更新履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版 | 更新日 | 更新項目 | 更新者 | 備考 |
| (会社名/氏名) |
| 1.0 | 2021/06/24 | 新規作成 | アイロベックス  若林 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目次

[1 はじめに 6](#_Toc75824748)

[2 システム構成 7](#_Toc75824749)

[2.1 システム構成図 7](#_Toc75824750)

[2.2 サービス構成 8](#_Toc75824751)

[2.2.1 サービス一覧 8](#_Toc75824752)

[2.2.2 リソースグループ 10](#_Toc75824753)

[2.2.3 サービス管理方式 11](#_Toc75824754)

[2.3 サーバー構成 11](#_Toc75824755)

[2.3.1 Elasticsearch 11](#_Toc75824756)

[2.3.2 APサーバー(Lambda) 13](#_Toc75824757)

[2.3.3 DBサーバー(RDS) 14](#_Toc75824758)

[2.3.4 ストレージ(S3) 15](#_Toc75824759)

[2.3.5 認証基盤(Cognito) 19](#_Toc75824760)

[2.4 ソフトウェア構成 23](#_Toc75824761)

[2.5 ネットワーク構成 23](#_Toc75824762)

[2.5.1 VPC 23](#_Toc75824763)

[2.5.2 サブネット 23](#_Toc75824764)

[2.5.3 ネットワークACL 24](#_Toc75824765)

[2.5.4 セキュリティグループ 25](#_Toc75824766)

[2.5.5 名前解決 25](#_Toc75824767)

[2.5.6 ルートテーブル 25](#_Toc75824768)

[2.5.7 VPCエンドポイント 25](#_Toc75824769)

[3 可用性 26](#_Toc75824770)

[3.1 耐障害性 26](#_Toc75824771)

[3.2 災害対策 26](#_Toc75824772)

[4 拡張性 27](#_Toc75824773)

[4.1 拡張性設計 27](#_Toc75824774)

[5 保守性 28](#_Toc75824775)

[5.1 バックアップ・リストア 28](#_Toc75824776)

[5.1.1 バックアップ 28](#_Toc75824777)

[5.1.2 リストア 28](#_Toc75824778)

[5.2 ジョブ管理 29](#_Toc75824779)

[5.2.1 ジョブ一覧 29](#_Toc75824780)

[5.2.2 ジョブ監視 30](#_Toc75824781)

[5.3 リソース監視 30](#_Toc75824782)

[5.3.1 リソース監視方式 30](#_Toc75824783)

[5.3.2 CloudWatchメトリクス保存期間 30](#_Toc75824784)

[5.3.3 リソース監視状況確認方法 30](#_Toc75824785)

[5.3.4 リソース監視項目 30](#_Toc75824786)

[5.3.5 しきい値監視 64](#_Toc75824787)

[5.4 ログ管理 65](#_Toc75824788)

[5.4.1 ログ一覧 65](#_Toc75824789)

[5.4.2 ログ保存期間 69](#_Toc75824790)

[5.4.3 ログ監視 69](#_Toc75824791)

[5.5 時刻同期 69](#_Toc75824792)

[5.6 ソフトウェアのアップデート 69](#_Toc75824793)

[6 セキュリティ 70](#_Toc75824794)

[6.1 ユーザー管理 70](#_Toc75824795)

[6.2 ロール管理 71](#_Toc75824796)

[6.3 暗号化方針 71](#_Toc75824797)

[6.3.1 Elasticsearch 71](#_Toc75824798)

[6.3.2 DBサーバー(RDS) 71](#_Toc75824799)

[6.3.3 ストレージ(S3) 71](#_Toc75824800)

[6.3.4 認証基盤(Cognito) 72](#_Toc75824801)

[6.3.5 バックアップデータ 72](#_Toc75824802)

[6.4 Webアクセス 72](#_Toc75824803)

[6.4.1 ACM 72](#_Toc75824804)

[6.4.2 AWS WAF 73](#_Toc75824805)

[6.4.3 API Gateway 75](#_Toc75824806)

[6.5 ウィルス対策 77](#_Toc75824807)

# はじめに

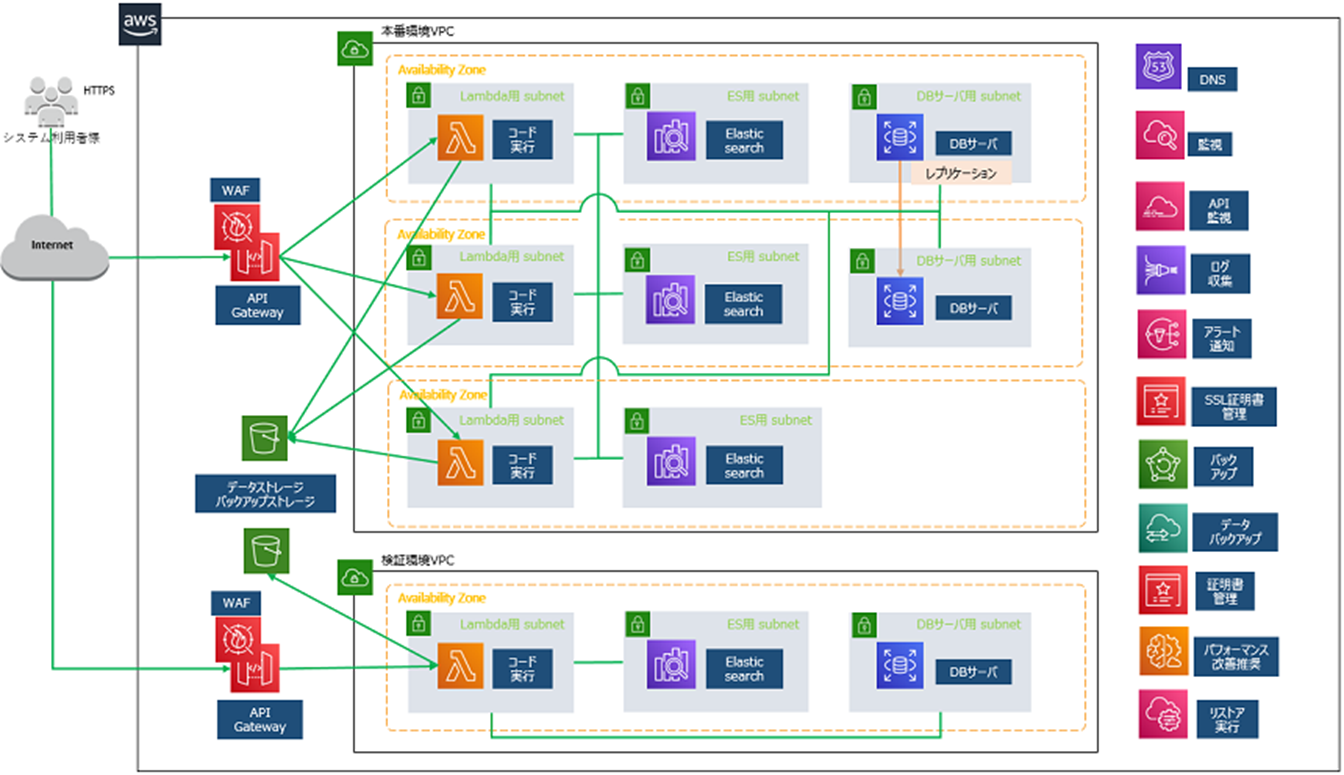
本書はNorthfaceシステム AWS環境(以下、本システム)の構成、機能の実現方法、及び運用方式について記載する。

なお、本システムについてはパブリッククラウドサービスであるAmazon Web Services(以下、AWS)を利用して構築する。

# システム構成

## システム構成図

以下に本システムのシステム構成図を示す。



## サービス構成

本システムで使用するサービスについて記載する。

### サービス一覧

以下に本システムで使用するサービス一覧とその概要を記載する。本システムではすべてのサービスをCloudFormationで管理する

CloudFormationではコードでインフラ環境を管理するInfrastructure as Codeを実現することにより、AWSリソースのコレクションをモデリングし、迅速に一貫してプロビジョニングし、ライフサイクル全体で管理することが容易となる。

|  |  |  |  |
| --- | --- | --- | --- |
|  | システム構成図内表記 | |  |
| サービス | アイコン | 説明 | 概要 |
| ACM |  | 証明書管理 | SSL証明書のプロビジョニング、管理、デプロイを簡単にする。AWS Certificate Manager を使用すれば、SSL証明書の購入、アップロード、更新という時間のかかるプロセスを手動で行う必要がなくなる。 |
| API Gateway |  | 同左 | API の作成、公開、保守、モニタリング、保護を行います。API は、アプリケーションがバックエンドサービスからのデータ、ビジネスロジック、機能にアクセスするための「フロントドア」として機能する。 |
| AWS Backup |  | バックアップ | 中央バックアップコンソールを使用してバックアップポリシーを設定することにより、シンプルなバックアップ管理で AWS のサービス全体のアプリケーションデータを簡単かつ確実にバックアップ、保護する。 |
| AWS Compute Optimizer |  | パフォーマンス改善推奨 | 使用率データに基づいて、Amazon EC2 インスタンス、Amazon EBS ボリューム、AWS Lambda 関数の 3 種類の AWS リソースに関する最適な構成を推奨する。 |
| AWS Systems Manager |  | リストア実行 | AWS運用上のハブ。Systems Manager は、統合されたユーザーインターフェイスを備えており、AWS のアプリケーションとリソース全体の運用上の問題を一元的に追跡および解決する。 |
| AWS WAF |  | WAF | 可用性、セキュリティ侵害、リソースの過剰消費といった一般的なWebの脆弱性からWebアプリケーションまたはAPIを保護するWebアプリケーションファイアウォール。 |
| CloudTrail |  | API監視 | AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を行うためのサービス。CloudTrail を使用すると、AWS インフラストラクチャ全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できる。 |
| CloudWatch |  | リソース監視  ログ監視 | ログ、メトリクス、およびイベントという形式でモニタリングデータと運用データを収集し、AWSのサーバーで実行されるAWSのリソース、アプリケーション、およびサービスの統合されたビューをユーザーに提供。 |
| Cognito |  | 認証基盤 | ウェブアプリケーションおよびモバイルアプリに素早く簡単にユーザーのサインアップ/サインインおよびアクセスコントロールの機能を提供する。 |
| DataSync |  | データバックアップ | AWS ストレージサービス間でのデータの移動を簡素化、自動化、および高速化するオンラインデータ転送サービス。 |
| ElasticSearch |  | 同左 | 分散型検索エンジンであるElasticsearchを大規模かつ簡単でコスト効率の良い方法を使用してデプロイ、保護、実行する完全マネージド型サービス。 |
| IAM |  | 権限管理 | AWS のサービスやリソースへのアクセスを安全に管理する。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否が可能となる。 |
| Kinesis Data Firehose |  | ログ収集 | ストリーミングデータをデータレイクやデータストア、分析サービスに確実にロードする最も簡単な方法を提供する。 |
| KMS |  | 暗号鍵管理 | 暗号化キーを簡単に作成して管理し、幅広い AWS のサービスやアプリケーションでの使用を制御できるようになる。セキュアで弾力性の高いサービスで、キーを保護するために FIPS 140-2 の検証済みまたは検証段階のハードウェアセキュリティモジュールを使用する。 |
| Lambda |  | コード実行 | サーバーのプロビジョニングや管理をすることなく、コードを実行。コードは他の AWS サービスから自動的にトリガーするよう設定することも、ウェブやモバイルアプリケーションから直接呼び出すよう設定することも可能。 |
| RDS |  | DBサーバー | クラウド上のリレーショナルデータベースのセットアップ、オペレーション、スケールが簡単になるサービス。ハードウェアのプロビジョニング、データベースのセットアップ、パッチ適用、バックアップなどの時間がかかる管理タスクを自動化しながら、コスト効率とサイズ変更可能なキャパシティーを提供。 |
| Route53 |  | DNS | 可用性と拡張性に優れたクラウドのDNSサービス。ドメイン登録、DNSルーティング、ヘルスチェックの3つの主要な機能を任意の組み合わせで実行可能。 |
| S3 |  | Webサイト  データストレージ  バックアップストレージ | 拡張性と耐久性を兼ね揃えたクラウドストレージ。 |
| SNS |  | アラート通知 | フルマネージド型メッセージングサービス。SMS やモバイルプッシュ、電子メールを介してユーザーと直接通信が可能。 |
| VPC |  | 本番環境VPC  検証環境VPC | AWS アカウント専用の仮想ネットワーク。 |

