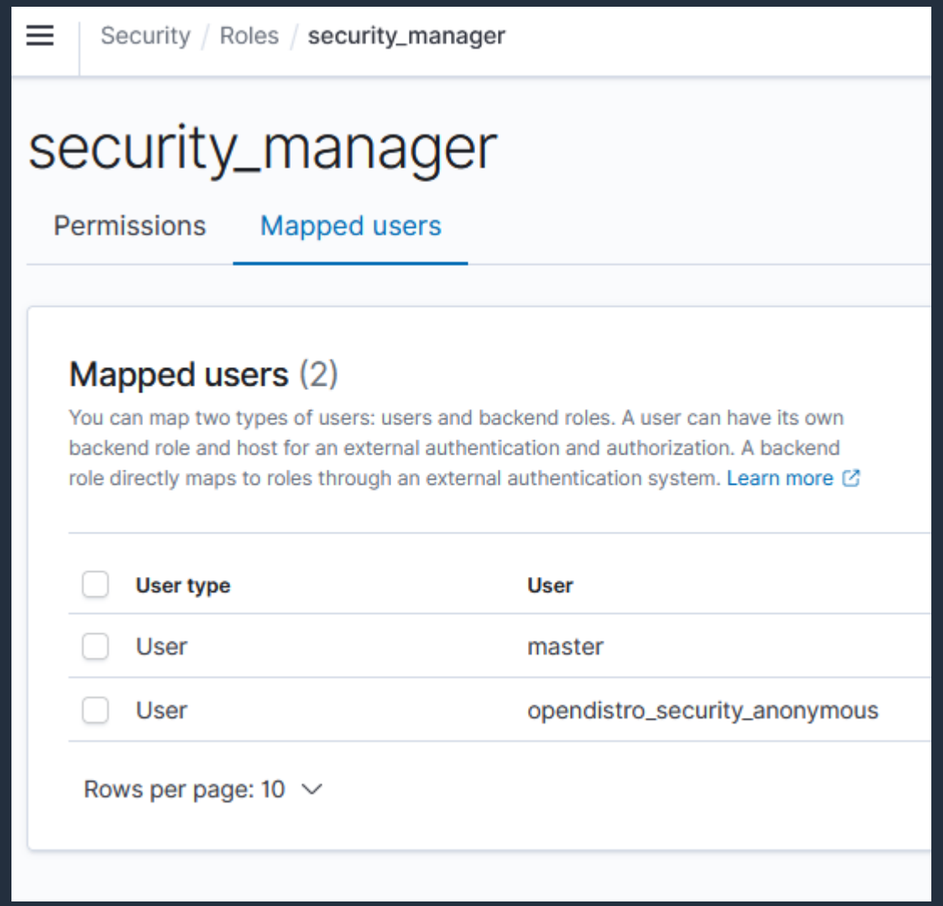




セキュリティ設定の変更 – 補足

- 匿名ユーザーの Backend role, 匿名ユーザー名を security_manager role に直接マップすると匿名ユーザーでもセキュリティ設定の変更は可能だが, セキュリティの観点から推奨しない





セキュリティ関連のアップデート
- Tag Based Access Control -

Tag Based Access Control

設定関連 API についてタグベースのアクセス制御をサポート

- 特定のタグが付与されたドメインのみ設定変更を許可することが可能
- ドメイン作成時, タグ付与時に特定のタグの組み合わせを強制することも可能

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Action": [
   "es:UpdateDomainConfig",
   "es:DescribeDomain",
   "es:DescribeDomainConfig“
  ],
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
   "ForAnyValue:StringEquals": {
    "aws:ResourceTag/team": [ "devops" ]
   }
  }
 }]
}
```