### リソースグループ　作成済み

すべてのサービスに共通して以下のリソースグループを指定する。

リソースグループを設定することにより、AWSマネジメントコンソールで関連するサービス一覧を表示することや、リソースグループ別に利用費を確認することが可能となる。

|  |  |  |
| --- | --- | --- |
|  | 本番環境 | 検証環境 |
| グループ名 | Northface-Production | Northface-Staging |
| グループタイプ | タグベース | |
| リソースタイプ | サポートされるすべてのリソースタイプ | |
| タグキー | Project | |
| オプションのタグ値 | Northface | |
| タグキー | Envirionment | |
| オプションのタグ値 | Production | Staging |

### サービス管理方式

本システムではすべてのサービスをCloudFormationで管理する

CloudFormationではコードでインフラ環境を管理するInfrastructure as Codeを実現することにより、AWSリソースのコレクションをモデリングし、迅速に一貫してプロビジョニングし、ライフサイクル全体で管理することが容易となる。

サービス定義はYAML 形式のテキストファイルである AWS CloudFormation テンプレートに記載する。テンプレートは最大51,200バイトの制約があるため、制約を超えるテンプレートを作成する必要がある場合にはネストされたスタックを使用して制約を回避する。

## サーバー構成

以下に本システムのサーバー構成を示す。

本番環境と検証環境を個別に管理するためサーバーを分離する。

各種サーバーは必要最小限のサービスから必要最小限の処理のみアクセスを許可する。

### Elasticsearch　作成済み（アクセス確認まだ）

本システムでは全文検索エンジンとして、Elasticsearchサービスを利用する。

以下にElasticsearchの設定値を示す。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 | 備考 |
| デプロイタイプ | | 本番稼働用  (複数のアベイラビリティゾーンと専用マスターノード) | 開発およびテスト  (エンドポイントが1つのみ、1つのアベイラビリティゾーン) |  |
| バージョン | | 7.10 | 7.10 | 構築時の最新バージョンを指定 |
| Elasticsearchドメイン名 | | prod-northface-es | stag-northface-es | 以下命名規約に則り指定  • アカウントおよびリージョンに固有  • 先頭が小文字  • 3 ～ 28 文字  • 小文字の a ～ z、0 ～ 9 の数字、ハイフン (-) のみ含まれる |
| カスタムエンドポイント | | 無効 | 無効 | 接続元はLambdaのみであるためカスタムエンドポイントは不要 |
| 自動調整 | | 有効 | 有効 | ログ分析ワークロードの取り込みスループットのパフォーマンスを向上させ、検索クエリのテールレイテンシーを短縮する。 |
| メンテナンスウィンドウ | |  |  |  |
|  | 期間 | 1時間 | 1時間 | Blue/Greenデプロイが必要となる一部の自動調整による最適化を実施するウィンドウ |
|  | 曜日 | 毎週土曜日 | 毎週土曜日 |
|  | 開始時刻(UTC) | 15:00 | 15:00 |
| データノード | |  |  |  |
|  | アベイラビリティゾーン | 3-AZ |  | 本番環境は冗長性を考慮し、3AZ構成とする。検証環境は冗長性を考慮する必要がないため、1AZ構成とする。 |
|  | インスタンスタイプ | r5.large.elasticsearch | r5.large.elasticsearch |
|  | vCPU | 2 | 2 |
|  | メモリ | 16 GiB | 16 GiB |
|  | ノードの数 | 3 | 1 |
| データノードストレージ | |  |  |  |
|  | データノードのストレージタイプ | EBS | EBS |  |
|  | EBSボリュームタイプ | 汎用(SSD) | 汎用(SSD) |  |
|  | ノードあたりのEBSストレージサイズ | 10 GiB | 10 GiB |  |
| 専用マスターノード | |  |  |  |
|  | インスタンスタイプ | r5.large.elasticsearch |  | 検証環境は検証用途のため、専用マスターノードは不要 |
|  | vCPU | 2 |  |
|  | メモリ | 16 GiB |  |
|  | マスターノードの数 | 3 |  |
| UltraWarm データノード | | 無効 |  | 大量の読み取り専用データを低コストで保存する。検証環境はシングル構成のため、有効化できない。 |
| コールドストレージ | | 無効 |  | アクセス頻度の低いデータや履歴データを低コストで保存する。検証環境はシングル構成のため、有効化できない。 |
| ネットワーク構成 | | 別途記載 | 別途記載 | 2.5ネットワーク構成を参照 |
| 細かいアクセスコントロール | | 有効 | 有効 | データを安全に保護する。 |
|  | マスターユーザー名 | admi | admin |  |
|  | マスターパスワード | パスワード一覧を参照 | パスワード一覧を参照 |  |
| KibanaのSAML認証 | | 無効 | 無効 |  |
| Amazon Cognito認証 | | 無効 | 無効 |  |
| アクセスポリシー | | ドメインのオープンアクセスを許可 | ドメインのオープンアクセスを許可 |  |
| 暗号化 | | 別途記載 | 別途記載 | 6.3暗号化方針を参照  細かいアクセスコントロールを有効とする場合は暗号化必須 |
| 支払い方法 | | オンデマンドインスタンス | オンデマンドインスタンス | リザーブドインスタンスはインスタンスタイプの変更不可。  本番稼働開始後にリザーブドインスタンスの購入を検討する。 |

### APサーバー(Lambda)作成済み

本システムではAPサーバーとしてLambdaサービスを利用する。

以下にLambdaの定義を示す。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| コード名 | 本番用関数名 | ランタイム | ハンドラー | アクセスする  サービス | メモリ(MB) | タイムアウト(秒) | 本番用環境変数 |
| 検証用関数名 | 検証用環境変数 |
| getSearchEvidence.zip　（ESテスト） | prod\_getSearchEvidence | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | stag\_getSearchEvidence |  |  |  |  |  | 未確定 |
| getAssociationList.zip | prod\_getAssociationList | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | stag\_getAssociationList |  |  |  |  |  | 未確定 |
| getUserUsedCapacity.zip | prod\_getUserUsedCapacity | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | stag\_getUserUsedCapacity |  |  |  |  |  | 未確定 |
| getUserUsableCapacity.zip　（RDSテスト） | prod\_getUserUsableCapacity | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_getUserUsableCapacity |  |  |  |  |  | 未確定 |
| updateUserUsableCapacity.zip | prod\_updateUserUsableCapacity | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_updateUserUsableCapacity |  |  |  |  |  | 未確定 |
| appendEvidenceData.zip | prod\_appendEvidenceData | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | stag\_appendEvidenceData |  |  |  |  |  | 未確定 |
| updateEvidenceData.zip | prod\_updateEvidenceData | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | stag\_updateEvidenceData |  |  |  |  |  | 未確定 |
| deleteEvidenceData.zip　（S3テスト） | prod\_deleteEvidenceData | Python3.8 | Index.handler | ES/S3 | 128 | 30 | 未確定 |
|  | stag\_deleteEvidenceData |  |  |  |  |  | 未確定 |
| getPurchaserOfPrefecture.zip | prod\_getPurchaserOfPrefecture | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | sag\_urchaserOfPrefecture |  |  |  |  |  | 未確定 |
| getTagOfPrefecturePurchaser.zip | prod\_getTagOfPrefecturePurchaser | Python3.8 | Index.handler | ES | 128 | 30 | 未確定 |
|  | stag\_getTagOfPrefecturePurchaser |  |  |  |  |  | 未確定 |
| getStepMemo.zip | prod\_getStepMemo | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_getStepMemo |  |  |  |  |  | 未確定 |
| updateStepMemo.zip | prod\_updateStepMemo | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_updateStepMemo |  |  |  |  |  | 未確定 |
| deleteStepMemo.zip | prod\_deleteStepMemo | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_deleteStepMemo |  |  |  |  |  | 未確定 |
| deleteUserAllData.zip | prod\_deleteUserAllData | Python3.8 | Index.handler | RDS/S3  /ES | 128 | 30 | 未確定 |
|  | stag\_deleteUserAllData |  |  |  |  |  | 未確定 |
| updateTagMaster.zip | prod\_updateTagMaster | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_updateTagMaster |  |  |  |  |  | 未確定 |
| deleteTagMaster.zip | prod\_deleteTagMaster | Python3.8 | Index.handler | RDS | 128 | 30 | 未確定 |
|  | stag\_deleteTagMaster |  |  |  |  |  | 未確定 |
| updateEvidenceFileIndex.zip | prod\_updateEvidenceFileIndex | Python3.8 | Index.handler | S3/ES | 128 | 30 | 未確定 |
|  | stag\_updateEvidenceFileIndex |  |  |  |  |  | 未確定 |

### DBサーバー(RDS)作成済み

本システムではDBサーバーとしてRDSサービスを利用する。

以下にRDSの設定値を示す。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 | 備考 |
| エンジン | | MySQL | MySQL |  |
| DBインスタンス識別子 | | prod-northface-rds | stag-northface-rds | AWSリージョン内で一意の名称を指定 |
| 認証情報の設定 | |  |  |  |
|  | マスターユーザー名 | admin | admin |  |
|  | マスターパスワード | パスワード一覧を参照 | パスワード一覧を参照 |  |
| DBインスタンスサイズ | | db.r5.large | db.r5.large | 最新世代のメモリ最適化インスタンス |
|  | vCPU | 2 | 2 |  |
|  | メモリ | 16 GiB | 16 GiB |  |
| バージョン | | MySQL 8.0.23 | MySQL 8.0.23 | 構築時の最新バージョンを指定 |
| ストレージタイプ | | 汎用(SSD) | 汎用(SSD) |  |
|  | ストレージ割り当て | 20 GiB | 20 GiB | 最小値を指定 |
|  | ストレージの自動スケーリング | 無効 | 無効 |  |
|  | 最大ストレージしきい値 | - | - | 自動スケーリング有効時は設定必須 |
| マルチAZ配置 | | スタンバイインスタンスを作成する | スタンバイインスタンスを作成しない |  |
| 接続 | |  |  |  |
|  | VPC | 別途記載 | 別途記載 | 2.5ネットワーク構成を参照 |
|  | サブネットグループ | 別途記載 | 別途記載 | 2.5ネットワーク構成を参照 |
|  | パブリックアクセス可能 | なし | なし |  |
|  | セキュリティグループ | 別途記載 | 別途記載 | 2.5ネットワーク構成を参照 |
|  | データベースポート | 3306 | 3306 | パブリックアクセス不可のため規定値の3306とする。 |
| データベース認証オプション | | パスワードとIAMデータベース認証 | パスワードとIAMデータベース認証 | AWS IAM ユーザーとロールを介して、データベースパスワードとユーザー認証情報を使用して認証する。 |
| 自動バックアップの有効化 | | 無効 | 無効 | バックアップは手動で実施する。 |
| 暗号化 | | 別途記載 | 別途記載 | 6.3暗号化方針を参照 |
| パフォーマンスインサイト | | 無効 | 無効 | パフォーマンスに問題が生じた場合に有効化を検討する。 |
| 拡張モニタリング | | 無効 | 無効 | パフォーマンスに問題が生じた場合に有効化を検討する。 |
| ログのエクスポート | | エラーログ  全般ログ  スロークエリログ | エラーログ  全般ログ  スロークエリログ | 各種ログを出力する。 |
| マイナーバージョン自動グレードアップ | | 別途記載 | 別途記載 | 5.6ソフトウェアのアップデートを参照 |
| 削除保護 | | 有効 | 有効 | データベースが誤って削除されるのを防ぐ。 |
| 支払い方法 | | オンデマンドインスタンス | オンデマンドインスタンス | リザーブドインスタンスはインスタンスタイプの変更不可。  本番稼働開始後にリザーブドインスタンスの購入を検討する。 |

### ストレージ(S3)作成済み

本システムではストレージとしてS3サービスを利用する。

以下にS3の設定値を示す。

#### データストレージ01

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-data01  検証環境：stag-northface-data01 |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambdaロール |  |
|  | 許可アクション | 読み書き可能 |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて | HTTPS通信のみ許可 |
|  | 拒否アクション | S3に関する全てのアクション |  |
|  | 条件 | 暗号化されていない通信 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | data01acclog/ |  |

#### データストレージ02

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-data02  検証環境：stag-northface-data02 |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambdaロール |  |
|  | 許可アクション | 読み書き可能 |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて | HTTPS通信のみ許可 |
|  | 拒否アクション | S3に関する全てのアクション |  |
|  | 条件 | 暗号化されていない通信 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | data02acclog/ |  |

#### データストレージ03

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-data03  検証環境：stag-northface-data03 |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambdaロール |  |
|  | 許可アクション | 読み書き可能 |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて | HTTPS通信のみ許可 |
|  | 拒否アクション | S3に関する全てのアクション |  |
|  | 条件 | 暗号化されていない通信 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | data03acclog/ |  |

#### データストレージ04

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-data04  検証環境：stag-northface-data04 |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambdaロール |  |
|  | 許可アクション | 読み書き可能 |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて | HTTPS通信のみ許可 |
|  | 拒否アクション | S3に関する全てのアクション |  |
|  | 条件 | 暗号化されていない通信 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | data04acclog/ |  |

#### データストレージ05

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-data05  検証環境：stag-northface-data05 |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | Lambdaロール |  |
|  | 許可アクション | 読み書き可能 |  |
| バケットポリシー | |  |  |
|  | プリンシパル | すべて | HTTPS通信のみ許可 |
|  | 拒否アクション | S3に関する全てのアクション |  |
|  | 条件 | 暗号化されていない通信 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | data05acclog/ |  |

#### アプリケーショストレージ

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-app  検証環境：stag-northface-app |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | appacclog/ |  |

#### バックアップストレージ

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-backup  検証環境：stag-northface-backup |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | 別VPC | オンプレ環境へバックアップデータを転送 |
|  | 許可アクション | 読取りのみ可能 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | bkacclog/ |  |

#### ログストレージ

|  |  |  |
| --- | --- | --- |
| 項目 | 設定値 | 備考 |
| バケット名 | 本番環境：prod-northface-log  検証環境：stag-northface-log |  |
| アクセス設定 | パブリックアクセスをすべてブロック |  |
| バケットポリシー | 設定不要 | AWS WAF / S3 が同一アカウントで動作するため、許可設定不要 |
| 暗号化 | 別途記載 | 6.3暗号化方針を参照 |
| ライフサイクルルール | 5年(1827日) | オブジェクトの現行バージョンの有効期限を5年(1827日)とし、有効期限が切れたオブジェクトを完全に削除する。 |

#### CloudTrailログストレージ

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-northface-cloudtrail  検証環境：stag-northface-cloudtrail |  |
| アクセス設定 | | パブリックアクセスをすべてブロック |  |
| バケットポリシー | |  |  |
|  | プリンシパル | CloudTrail |  |
|  | 許可アクション | 読み書き可能 |  |
| 暗号化 | | 別途記載 | 6.3暗号化方針を参照 |
| サーバーアクセスのログ記録 | | 有効 |  |
|  | ターゲットバケット | S3(ログストレージ) |  |
|  | プレフィックス | ctacclog/ |  |
| ライフサイクルルール | | 5年(1827日) | オブジェクトの現行バージョンの有効期限を5年(1827日)とし、有効期限が切れたオブジェクトを完全に削除する。 |

### 認証基盤(Cognito)作成済み

本システムでは、認証基盤としてCognitoを利用する。

以下にCognitoの定義を示す。

#### ユーザープール

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 項目 | | | | 設定値 | 備考 |
| ユーザープール名 | | | | 本番環境：Northface  検証環境：Northface\_Test |  |
| 属性 | | | |  |  |
|  | サインインオプション | | |  |  |
|  |  | ユーザー名 | | 有効 | ユーザー名、E メールアドレスおよび電話番号の何れかを選択 |
|  |  |  | 検証済みの E メールアドレスでのサインインも許可 | 無効 | ユーザーは、ユーザー名を使用するか、オプションで複数の選択肢を使用してサインアップおよびサインインできる。 |
|  |  |  | 検証済みの電話番号でのサインインも許可 | 無効 |
|  |  |  | 任意のユーザー名 (ユーザーが変更できるユーザー名) でのサインインも許可 | 無効 |
|  |  | E メールアドレスおよび電話番号 | | 無効 | ユーザー名、E メールアドレスおよび電話番号の何れかを選択 |
|  |  |  | E メールアドレスを許可 | 無効 | ユーザーは、E メールアドレスまたは電話番号を「ユーザー名」として使用してサインアップおよびサインインできる。 |
|  |  |  | 電話番号を許可 | 無効 |
|  |  |  | E メールアドレスと電話番号の両方を許可 (ユーザーは 1 つを選択できます) | 無効 |
|  | (推奨) ユーザー名入力で大文字と小文字を区別しないことを有効にする | | | 無効 | 有効にすると、ユーザーは「username」または「Username」のいずれでもサインイン可能となる。 |
|  | 標準属性 | | | name | 以下標準属性のうち、サインアップに必須とする属性を選択する。  address / nickname / birthdate / phone number / email / picture / family name / preferred username / gender / profile / given name / zoneinfo / locale / updated at / middle name / website / name |
| ポリシー | | | |  |  |
|  | パスワードの強度 | | |  |  |
|  |  | 最小長 | | 8 | 最小文字数 |
|  |  | 必須文字種別 | | 数字 / 特殊文字 / 大文字 / 小文字 | 以下から必須とする文字種別を選択する。  数字 / 特殊文字 / 大文字 / 小文字 |
|  | 自己サインアップ | | | 管理者のみ | 以下からユーザーの作成を許可する対象を選択する。  管理者のみ / ユーザー |
|  | 有効期限 (日数) | | | 7 | 管理者が設定した一時パスワードが使用されないまま有効期限になるまでの期間 |
| MFA、確認 | | | |  |  |
|  | 多要素認証 (MFA) | | | オフ | 以下からMFAの設定を選択する。  オフ / 省略可能 / 必須 |
|  | アカウント回復方法 | | | 使用可能な場合は E メール、それ以外の場合は電話。ただし、MFA にも使用している場合、電話でパスワードをリセットすることは許可しません | 以下からユーザーがパスワードを忘れた場合のアカウント回復方法を選択する。  ・使用可能な場合は Eメール、それ以外の場合は電話。ただし、MFA にも使用している場合、電話でパスワードをリセットすることは許可しません  ・使用可能な場合は電話、それ以外の場合は E メール。ただし、MFA にも使用している場合は、電話でパスワードをリセットすることは許可しません  ・Eメールのみ  ・電話のみ。ただし、MFA にも使用している場合は、電話でパスワードをリセットすることは許可しません  ・(非推奨) 使用可能な場合は電話、それ以外の場合は Eメール。MFA にも使用している場合は、電話でパスワードをリセットすることができます  ・なし – ユーザーは管理者に連絡してパスワードをリセットする必要があります |
|  | 属性の確認 | | |  | 以下からユーザーの検証方法を選択する。  Eメール / 電話番号 / Eメールまたは電話番号 / 検証なし |
|  | SMSメッセージ送信ロール | | | (SMSメッセージ送信ロール) | Amazon Cognito に対して SMS メッセージの送信を許可する。 |
| メッセージのカスタマイズ | | | |  |  |
|  | Eメールアドレスカスタマイズ | | |  |  |
|  |  | SESリージョン | | 米国東部(バージニア) | SES の検証済み ID から E メールを送信できる。 |
|  |  | FROM EメールアドレスARN | | デフォルト |
|  |  | FROM Eメールアドレス | |  |
|  |  | REPLY-TO Eメールアドレス | |  |
|  | SESでEメールを送信する | | | いいえ | 毎日の E メールの制限を上げる必要がある場合は [はい] を選択し、それ以外の場合は [いいえ] を選択する。 |
|  | Eメール検証メッセージのカスタマイズ | | |  |  |
|  |  | 検証タイプ | | コード | コードまたはクリック可能リンクを選択して、E メールアドレスを選択する。 |
|  |  | Eメールの件名 | | 検証コード |
|  |  | Eメールのメッセージ | | 検証コードは {####} です。 |
|  | ユーザー招待メッセージのカスタマイズ | | |  |  |
|  |  | SMSメッセージ | | ユーザー名は {username}、仮パスワードは {####} です。 | メッセージはカスタマイズし、HTML タグを含めることができるが、「{username}」および「{####}」プレースホルダーを含める必要がある。このプレースホルダーはそれぞれユーザー名および仮パスワードで置き換えられる。 |
|  |  | Eメールの件名 | | 仮パスワード |
|  |  | Eメールのメッセージ | | ユーザー名は {username}、仮パスワードは {####} です。 |
| デバイスの記憶 | | | | いいえ |  |

#### IDプール

|  |  |  |
| --- | --- | --- |
| 項目 | 設定値 | 備考 |
| IDプール名 | 本番環境：Northface  検証環境：Northface\_Test |  |
| 認証されていないID | 無効 | 認証されていない ID に対するアクセスの有効/無効を選択する。このオプションを有効にすると、インターネットアクセスが可能なユーザー全員に AWS 認証情報を付与することができる。 |
| 認証フローの設定 | 無効 | Cognito では、拡張された認証フローの使用を推奨しています。ただし、基本的なフローを使用する場合は、ここで有効にすることができます |
| 認証プロバイダー |  | 以下から、Cognitoの認証方法を選択する。  ・Cognito  ・Amazon  ・Apple  ・Facebook  ・Google+  ・Twitter / Digits  ・OpenID  ・SAML  ・カスタム |

## ソフトウェア構成

本システムのソフトウェアは全てAWSマネージドサービスを利用し、ユーザー管理によるソフトウェアは導入しない。

## ネットワーク構成

本システムのネットワーク構成を以下に示す。

### VPC作成済み

本システムでは各種機密データを専用ネットワーク内で処理するため、アカウント専用の仮想ネットワークであるVPCを作成する。

一方の環境の変更がもう一方の環境に影響を与えないようにするため、本番環境と検証環境でVPCを分ける。

以下にVPCの定義を示す。

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | 本番環境 | 検証環境 | 備考 |
| VPC名 | prod-northface-vpc | stag-northface-vpc | 一方の環境の変更がもう一方の環境に影響を与えないようにするため、本番環境と検証環境でVPCを分ける。 |
| VPC IPv4 CIDR | 172.29.0.0/18 | 172.30.0.0/18 | 関連システムとネットワーク接続可能とするため、既存の関連システムと重複しないネットワーク(CIDR)を割り当てる。 |
| IPv6ブロック | IPv6 CIDR ブロックなし | IPv6 CIDR ブロックなし | 既存の関連システムがIPv4を使用しているため、IPv4を使用し、IPv6は使用しない。 |
| テナンシー | デフォルト | デフォルト | VM、ソケット、または物理コアにバインドされたソフトウェアライセンスを含む専有テナントインスタンスを使用しないため。 |