```
{
 "Version": "2012-10-17",
 "Statement": {
  "Effect": "Allow",
  "Action": [
   "es:CreateDomain",
   "es:AddTags"
  ],
  "Resource": "*",
  "Condition": {
   "StringEquals": {
    "aws:RequestTag/team": [ "it" ]
   }
  }
 }
}
```

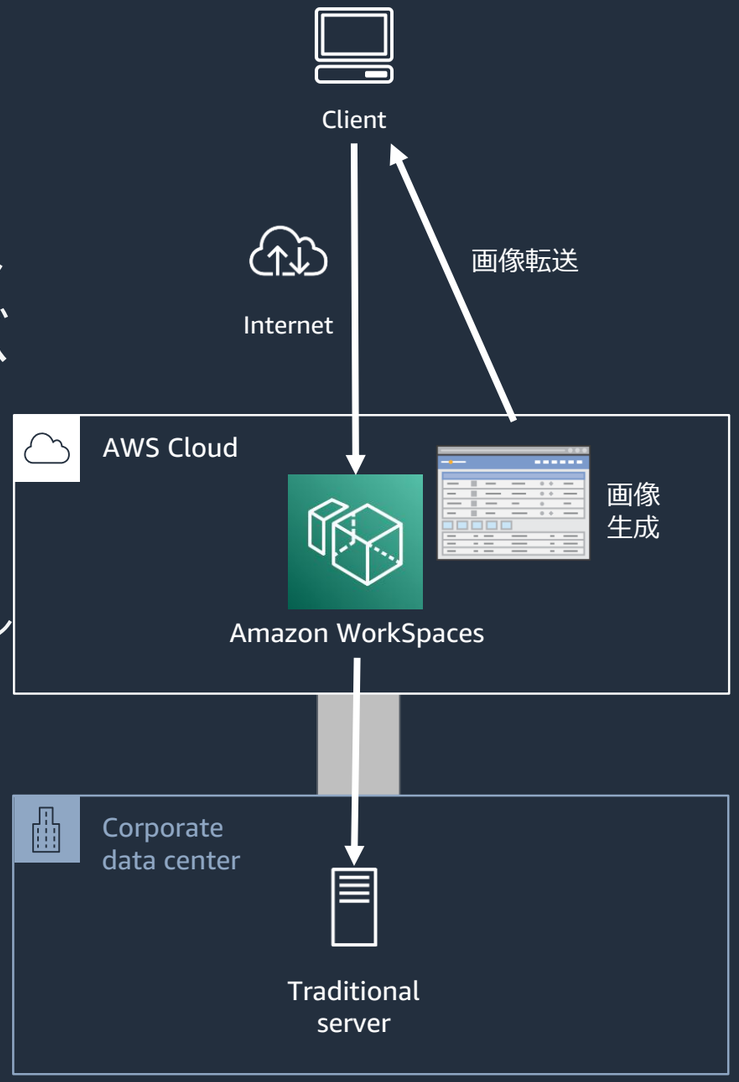
https://docs.aws.amazon.com/opensearch-service/latest/developerguide/ac.html

セキュリティ関連のアップデート

- WorkSpaces Web による VPC ドメインへのアクセス -

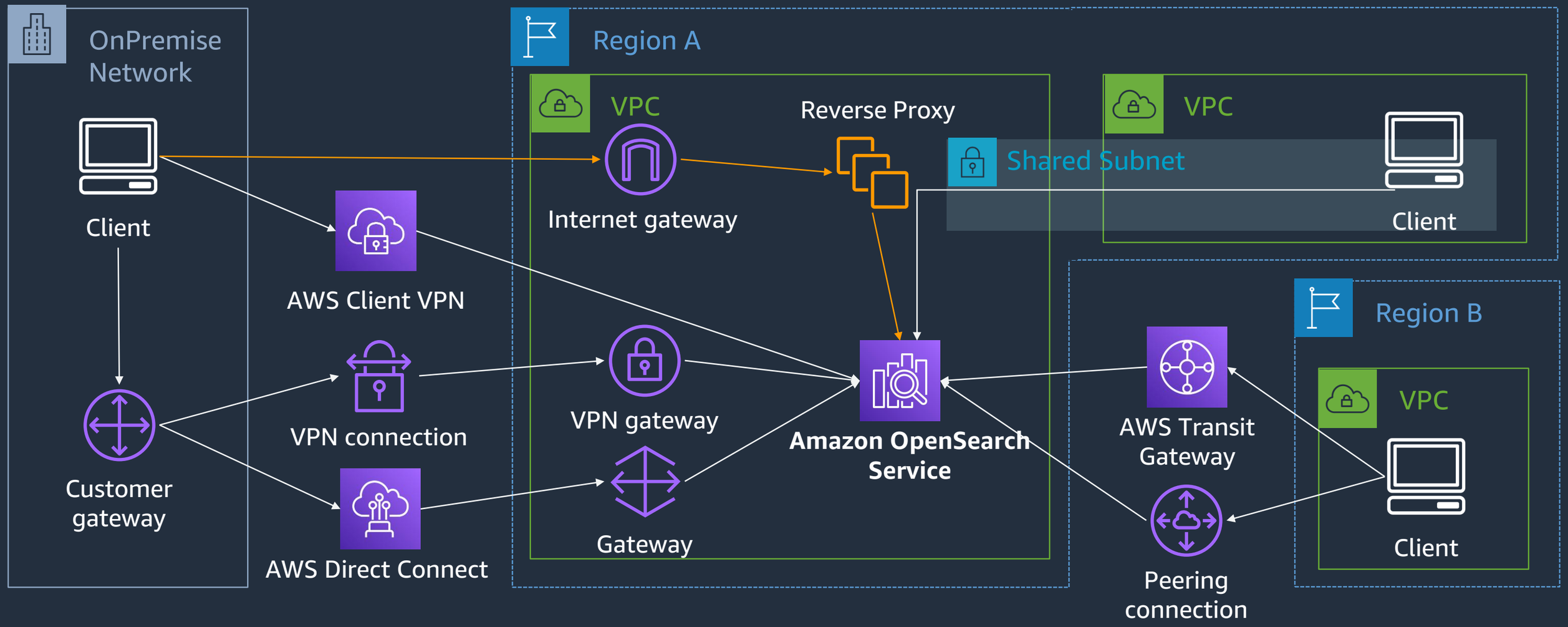
Amazon WorkSpaces Web を発表

- 内部用の Web サイトや Web アプリケーションへのアクセスを安全に提供するための新機能
- AWS 内に起動されるコンテナで Web サイトがレンダリングされ, ユーザには画像のみを転送するため, リモートデバイスに情報が残ることがない