### サブネット

インターネットに接続しないため、プライベートサブネットのみ作成する。

Elasticsearch専用、Lambda専用のサブネットを作成することで他のアプリケーションやサービスとの重複を回避し、スケールアウトを可能とする。

#### 本番環境用サブネット作成済み

|  |  |  |  |
| --- | --- | --- | --- |
| プライベートサブネット | サブネット名 | アベイラビリティゾーン | IPv4 CIDRブロック |
| Elasticsearch用サブネット | prod-northface-es-subnet01 | ap-northeast-1a | 172.29.0.0/28 |
|  | prod-northface-es-subnet02 | ap-northeast-1c | 172.29.0.16/28 |
|  | prod-northface-es-subnet03 | ap-northeast-1d | 172.29.0.32/28 |
| Lambad用サブネット | prod-northface-lambda-subnet01 | ap-northeast-1a | 172.29.8.0/21 |
|  | prod-northface-lambda-subnet02 | ap-northeast-1c | 172.29.16.0/21 |
|  | prod-northface-lambda-subnet03 | ap-northeast-1d | 172.29.24.0/21 |
| RDS用サブネット | prod-northface-rds-subnet01 | ap-northeast-1a | 172.29.0.48/29 |
|  | prod-northface-rds-subnet02 | ap-northeast-1c | 172.29.0.56/29 |

#### 検証環境用サブネット

|  |  |  |  |
| --- | --- | --- | --- |
| プライベートサブネット | サブネット名 | アベイラビリティゾーン | IPv4 CIDRブロック |
| Elasticsearch用サブネット | stag-northface-es-subnet01 | ap-northeast-1a | 172.30.0.0/28 |
| Lambad用サブネット | stag-northface-lambda-subnet01 | ap-northeast-1a | 172.30.8.0/21 |
| RDS用サブネット | stag-northface-rds-subnet01 | ap-northeast-1a | 172.30.0.48/29 |

### ネットワークACL作成済み

サブネットに指定するIPアドレス範囲間で通信許可を設定する。

ネットワークACLはステートレスでインバウンドルールとアウトバウンドルールを詳細に設定する必要があり、またサブネット全体に影響を与えるため管理が複雑となる。構成管理の簡素化のため、通信を許可するタイプ、プロトコル、ポート番号の範囲はネットワークACLでは設定せず、セキュリティグループで設定する。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ネットワークACL名 | |  | 許可設定内容 | |
| ネットワークACL | 本番環境 | 検証環境 | 割当先サブネット | インバウンドルール | アウトバウンドルール |
| Elasticsearch用NACL | prod-northface-es-nacl | stag-northface-es-nacl | Elasticsearch用サブネット | Lambda用サブネット | Lambda用サブネット |
| Lambda用NACL | prod-northface-lambda-nacl | stag-northface-lambda-nacl | Lambda用サブネット | Elasticsearch用サブネット | Elasticsearch用サブネット |
|  |  |  |  | RDS用サブネット | RDS用サブネット |
| RDS用NACL | prod-northface-rds-nacl | stag-northface-rds-nacl | RDS用サブネット | Lambda用サブネット | Lambda用サブネット |

ルール番号は将来的に前後に別のルールを挿入することを可能とするため、以下の通り付番する。

|  |  |
| --- | --- |
| 開始番号 | 増分 |
| 100 | 10 |

### セキュリティグループ作成済み

セキュリティグループ間で必要最小限のプロトコル、ポート番号範囲の通信許可を設定する。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | セキュリティグループ名 | | インバウンドルール | | アウトバウンドルール | |
| セキュリティグループ | 本番環境 | 検証環境 | プロトコル：ポート範囲 | ソース | プロトコル：ポート範囲 | ソース |
| Elasticsearch用セキュリティグループ | prod-northface-es-secg | stag-northface-es-secg | TCP：9300 | Lambda用セキュリティグループ | すべて：すべて | 0.0.0.0/0 |
| RDS用セキュリティグループ | prod-northface-rds-secg | stag-northface-rds-secg | TCP：3306 | Lambda用セキュリティグループ | すべて：すべて | 0.0.0.0/0 |

### 名前解決

Route53のプライベートホストゾーンを使用する。

### ルートテーブル作成済み

以下のルートテーブルを作成し、VPC内の全プライベートサブネット間をルーティング可能とする。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 | 備考 |
| ルートテーブル名 | | prod-northface-private-routetable | stag-northface-private-routetable |  |
| ルート | |  |  |  |
|  | 送信先 | (本番環境VPCのCIDR) | (検証環境VPCのCIDR) |  |
|  | ターゲット | Local | Local |  |
|  | サブネットの関連付け | (本番環境の全サブネット) | (検証環境の全サブネット) | プライベートサブネット |

### VPCエンドポイント作成済み

別のシステムとの連携のために以下のVPCエンドポイントを作成する。

・バックアップストレージ(S3)のVPCエンドポイント

# 可用性

## 耐障害性

本システムが利用する各種サービスはすべてAWSが管理・提供するAWSグローバルインフラストラクチャ上で実行される。

本システムは東京リージョン内の複数のアベイラビリティーゾーン(以下AZ)で稼働し、単一のAZ障害からシステムを保護する。

AWSのグローバルインフラストラクチャは、AWSリージョンとAZを中心として構成されている。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立・隔離されたAZがある。

AZは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れており、AZ間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを運用することができる。

AWSサービスはサービス別にSLAを定義している。以下に本システムが使用するサービスのSLA最低値、及びSLAが最低値の場合の週単位・月単位・年単位でシステムが停止する最大時間を示す。

|  |  |  |  |
| --- | --- | --- | --- |
| SLA最低値 | 週間停止時間 | 月間停止時間 | 年間停止時間 |
| 99.9% | 10.08分 | 43.20分 | 8.76時間 |

本システムが使用するサービスのSLAを示す。

|  |  |
| --- | --- |
| SLA | サービス |
| 100% | Route53 |
| 99.99% | Kinesis Data Firehose |
| 99.95% | API Gateway / AWS WAF / Lambda / RDS |
| 99.9% | ACM / AWS Backup / AWS Systems Manager / CloudTrail / CloudWatch / Cognito / DataSync / ElasticSearch / KMS / S3 / SNS |

## 災害対策

災害対策については考慮しない。

# 拡張性

## 拡張性設計

本システムでは、使用状況に応じて各種リソースを拡張する。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | 変更時サーバー停止の必要性 | |  |
| サーバー | 対象リソース | 拡張方式 | 本番環境 | 検証環境 | 備考 |
| Elasticsearch  データノード | ストレージ容量 | ストレージ容量の自動追加 | 不要 | 必要 | 残量が3 GB以下になった場合に自動で10 GB追加する |
| CPU | インスタンスタイプの変更 | 不要 | 必要 |  |
| インスタンスの追加・削除 | 不要 | 必要 |  |
| メモリ | インスタンスタイプの変更 | 不要 | 必要 |  |
| Elasticsearch  マスターノード | CPU | インスタンスタイプの変更 | 不要 | - |  |
| メモリ | インスタンスタイプの変更 | 不要 | - |  |
| APサーバー  (Lambda) | メモリ | 128 MB～10,240 MBの値を1MB単位で指定 | 不要 | | 運用上、問題が発生した場合にAWS Compute Optimizerによる推奨事項を参考に拡張可否を検討する |
| CPU | メモリ割り当て容量に応じて自動調整される。(1,769 MBあたり1 vCPU) | 不要 | |
| DBサーバー  (RDS) | ストレージ容量 | ストレージ容量の自動追加 | 不要 | | 空き容量10%未満が5分以上継続し、かつ最後のストレージ変更から6時間以上経過している場合、以下のうち何れか大きいストレージ容量を追加する。  ・5GiB  ・現在割り当てられているストレージの10%  ・直近1時間のFreeStorageSpaceメトリクスの変動に基づいて予測される7時間のストレージの増分。 |
| CPU | インスタンスタイプの変更 | 必要 | |  |
| メモリ | インスタンスタイプの変更 | 必要 | |  |
| IOPS | インスタンスタイプの変更 | 必要 | |  |
| ストレージ  (S3) | ストレージ容量 | ストレージ容量の自動追加 | 不要 | |  |

# 保守性

## バックアップ・リストア

本システムのバックアップ・リストアの方式を示す。

### バックアップ

アプリケーション要件として、バックアップ対象データ間の整合性を保護するためにバックアップは同一時間に実行する。

一次バックアップ保存先へのバックアップが完了した後に一次バックアップ保存先から二次バックアップ保存先へバックアップデータをコピーする。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 対象 | 保存期間 | スケジュール | バックアップ方式 | 暗号化 | 一次バックアップ  保存先 | 二次バックアップ  保存先 |
| Elasticsearch | 1ヶ月  (30日) | 日次  1:00 | 増分バックアップ | 6.3暗号化方針を参照 | バックアップストレージ | オンプレ環境ストレージ |
| データベース(RDS) | 増分バックアップ |
| データストレージ(S3) | 増分バックアップ |

### リストア

一次バックアップ保存先にアクセス可能な場合は一次バックアップ保存先から復旧する。

東京リージョン障害発生時等、一次バックアップ保存先にアクセス不可の場合は二次バックアップ保存先から復旧する。

復旧時間についてはS3バケット間の転送速度は保証されていないため、「クロスリージョンのバケット間転送が30MB/s程度」の実測結果を参考に試算する。

#### 一次バックアップからのリストア

|  |  |  |  |
| --- | --- | --- | --- |
| 対象 | リストア方式 | 復旧時点 | 復旧時間 |
| Elasticsearch | AWS Systems Managerより、Elasticsearchの復元処理を実行する。 | バックアップ取得時点 | テスト実施時に時間を計測して記載 |
| データベース(RDS) | AWSマネジメントコンソールより、データベースの復元処理を実行する。 | バックアップ取得時点 | テスト実施時に時間を計測して記載 |
| データストレージ(S3) | AWSマネジメントコンソールより、データストレージの復元処理を実行する。 | バックアップ取得時点 | リストアデータ量10GBあたり6分程度 |

#### 二次バックアップからのリストア

|  |  |  |  |
| --- | --- | --- | --- |
| 対象 | リストア方式 | 復旧時点 | 復旧時間 |
| Elasticsearch | 二次バックアップ保存先から一次バックアップ保存先へバックアップデータを転送する。  AWS Systems Managerより、Elasticsearchの復元処理を実行する。 | バックアップ取得時点 | テスト実施時に時間を計測して記載 |
| データベース(RDS) | 二次バックアップ保存先から一次バックアップ保存先へバックアップデータを転送する。  AWS Systems Managerより、データベースの復元処理を実行する。 | バックアップ取得時点 | テスト実施時に時間を計測して記載 |
| データストレージ(S3) | 二次バックアップ保存先から一次バックアップ保存先へバックアップデータを転送する。  AWSマネジメントコンソールより、データストレージの復元処理を実行する。 | バックアップ取得時点 | テスト実施時に時間を計測して記載 |

## ジョブ管理

本システムのジョブ管理について記載する。

### ジョブ一覧

本システムでは以下のジョブを実行する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 種別 | ジョブ | 内容 | 成功時 | 失敗時 |
| バックアップ | Elasticsearchの日次バックアップ | LambdaによりElasticsearchのバックアップを取得する。 | ログ出力 | ログ出力  アラート通知 |
|  | データベース(RDS)の日次バックアップ | AWS Backup / Lamdbaによりデータベースのバックアップを取得する。 | ログ出力 | ログ出力  アラート通知 |
|  | データストレージ(S3)の日次バックアップ | DataSyncによりデータストレージをバックアップストレージに同期する。 | ログ出力 | ログ出力  アラート通知 |