  - 全てのユーザ利用セッションにおいて, 新たに起動された最新バージョンのブラウザを利用できる
  - 管理者側から拡張機能の有効・無効や, 特定 URL の許可・拒否, ローカルプリンタの利用可否などのポリシーを設定できる
- 費用は MAU で算出. 1 MAU あたり 200 時間までの利用が可能で月額 $7となる. 200 時間超過時は $0.035/時間 の追加費用
- バージニア, オレゴン, アイルランドにて提供



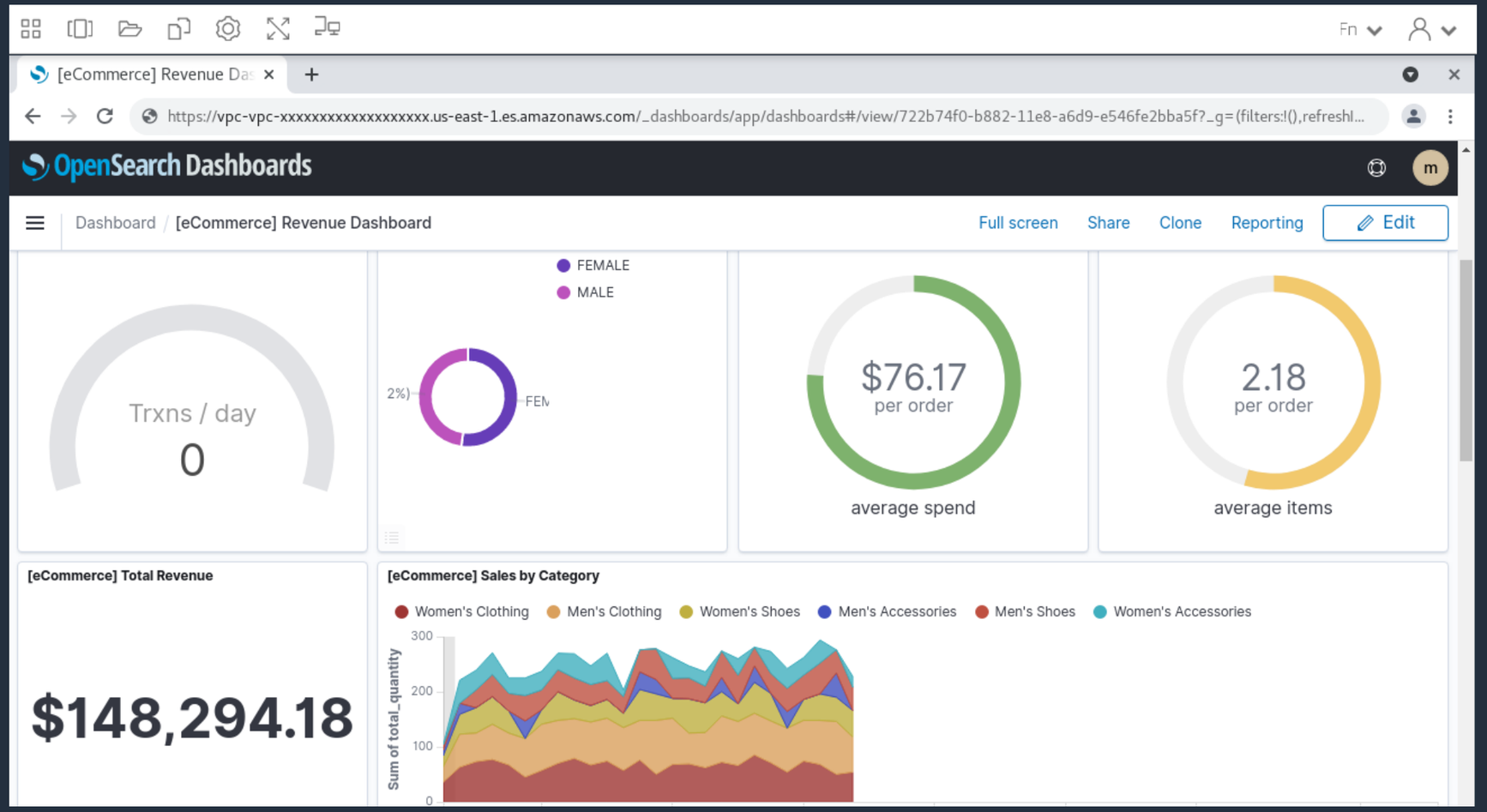
VPC からドメインにプライベート接続

- VPC ドメインに対してインターネット経由で接続することはできない. ブラウザから ダッシュボードへのアクセスには, Proxy や VPN などの仕組みが必要となる



VPC ドメインに対して WorkSpaces Web から安全な接続が可能に

- 常時起動型のリソースを経由する必要無し
- ブラウザ画面自体をネットワーク越しに転送するため, VPN 等を利用して直接ダッシュボードにアクセスする場合と比較すると応答性の面で劣る



Thank you!

Takayuki Enomoto

Solution Architect,
Analytics
Amazon Web Services
Japan G.K.