### ジョブ監視

本システムではジョブが失敗した際にメールによるアラート通知を行う。

|  |
| --- |
| 通知先メールアドレス |
| d-suzuki@cstnet.co.jp |
| y-chida@cstnet.co.jp |
| t-gotoh@cstnet.co.jp |

## リソース監視

本システムのリソース監視について記載する。

### リソース監視方式

本システムはCloudWatchサービスによりリソースを監視する。

### CloudWatchメトリクス保存期間

メトリクスの保存期間を示す。変更はできない。

|  |  |
| --- | --- |
| 期間 | 保存期間 |
| 60秒未満のデータポイント | 3時間 |
| 60秒(1分)のデータポイント | 15日間 |
| 300秒(5分)のデータポイント | 63日間 |
| 3600秒(1時間)のデータポイント | 455日間(15ヶ月) |

### リソース監視状況確認方法

本システムのリソース監視状況はAWSマネジメントコンソールのCloudWatchページで確認する。

### リソース監視項目

本システムの監視項目をサービス別に記載する。

#### ACM

|  |  |
| --- | --- |
| メトリクス | 内容 |
| DaysToExpiry | 証明書の有効期限が切れるまでの日数。ACMは、証明書の有効期限が切れると、このメトリックの公開を停止する。 |

#### API Gateway

|  |  |
| --- | --- |
| メトリクス | 内容 |
| 4XXError | 指定された期間に取得されたクライアント側エラーの数。  Sum 統計は、このメトリクス、つまり、指定された期間内の 4XXError エラーの合計数を表す。Average 統計は、4XXError のエラー率、つまり、4XXError エラーの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| 5XXError | 指定された期間に取得されたサーバー側エラーの数。  Sum 統計は、このメトリクス、つまり、指定された期間内の 5XXError エラーの合計数を表す。Average 統計は、5XXError のエラー率、つまり、5XXError エラーの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| CacheHitCount | 指定された期間内に API キャッシュから配信されたリクエストの数。  Sum 統計は、このメトリクス、つまり、指定された期間内のキャッシュヒットの合計数を表す。Average 統計は、キャッシュヒット率、つまり、キャッシュヒットの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| CacheMissCount | API キャッシュが有効になっている特定の期間における、バックエンドから提供されたリクエストの数。  Sum 統計は、このメトリクス、つまり、指定された期間内のキャッシュミスの合計数を表す。Average 統計は、キャッシュミス率、つまり、キャッシュミスの合計数をその期間のリクエストの合計数で割ったもの。分母は Count メトリクス (下記) に対応する。 |
| Count | 指定された期間内の API リクエストの合計数。  SampleCount 統計は、このメトリクスを表す。 |
| IntegrationLatency | API Gateway がバックエンドにリクエストを中継してから、バックエンドからレスポンスを受け取るまでの時間。 |
| Latency | API Gateway がクライアントからリクエストを受け取ってから、クライアントにレスポンスを返すまでの時間。レイテンシーには、統合のレイテンシーおよびその他の API Gateway のオーバーヘッドが含まれる。 |

#### AWS Backup

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| ジョブ | CREATED | 1 つ以上の特定のバックアップボールト内で失敗したバックアップジョブの数。 |
|  | PENDING |
|  | RUNNING |
|  | ABORTED |
|  | COMPLETED |
|  | FAILED |
|  | EXPIRED |
| 復旧ポイント | MODIFIED | 状態別の復旧ポイントの数 |
|  | COMPLETED |  |
|  | PARTIAL |  |
|  | EXPIRED |  |
|  | DELETED |  |
| - | NumberOfBackupJobsCreated | AWS Backup が作成したバックアップジョブの数。 |
|  | NumberOfBackupJobsPending | AWS Backup で実行しようとしているバックアップジョブの数。 |
|  | NumberOfBackupJobsRunning | AWS Backup で現在実行中のバックアップジョブの数。 |
|  | NumberOfBackupJobsAborted | AWS Backup がスケジュールしたのに開始しなかったバックアップジョブの数。多くの場合、データベースリソースのメンテナンスウィンドウまたは自動バックアップウィンドウの 4 時間前、またはバックアップジョブのスケジューリングが原因。AWS Backup は、データの整合性を維持するために、スケジュールされたジョブを実行しない。 |
|  | NumberOfBackupJobsCompleted | AWS Backup が終了したバックアップジョブの数。 |
|  | NumberOfBackupJobsFailed | AWS Backup が試行したが完了できなかったバックアップジョブの数。 |
|  | NumberOfBackupJobsExpired | AWS Backup がバックアップ保持ライフサイクルに基づいて削除しようとしたが、削除できなかったバックアップジョブの数。期限切れのバックアップが消費したストレージに対して課金されるため、手動で削除する必要がある。 |
|  | NumberOfCopyJobsCreated | AWS Backup が作成したクロスアカウントおよびクロスリージョンコピージョブの数。 |
|  | NumberOfCopyJobsRunning | AWS Backup で現在実行中のクロスアカウントおよびクロスリージョンコピージョブの数。 |
|  | NumberOfCopyJobsCompleted | AWS Backup が完了したクロスアカウントおよびクロスリージョンコピージョブの数。 |
|  | NumberOfCopyJobsFailed | AWS Backup が試行したが完了できなかったクロスアカウントおよびクロスリージョンコピージョブの数。 |
|  | NumberOfRestoreJobsPending | AWS Backup で実行しようとしている復元ジョブの数。 |
|  | NumberOfRestoreJobsRunning | AWS Backup で現在実行中の復元ジョブの数。 |
|  | NumberOfRestoreJobsCompleted | AWS Backup が終了した復元ジョブの数。 |
|  | NumberOfRestoreJobsFailed | AWS Backup が試行したが完了できなかった復元ジョブの数。 |
|  | NumberOfRecoveryPointsCompleted | AWS Backup が作成した復旧ポイントの数。 |
|  | NumberOfRecoveryPointsPartial | AWS Backup が作成を開始したが、完了できなかった復旧ポイントの数。AWS はプロセスを後で再試行するが、再試行は後で行われるため、部分的な復旧ポイントを保持する。 |
|  | NumberOfRecoveryPointsExpired | AWS Backup がバックアップ保持ライフサイクルに基づいて削除しようとしたが、削除できなかった復旧ポイントの数。期限切れのバックアップが消費したストレージに対して課金されるため、手動で削除する必要がある。 |
|  | NumberOfRecoveryPointsDeleting | AWS Backup が削除している復旧ポイントの数。 |
|  | NumberOfRecoveryPointsCold | AWS Backup がコールドストレージに階層化した復旧ポイントの数。 |

#### AWS Systems Manager

|  |  |
| --- | --- |
| メトリクス | 内容 |
| CommandsDeliveryTimedOut | 端末ステータスが Delivery Timed Out のコマンドの数。 |
| CommandsFailed | 端末ステータスが Failed のコマンドの数。 |
| CommandsSucceeded | 端末ステータスが Success のコマンドの数。 |

#### AWS WAF

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| Web ACL、ルールグループ、ルールメトリックス | AllowedRequests | 許可された、ウェブリクエストの数。  レポート条件 ゼロ以外の値がある。 |
|  | BlockedRequests | ブロックされたウェブリクエストの数。  レポート条件 ゼロ以外の値がある。 |
|  | CountedRequests | カウントされたウェブリクエストの数。  レポート条件 ゼロ以外の値がある。  カウントされたウェブリクエストは、少なくとも 1 つのルールに一致するリクエスト。リクエストカウントは、通常、テストに使用される。 |
|  | PassedRequests | 渡されたリクエストの数。これは、規則グループのどの規則にも一致しないで、規則グループの評価を通過する要求にのみ使用される。  レポート条件 ゼロ以外の値がある。  渡されたリクエストは、ルールグループのどのルールにも一致しないリクエスト。 |
| ラベルと AWS WAF ボットコントロールメトリックス | AllowedRequests | 許可アクション設定を持つルールによって Web リクエストに適用されたラベルの数。  レポート条件 ゼロ以外の値がある。 |
|  | BlockedRequests | ブロックアクション設定を持つルールによって Web リクエストに適用されたラベルの数。  レポート条件 ゼロ以外の値がある。 |
|  | CountedRequests | count アクション設定を持つルールによって Web リクエストに適用されるラベルの数。  レポート条件 ゼロ以外の値がある。 |
| 無料のボットの可視性指標 | SampleAllowedRequests | 許可アクションを持つサンプリングされたリクエストの割合。  レポート条件 ゼロ以外の値がある。 |
|  | SampleBlockedRequests | ブロックアクションを持つサンプリングされたリクエストの割合。  レポート条件 ゼロ以外の値がある。 |

#### Cognito

|  |  |
| --- | --- |
| メトリクス | 内容 |
| SignUpSuccesses | Amazon Cognito ユーザープールに対して成功したユーザー登録リクエストの総数を提供する。成功したユーザー登録リクエストでは値 1 を生成し、失敗したリクエストでは値 0 を生成する。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  成功したユーザー登録リクエストの割合を調べるには、このメトリクスの Average 統計を使用する。ユーザー登録リクエストの合計数をカウントするには、このメトリクスの Sample Count 統計を使用する。成功したユーザー登録リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。失敗したユーザー登録リクエストの合計数をカウントするには、CloudWatch を使用する。Math式を減算し、Sumの統計をSample Countの統計情報を使用する。  このメトリックは、各ユーザー・プール・クライアントのユーザー・プールごとに発行される。ユーザー登録が管理者によって実行された場合、メトリクスはユーザープールクライアントで管理する。  このメトリクスは、ユーザーインポートおよびユーザー移行の場合には発行されない。 |
| SignUpThrottles | Amazon Cognito ユーザープールに対してスロットリングされたユーザー登録リクエストの総数を提供する。ユーザー登録リクエストがスロットリングされるたびに、カウント 1 が発行される。  スロットリングされたユーザー登録リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用します。  このメトリックは、各クライアントのユーザー・プールごとに発行されます。スロットリングされたリクエストが管理者によって行われた場合、メトリクスはユーザープールクライアントで管理する。 |
| SignInSuccesses | Amazon Cognito ユーザープールに対して成功したユーザー認証リクエストの総数を提供する。認証トークンがユーザーに発行されると、ユーザー認証は成功したとみなされる。認証が成功すると値 1 が生成され、リクエストが失敗すると値 0 が生成される。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  成功したユーザー認証リクエストの割合を調べるには、このメトリクスの Average 統計を使用する。ユーザー認証リクエストの合計数をカウントするには、このメトリクスの Sample Count 統計を使用する。成功したユーザー認証リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。失敗したユーザー認証リクエストの合計数をカウントするには、Math式を減算し、Sumの統計をSample Countの統計情報を使用する。  このメトリックは、各クライアントのユーザー・プールごとに発行される。無効なユーザープールクライアントがリクエストで提供された場合、メトリクスの対応するユーザープールクライアント値には、固定値Invalidリクエストで送信された実際の無効な値の代わりに提供する。  Amazon Cognito トークンの更新リクエストは、このメトリクスには含まれないことに注意する。TokenRefreshSuccessesにより提供する。 |
| SignInThrottles | Amazon Cognito ユーザープールに対してスロットリングされたユーザー認証リクエストの総数を提供する。認証リクエストがスロットリングされるたびに、カウント 1 が発行される。  スロットリングされたユーザー認証リクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。  このメトリックは、各クライアントのユーザー・プールごとに発行される。無効なユーザープールクライアントがリクエストで提供された場合、メトリクスの対応するユーザープールクライアント値には、固定値Invalidリクエストで送信された実際の無効な値の代わりに提供する。  Amazon Cognito トークンの更新リクエストは、このメトリクスには含まれない。TokenRefreshThrottlesにより提供する。 |
| TokenRefreshSuccesses | Amazon Cognito ユーザープールに対して実行された Amazon Cognito トークンの更新に成功したリクエストの合計数を提供する。Amazon Cognito トークンの更新リクエストが成功すると、値 1 が生成されます。一方、失敗したリクエストでは 0 が生成される。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  Amazon Cognito トークンの更新リクエストの割合を調べるには、Averageこのメトリクスの [] の統計を表示する。Amazon Cognito トークンの更新リクエストの合計数をカウントするには、Sample Countこのメトリクスの [] の統計を表示する。Amazon Cognito トークンの更新リクエストの合計数をカウントするには、Sumこのメトリクスの [] の統計を表示する。Amazon Cognito トークンの更新に失敗したリクエストの総数をカウントするには、CloudWatch を使用する。Math式を減算し、Sumの統計をSample Countの統計情報を提供する。  このメトリクスは、各ユーザープールクライアントごとに発行される。無効なユーザープールクライアントが要求内にある場合、ユーザープールクライアントの値には固定値Invalidが入る。 |
| TokenRefreshThrottles | Amazon Cognito ユーザープールに対して実行された Amazon Cognito トークン更新のスロットリングされたリクエストの合計数を提供する。Amazon Cognito トークンの更新リクエストがスロットリングされるたびに、カウント 1 が発行される。  Amazon Cognito トークンの更新のスロットリングされたリクエストの合計数をカウントするには、Sumこのメトリクスの統計を表示する。  このメトリックは、各クライアントのユーザー・プールごとに発行される。無効なユーザープールクライアントがリクエストで提供された場合、メトリクスの対応するユーザープールクライアント値には、リクエストで送信された実際の無効な値の代わりに固定値Invalidが入る。 |
| FederationSuccesses | Amazon Cognito ユーザープールに対して成功した ID フェデレーションリクエストの総数を提供する。ID フェデレーションリクエストが成功すると値 1 が生成され、失敗すると値 0 が生成される。スロットリングされたリクエストも失敗したリクエストと見なされるため、スロットリングされたリクエストも 0 のカウントを生成する。  成功した ID フェデレーションリクエストの割合を調べるには、このメトリクスの Average 統計を使用する。ID フェデレーションリクエストの合計数をカウントするには、このメトリクスの Sample Count 統計を使用する。成功した ID フェデレーションリクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。失敗した ID フェデレーションリクエストの合計数をカウントするには、Math式を減算し、Sumの統計をSample Countの統計情報を使用する。 |
| FederationThrottles | Amazon Cognito ユーザープールに対してスロットリングされた ID フェデレーションリクエストの総数を提供する。ID フェデレーションリクエストがスロットリングされるたびに、カウント 1 が発行される。  スロットリングされた ID フェデレーションリクエストの合計数をカウントするには、このメトリクスの Sum 統計を使用する。 |
| CallCount | カテゴリに関連して顧客が発信したコールの総数を示す。このメトリックには、スロットル・コール、失敗したコール、成功したコールなど、すべてのコールが含まれる。  このメトリクスは、使用状況を表す。  カテゴリクォータは、アカウントおよびリージョンのすべてのユーザープールにわたって、各 AWS アカウントに対して適用される。  カテゴリ内のコールの合計数をカウントするには、Sumこのメトリクスの [] の統計を表示する。 |
| ThrottleCount | カテゴリに関連するスロットリングされたコールの総数を提供する。  このメトリクスは、使用状況を表す。  このメトリックは、アカウント・レベルで発行される。  カテゴリ内のコールの合計数を数えるには、Sumこのメトリクスの [] の統計を表示す。 |

#### Elasticsearch

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| クラスターメトリクス | ClusterStatus.green | 値 1 は、すべてのインデックスシャードがクラスターのノードに割り当てられることを示す。 |
|  | ClusterStatus.yellow | 値 1 は、すべてのインデックスのプライマリシャードがクラスターのノードに割り当てられていることを示すが、少なくとも 1 つのインデックスのレプリカシャードは割り当てられていない。 |
|  | ClusterStatus.red | 値 1 は、少なくとも 1 つのインデックスのプライマリとレプリカの両方のシャードが、クラスターのノードに割り当てられないことを示す。 |
|  | Nodes | Amazon ES クラスターのノード数 (例:専用マスターノードと UltraWarm ノード)。 |
|  | SearchableDocuments | クラスター内のすべてのデータノードで検索可能なドキュメントの合計数。 |
|  | DeletedDocuments | クラスター内のすべてのデータノードで削除対象としてマークされたドキュメントの合計数。これらのドキュメントは検索結果に表示されなくなっているが、Elasticsearch はセグメントマージ中にディスクから削除されたドキュメントのみを削除する。このメトリクスは、削除リクエスト後に増加し、セグメントマージ後に減少する。 |
|  | CPUUtilization | クラスター内のデータノードの CPU 使用率の割合。Maximum は、CPU 使用率が最も高いノードを示す。Average は、クラスター内のすべてのノードを表す。このメトリクスは、個別のノードでも利用できる。 |
|  | FreeStorageSpace | クラスター内のデータノードの空き容量。Sumは、クラスターの合計空き容量を示すが、正確な値を取得するには期間を 1 分のままにしておく必要がある。MinimumおよびMaximumは、それぞれ最小空き領域と最大の空き領域を持つノードを表示する。このメトリクスは、個別のノードでも利用できる。Amazon ES スローClusterBlockExceptionこのメトリックが0。復旧するには、インデックスを削除する、より大きなインスタンスを追加する、既存のインスタンスに EBS ベースのストレージを追加する、のいずれかを実行する必要がある。 |
|  | ClusterUsedSpace | クラスターの合計使用領域。正確な値を取得するには、期間を 1 分のままにしておく必要がある。 |
|  | ClusterIndexWritesBlocked | クラスターで、着信する書き込みリクエストを受け入れるか、ブロックするかを示す。値 0 では、クラスターでリクエストを受け入れる。値 1 ではリクエストをブロックする。一般的な要因には次のようなものがある。FreeStorageSpaceが低すぎる、またはJVMMemoryPressureが高すぎる。この問題を軽減するには、ディスク容量の追加やクラスターのスケーリングを検討する。 |
|  | JVMMemoryPressure | クラスター内のすべてのデータノードで使用する Java ヒープの最大パーセンテージ。Amazon ES は、インスタンスの RAM の半分を Java ヒープ (32 GiB のヒープサイズまで) に使用する。インスタンスは最大 64 GiB の RAM まで垂直スケーリングでき、それ以上はインスタンスを追加することで水平方向にスケーリングできる。 |
|  | AutomatedSnapshotFailure | クラスターの失敗した自動スナップショットの数。1 の値は、自動スナップショットが過去 36 時間、ドメイン用に取られなかったことを示す。 |
|  | CPUCreditBalance | クラスター内の、データノードに使用できる残りの CPU クレジット。CPU クレジットは、フル CPU パフォーマンスを 1 分間実現する。このメトリクスは、T2 インスタンスタイプでのみ使用できる。 |
|  | KibanaHealthyNodes | Kibana のヘルスチェック。最小値、最大値、平均値がすべて1に等しい場合、Kibanaは正常に動作している。最大が 1、最小が 0、平均が 0.7 の 10 個のノードがある場合、これは、7 個のノード (70%) が正常であり、3 個のノード (30%) が正常でないことを意味する。 |
|  | KMSKeyError | 値 1 は、保管時のデータを暗号化するために使用される KMS カスタマーマスターが無効になっていることを示す。通常のオペレーションにドメインを復元するには、キーを再度有効にする。コンソールでは、保管時のデータを暗号化するドメインに対してのみこのメトリクスが表示される。 |
|  | KMSKeyInaccessible | 値 1 は、保管時のデータを暗号化するために使用される KMS カスタマーマスターが削除されたか、Amazon ES への権限が失効したことを示す。この状態にあるドメインを復元することはできない。ただし、手動のスナップショットがある場合は、それを使用してドメインのデータを新しいドメインに移行できる。コンソールでは、保管時のデータを暗号化するドメインに対してのみこのメトリクスが表示される。 |
|  | InvalidHostHeaderRequests | Elasticsearch クラスターに対する HTTP リクエストのうち、ホストヘッダーが無効な (または欠落している) ものの数。有効なリクエストには、ホストヘッダー値としてドメインホスト名が含まれる。Amazon ES は、制限的なアクセスポリシーを持たないパブリックアクセスドメインの不正なリクエストを拒否する。すべてのドメインに制限付きアクセスポリシーを適用することをお勧めする。  このメトリクスで大きな値が表示される場合は、Elasticsearch クライアントのリクエストにドメインホスト名が含まれていることを確認する。(ない場合は、IP アドレスなど)。 |
|  | ElasticsearchRequests | Elasticsearch クラスターに対するリクエストの数。 |
|  | 2xx, 3xx, 4xx, 5xx | 特定の HTTP レスポンスコード (2xx、3xx、4xx、5xx) の発生につながった、ドメインへのリクエストの数。 |
| 専用マスターノードメトリクス | MasterCPUUtilization | 専用マスターノードが使用する CPU リソースの最大パーセンテージ。このメトリクスが 60 パーセントに達する場合、インスタンスタイプのサイズを増やすことをお勧めする。 |
|  | MasterFreeStorageSpace | このメトリクスは関係ないため無視できる。このサービスはデータノードとしてマスターノードを使用しない。 |
|  | MasterJVMMemoryPressure | クラスター内のすべての専用マスターノードで使用する Java ヒープの最大パーセンテージ。このメトリクスが 85 パーセントに達する場合、より大規模なインスタンスタイプに移行することをお勧めする。 |
|  | MasterCPUCreditBalance | クラスター内の専用マスターノードで使用できる、残りの CPU クレジット。CPU クレジットは、フル CPU パフォーマンスを 1 分間実現する。このメトリクスは、T2 インスタンスタイプでのみ使用できる。 |
|  | MasterReachableFromNode | MasterNotDiscovered 例外のヘルスチェック。値 1 は正常な動作を示す。値 0 は、/\_cluster/health/ の動作が正常ではないことを示す。  動作が正常でないとは、マスターノードが停止しているか、到達不可能であることを意味する。通常、これらの原因はネットワーク接続または AWS 依存関係の問題。t |
|  | MasterSysMemoryUtilization | 使用中のマスターノードのメモリの割合。 |
| EBS ボリュームメトリクス | ReadLatency | EBS ボリュームでの読み取り操作のレイテンシー (秒単位)。 |
|  | WriteLatency | EBS ボリュームでの書き込み操作のレイテンシー (秒単位)。 |
|  | ReadThroughput | EBS ボリュームでの読み取り操作のスループット (バイト/秒単位)。 |
|  | WriteThroughput | EBS ボリュームでの書き込み操作のスループット (バイト/秒単位)。 |
|  | DiskQueueDepth | EBS ボリュームに対する保留中の入出力 (I/O) リクエストの数。 |
|  | ReadIOPS | EBS ボリュームでの読み取り操作の入出力 (I/O) 操作数 (1 秒あたり)。 |
|  | WriteIOPS | EBS ボリュームでの書き込み操作の入出力 (I/O) 操作数 (1 秒あたり)。 |
| インスタンスメトリクス | IndexingLatency | インデックス作成オペレーションを完了するためにシャードで必要な平均時間 (ミリ秒)。 |
|  | IndexingRate | 1 分あたりのインデックス作成オペレーションの数。2 つのドキュメントを追加し、2 つのカウントを 4 つのオペレーションとして更新する \_bulk API への 1 回の呼び出し。これは 1 つ以上のノードに分散する可能性がある。そのインデックスに 1 つ以上のレプリカがある場合、クラスター内の他のノードにも合計 4 つのインデックス作成オペレーションが記録される。ドキュメントの削除はこのメトリクスに対してカウントされない。 |
|  | SearchLatency | 検索オペレーションを完了するためにデータノードのシャードで必要な平均時間 (ミリ秒)。 |
|  | SearchRate | データノードのすべてのシャードに対する 1 分あたりの検索リクエストの総数。\_search API への 1 回の呼び出しに対して、さまざまなシャードから結果が返される可能性がある。これらのシャードのうちの 5 つが 1 つのノードにある場合、クライアントが 1 つのリクエストしか行っていない場合でも、ノードはこのメトリクスについて 5 を報告する。 |
|  | SysMemoryUtilization | インスタンスが使用中のメモリの割合。このメトリクスの高い値は正常であり、通常はクラスターに問題はない。 |
|  | JVMGCYoungCollectionCount | 「新世代」ガベージコレクションが実行された回数。実行数が大量になり、かつ増え続けることは、通常のクラスター操作の一部。 |
|  | JVMGCYoungCollectionTime | クラスターで「新世代」ガベージコレクションの実行にかかった時間 (ミリ秒)。 |
|  | JVMGCOldCollectionCount | 「旧世代」ガベージコレクションが実行された回数。十分なリソースがあるクラスターでは、この回数は少ないままであるが、まれに増加する。 |
|  | JVMGCOldCollectionTime | クラスターで「旧世代」ガベージコレクションの実行にかかった時間 (ミリ秒)。 |
|  | KibanaConcurrentConnections | Kibanaへのアクティブな同時接続の数。この数が増え続ける場合は、クラスターのスケーリングを検討する。 |
|  | KibanaHealthyNode | 個々の Kibana ノードのヘルスチェック。値 1 は正常な動作を示す。値 0 は Kibana がアクセス不可であることを示す。 |
|  | KibanaHeapTotal | MiB 単位の Kibana に割り当てられたヒープメモリの量。EC2 インスタンスタイプが異なると、正確なメモリ割り当てに影響する可能性がある。 |
|  | KibanaHeapUsed | Kibana が使用するヒープメモリの絶対量（MiB）。 |
|  | KibanaHeapUtilization | Kibana が使用する使用可能なヒープメモリの最大パーセンテージ。この値が 80% を超える場合は、クラスターのスケーリングを検討する。 |
|  | KibanaOS1MinuteLoad | Kibanaの 1 分の CPU 負荷平均。CPU の負荷は、理想的には 1.00 未満にとどまるはず。一時的なスパイクは問題ないが、このメトリックスが一貫して 1.00 を超える場合は、インスタンスタイプのサイズを増やすことをお勧めする。 |
|  | KibanaRequestTotal | Kibana に対して行われた HTTP リクエストの合計数。システムの速度が遅い、または Kibana リクエストの数が多い場合は、インスタンスタイプのサイズを増やすことを検討する。 |
|  | KibanaResponseTimesMaxInMillis | Kibana がリクエストに応答するのに必要な最大時間 (ミリ秒)。リクエストで結果が返ってくるのに時間がかかる場合は、インスタンスタイプのサイズを増やすことを検討する。 |
|  | ThreadpoolForce\_mergeQueue | 強制マージスレッドプールでキューに入っているタスクの数。キューのサイズが一貫して大きい場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolForce\_mergeRejected | 強制マージスレッドプールで拒否されたタスクの数。この数が増え続ける場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolForce\_mergeThreads | 強制マージスレッドプールのサイズ。 |
|  | ThreadpoolIndexQueue | インデックス作成スレッドプールでキューに入っているタスクの数。キューのサイズが一貫して大きい場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolIndexRejected | インデックス作成スレッドプールで拒否されたタスクの数。この数が増え続ける場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolIndexThreads | インデックス作成スレッドプールのサイズ。 |
|  | ThreadpoolSearchQueue | 検索スレッドプールでキューに入っているタスクの数。キューのサイズが一貫して大きい場合は、クラスターのスケーリングを検討する。検索キューの最大サイズは 1,000。 |
|  | ThreadpoolSearchRejected | 検索スレッドプールで拒否されたタスクの数。この数が増え続ける場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolSearchThreads | 検索スレッドプールのサイズ。 |
|  | ThreadpoolBulkQueue | バルクスレッドプールでキューに入っているタスクの数。キューのサイズが一貫して大きい場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolBulkRejected | バルクスレッドプールで拒否されたタスクの数。この数が増え続ける場合は、クラスターのスケーリングを検討する。 |
|  | ThreadpoolBulkThreads | バルクスレッドプールのサイズ。 |
|  | ThreadpoolWriteThreads | 書き込みスレッドプールのサイズ。 |
|  | ThreadpoolWriteQueue | 書き込みスレッドプールでキューに入っているタスクの数。 |
|  | ThreadpoolWriteRejected | 書き込みスレッドプールで拒否されたタスクの数。 |
|  | CoordinatingWriteRejected | 最後の Amazon ES プロセスの起動以降のインデックス作成の圧力により、調整ノードで発生した拒否の総数。 |
|  | PrimaryWriteRejected | 最後の Amazon ES プロセスの起動以降のインデックス作成の圧力により、プライマリシャードで発生した拒否の総数。 |
|  | ReplicaWriteRejected | 最後の Amazon ES プロセスの起動以降のインデックス作成の負荷が原因で、レプリカシャードで発生した拒否の合計数。 |
| UltraWarm メトリクス | WarmCPUUtilization | クラスター内の UltraWarm ノードの CPU 使用率の割合。Maximum は、CPU 使用率が最も高いノードを示す。Average は、クラスター内のすべての UltraWarm ノードを表す。このメトリクスは、個々の UltraWarm ノードでも利用できる。正確な値を取得するには、期間を 1 分のままにしておく必要がある。 |
|  | WarmFreeStorageSpace | ウォームストレージの空き容量 (MiB)。UltraWarm はアタッチされたディスクではなく Amazon S3 を使用するため、Sumは関連する唯一の統計情報。 |
|  | WarmJVMMemoryPressure | UltraWarm ノードで使用する Java ヒープの最大割合。 |
|  | WarmSearchableDocuments | クラスター内のすべてのウォームインデックスで検索可能なドキュメントの合計数。正確な値を取得するには、期間を 1 分のままにしておく必要がある。 |
|  | WarmSearchLatency | 検索オペレーションを完了するために UltraWarm ノードのシャードで必要な平均時間 (ミリ秒)。 |
|  | WarmSearchRate | UltraWarm ノードのすべてのシャードに対する 1 分あたりの検索リクエストの総数。\_search API への 1 回の呼び出しに対して、さまざまなシャードから結果が返される可能性がある。これらのシャードのうちの 5 つが 1 つのノードにある場合、クライアントが 1 つのリクエストしか行っていない場合でも、ノードはこのメトリクスについて 5 を報告する。 |
|  | WarmStorageSpaceUtilization | クラスターで使用中のウォームストレージスペースの合計容量 (MiB 単位)。 |
|  | HotStorageSpaceUtilization | クラスターで使用しているホットストレージの合計容量。 |
|  | WarmSysMemoryUtilization | 使用中のウォームノードのメモリの割合。 |
|  | HotToWarmMigrationQueueSize | 現在、ホットストレージからウォームストレージに移行するのを待機しているインデックスの数。 |
|  | WarmToHotMigrationQueueSize | 現在、ウォームストレージからホットストレージに移行するのを待機しているインデックスの数。 |
|  | HotToWarmMigrationFailureCount | 失敗したホット・ツー・ウォーム移行の合計数。 |
|  | HotToWarmMigrationForceMergeLatency | 移行プロセスの強制マージステージの平均待ち時間。 |
|  | HotToWarmMigrationSnapshotLatency | 移行プロセスのスナップショット段階の平均待機時間。このステージに常に時間がかかりすぎる場合は、シャードが適切にサイズ設定され、クラスター全体に分散されていることを確認する。 |
|  | HotToWarmMigrationProcessingLatency | ホットからウォームへの移行が成功した場合の平均レイテンシーないキュー内で過ごした時間を含む。この値は、移行プロセスの強制マージ、スナップショット、およびシャード再配置ステージを完了するのにかかる時間の合計。 |
|  | HotToWarmMigrationSuccessCount | ホットからウォームへの移行に成功した合計数。 |
|  | HotToWarmMigrationSuccessLatency | ホットからウォームへの移行が成功した場合の平均レイテンシー（キューに費やされた時間を含む）。 |
| コールドストレージのメトリクス | ColdStorageSpaceUtilization | クラスターで使用しているコールドストレージスペースの合計容量 (MiB 単位)。 |
|  | ColdToWarmMigrationFailureCount | コールドからウォームへの移行に失敗した合計数。 |
|  | ColdToWarmMigrationLatency | コールドからウォームへの移行が完了するまでの時間。 |
|  | ColdToWarmMigrationQueueSize | 現在、コールドストレージからウォームストレージに移行するのを待機しているインデックスの数。 |
|  | ColdToWarmMigrationSuccessCount | コールドからウォームへの移行に成功した合計数。 |
|  | WarmToColdMigrationFailureCount | ウォームからコールドへの移行に失敗した合計数。 |
|  | WarmToColdMigrationLatency | ウォームからコールドへの移行が正常に完了するまでの時間。 |
|  | WarmToColdMigrationQueueSize | 現在、ウォームストレージからコールドストレージに移行するのを待機しているインデックスの数。 |
|  | WarmToColdMigrationSuccessCount | ウォームからコールドへの移行に成功した合計数。 |
| アラートメトリクス | AlertingDegraded | 値 1 は、アラートインデックスが赤であるか、1 つ以上のノードがスケジュールどおりでないことを意味する。値 0 は正常な動作を示す。 |
|  | AlertingIndexExists | 値 1 は、.opendistro-alerting-config インデックスが存在することを意味する。値 0 は、そのインデックスが存在しないことを意味する。アラート機能を初めて使用するまで、この値は 0 のまま。 |
|  | AlertingIndexStatus.green | インデックスのヘルス。値 1 は、緑を意味する。値 0 は、インデックスが存在しないか、緑ではないことを意味する。 |
|  | AlertingIndexStatus.red | インデックスのヘルス。値 1 は、赤を意味する。値 0 は、インデックスが存在しないか、赤でないことを意味する。 |
|  | AlertingIndexStatus.yellow | インデックスのヘルス。値 1 は、黄色を意味する。値 0 は、インデックスが存在しないか、黄色でないことを意味する。 |
|  | AlertingNodesNotOnSchedule | 値 1 は、一部のジョブがスケジュールどおりに実行されていないことを意味する。値 0 は、すべてのアラートジョブがスケジュールどおりに実行されていることを意味する (またはアラートジョブが存在しないことを意味する)。Amazon ES コンソールを確認するか、\_nodes/statsリクエストを実行して、リソースの使用率が高いノードがあるかどうかを確認する。 |
|  | AlertingNodesOnSchedule | 値 1 は、すべてのアラートジョブがスケジュールどおりに実行されていることを意味する (またはアラートジョブが存在しないことを意味する)。値 0 は、一部のジョブがスケジュールどおりに実行されていないことを意味する。 |
|  | AlertingScheduledJobEnabled | 値 1 は、opendistro.scheduled\_jobs.enabled クラスター設定が true であることを意味する。値 0 は、その設定が false であり、スケジュールされたジョブが無効であることを意味する。 |
| 異常検出メトリクス | AnomalyDetectionPluginUnhealthy | 値 1 は、異常検出プラグインが正しく動作していないことを意味する。これは、障害の数が多いか、使用されているインデックスの 1 つが赤の状態であるため。値 0 は、プラグインが想定どおりに動作していることを示す。 |
|  | AnomalyDetectionRequestCount | 異常検出のリクエストの数。 |
|  | AnomalyDetectionFailureCount | 異常検出に失敗したリクエストの数。 |
|  | AnomalyResultsIndexStatusIndexExists | 値 1 は、.opendistro-anomaly-results エイリアスが指すインデックスが存在することを意味する。異常検出機能を初めて使用するまで、この値は 0 のまま。 |
|  | AnomalyResultsIndexStatus.red | 値 1 は、 .opendistro-anomaly-results エイリアスが指すインデックスが赤の状態であることを意味する。値 0 は、そうでないことを意味する。異常検出機能を初めて使用するまで、この値は 0 のまま。 |
|  | AnomalyDetectorsIndexStatusIndexExists | 値 1 は、.opendistro-anomaly-detectors インデックスが存在することを意味する。値 0 は、そのインデックスが存在しないことを意味する。異常検出機能を初めて使用するまで、この値は 0 のまま。 |
|  | AnomalyDetectorsIndexStatus.red | 値 1 は、.opendistro-anomaly-detectors インデックスが赤の状態であることを意味する。値 0 は、そうでないことを意味する。異常検出機能を初めて使用するまで、この値は 0 のまま |
|  | ModelsCheckpointIndexStatusIndexExists | 値 1 は、.opendistro-anomaly-checkpoints インデックスが存在することを意味する。値 0 は、そのインデックスが存在しないことを意味する。異常検出機能を初めて使用するまで、この値は 0 のまま。 |
|  | ModelsCheckpointIndexStatus.red | 値 1 は、.opendistro-anomaly-checkpoints インデックスが赤の状態であることを意味する。値 0 は、そうでないことを意味する。異常検出機能を初めて使用するまで、この値は 0 のまま。 |
| 非同期検索のメトリクス | AsynchronousSearchSubmissionRate | 過去 1 分間に送信された非同期検索の数。 |
| 非同期検索コーディネータノードの統計 (コーディネータノードあたり) | AsynchronousSearchInitializedRate | 過去 1 分間に初期化された非同期検索の数。 |
|  | AsynchronousSearchCompletionRate | 過去 1 分間に正常に完了した非同期検索の数。 |
|  | AsynchronousSearchFailureRate | 直前までに完了し、失敗した非同期検索の数。 |
|  | AsynchronousSearchPersistRate | 過去 1 分間に持続した非同期検索の数。 |
|  | AsynchronousSearchPersistFailedRate | 直前までに持続できなかった非同期検索の数。 |
|  | AsynchronousSearchRejected | ノードの稼働時間以降に拒否された非同期検索の合計数。 |
|  | AsynchronousSearchCancelled | ノードの稼働時間以降にキャンセルされた非同期検索の合計数。 |
|  | AsynchronousSearchMaxRunningTime | 過去 1 分間にノード上で実行されている非同期検索の最長時間。 |
| 非同期検索のメトリクス  非同期検索クラスター統計 | AsynchronousSearchStoreHealth | 直近の永続化されたインデックス（赤/赤以外）内のストアの健全性。 |
| AsynchronousSearchStoreSize | 過去 1 分間に、すべてのシャードにわたるシステムインデックスのサイズ。 |
|  | AsynchronousSearchStoredResponseCount | 過去 1 分間にシステムインデックスに保存されたレスポンスの数。 |
| SQL メトリクス | SQLFailedRequestCountByCusErr | クライアントの問題により失敗した \_opendistro/\_sql API へのリクエストの数。たとえば、IndexNotFoundException により、リクエストが HTTP ステータスコード 400 を返す場合がある。 |
|  | SQLFailedRequestCountBySysErr | サーバーの問題または機能の制限により失敗した \_opendistro/\_sql API へのリクエストの数。たとえば、VerificationException により、リクエストが HTTP ステータスコード 503 を返す場合がある。 |
|  | SQLRequestCount | \_opendistro/\_sql API へのリクエストの数。 |
|  | SQLDefaultCursorRequestCount | SQLRequestCount に似ていますが、カウント対象はページ分割リクエストのみ。 |
|  | SQLUnhealthy | 値 1 は、特定のリクエストへのレスポンスで、SQL プラグインが 5 を返すことを示す。xxレスポンスコードを使用するか、無効なクエリDSLをElasticsearchに渡す 他のリクエストは引き続き成功する。値 0 は、最近の障害がないことを示す。値 1 が持続して表示される場合、クライアントがプラグインに対して行っているリクエストのトラブルシューティングを行う。 |
| k-NN メトリクス | KNNCacheCapacityReached | キャッシュ容量に達したかどうかを示すノード単位のメトリック。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNCircuitBreakerTriggered | 回路ブレーカーがトリガーされるかどうかを示すクラスタ単位のメトリック。いずれかのノードが 1 の値を返す場合、KNNCacheCapacityReachedの場合、この値も 1 を返す。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNEvictionCount | メモリ制約またはアイドル時間のためにキャッシュからエビクトされたグラフ数のノード単位のメトリック。インデックスの削除のために発生した明示的な削除はカウントされない。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNGraphIndexErrors | 追加するリクエスト数のノードごとのメトリック。knn\_vectorフィールドを、エラーを生成したグラフに設定する |
|  | KNNGraphIndexRequests | 追加するリクエスト数のノードごとのメトリック。knn\_vectorフィールドをグラフに追加する。 |
|  | KNNGraphMemoryUsage | 現在のキャッシュ・サイズ（メモリ内のすべてのグラフの合計サイズ）のノードごとのメトリック（キロバイト単位）。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNGraphQueryErrors | エラーを生成したグラフクエリの数を表すノード単位のメトリック。 |
|  | KNNGraphQueryRequests | グラフクエリ数のノード単位のメトリック。 |
|  | KNNHitCount | キャッシュ・ヒット数のノード単位のメトリック。キャッシュ・ヒットは、ユーザーがすでにメモリにロードされているグラフを照会したときに発生する。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNLoadExceptionCount | グラフをキャッシュにロードしようとしたときに例外が発生した回数を示すノード単位のメトリック。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNLoadSuccessCount | プラグインがグラフをキャッシュに正常にロードした回数を示すノード単位のメトリック。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNMissCount | キャッシュミスの数のノード単位のメトリック。キャッシュミスは、ユーザーがまだメモリにロードされていないグラフを照会したときに発生する。この指標は、おおよそのK-NN検索にのみ関係する。 |
|  | KNNQueryRequests | k-nN プラグインが受信したクエリ要求数のノード単位のメトリック。 |
|  | KNNScriptCompilationErrors | スクリプトのコンパイル中のエラー数のノード単位のメトリック。この統計は、K-nN スコアスクリプト検索にのみ関係する。 |
|  | KNNScriptCompilations | k-nn スクリプトがコンパイルされた回数のノードごとのメトリック。通常、この値は 1 または 0 でなければならないが、コンパイルされたスクリプトを含むキャッシュがいっぱいになると、K-nn スクリプトが再コンパイルされる可能性がある。この統計は、K-nN スコアスクリプト検索にのみ関係する。 |
|  | KNNScriptQueryErrors | スクリプトクエリ中のエラー数を表すノード単位のメトリック。この統計は、K-nN スコアスクリプト検索にのみ関係する。 |
|  | KNNScriptQueryRequests | スクリプトクエリーの合計数に対するノード単位のメトリック。この統計は、K-nN スコアスクリプト検索にのみ関係する。 |
|  | KNNTotalLoadTime | k-nn がグラフをキャッシュにロードするのにかかった時間（ナノ秒）。この指標は、おおよそのK-NN検索にのみ関係する。 |
| クラスター間検索のメトリクス  ソースドメインのメトリクス | CrossClusterOutboundConnections | 接続されたノードの数。スキップされたドメインが 1 つ以上レスポンスに含まれている場合は、このメトリクスを使用して異常な接続を追跡する。この数が 0 になった場合、その接続は正常ではない。 |
|  | CrossClusterOutboundRequests | ターゲットドメインに送信された検索リクエストの数。ドメインでクラスター間検索リクエストが過負荷になっているかどうかを確認し、このメトリクスのスパイクと JVM/CPU スパイクの関連性を探るために使用する。 |
| クラスター間検索のメトリクス  指標をランク付けする学習 | CrossClusterInboundRequests | ソースドメインから受信した着信接続リクエストの数。 |
| 指標をランク付けする学習 | LTRRequestTotalCount | ランク付けリクエストの合計数。 |
|  | LTRRequestErrorCount | 失敗したリクエストの合計数。 |
|  | LTRStoreIndexIsRed | プラグインの実行に必要なインデックスの1つが赤であるかどうかを追跡する。 |
|  | LTRMemoryUsage | プラグインで使用されるメモリの合計。 |

#### DataSync

|  |  |
| --- | --- |
| メトリクス | 内容 |
| BytesVerifiedSource | 送信元の場所で検証されたデータの合計バイト数。 |
| BytesPreparedSource | 送信元の場所で準備されたデータの合計バイト数。 |
| FilesVerifiedSource | 送信元の場所で検証されたファイルの合計数。 |
| FilesPreparedSource | 送信元の場所で準備されたファイルの合計数。 |
| BytesVerifiedDestination | 送信先の場所で検証されたデータの合計バイト数。 |
| BytesPreparedDestination | 送信先の場所で準備されたデータの合計バイト数。 |
| FilesVerifiedDestination | 送信先の場所で検証されたファイルの合計数。 |
| FilesPreparedDestination | 送信先の場所で準備されたファイルの合計数。 |
| FilesTransferred | ネットワーク経由で転送された実際のファイル数またはメタデータ。この値は、計算され、TRANSFERRING (転送中) フェーズに継続的に更新される。これは、各ファイルが送信元の場所から読み取られるごとに定期的に更新され、ネットワーク経由で送信さる。  転送中に障害が発生した場合、この値は EstimatedFilesToTransfer 未満になることがある。場合によっては、この値は EstimatedFilesTransferred より大きくなることもある。一部の場所タイプではこの要素が実装固有であるため、正確なファイル数あるいはタスク実行のモニタリングのインジケータとしてはこれを使用しない。 |
| BytesTransferred | エージェントが送信元の場所から送信先の場所に読み込む際に、ネットワーク経由で転送された合計バイト数。 |
| BytesWritten | 送信先の場所に転送されたすべてのファイルの合計論理サイズ。 |

#### Kinesis Data Firehose

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| Amazon S3 への配信 | DeliveryToS3.Bytes | 指定された期間に Amazon S3 に配信されたバイト数。 |
|  | DeliveryToS3.DataFreshness | Kinesis Data Firehose の最も古いレコードの経過時間。この経過時間より古いレコードは S3 バケットに配信済み。 |
|  | DeliveryToS3.Records | 指定された期間に Amazon S3 に配信されたレコード数。 |
|  | DeliveryToS3.Success | すべての Amazon S3 put コマンドの合計に対する正常に実行された Amazon S3 put コマンドの合計。 |
|  | BackupToS3.Bytes | 指定された期間に バックアップがAmazon S3 に配信されたバイト数。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
|  | BackupToS3.DataFreshness | バックアップに関するKinesis Data Firehose の最も古いレコードの経過時間。この経過時間より古いレコードは Amazon S3 バケットに配信済み。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
|  | BackupToS3.Records | 指定された期間にバックアップが Amazon S3 に配信されたレコードの数。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
|  | BackupToS3.Success | すべての Amazon S3 バックアップの put コマンドの合計に対する、成功したバックアップの Amazon S3 put コマンドの合計。Kinesis Data Firehose は、バックアップが有効になっているとき (データ変換も有効になっている場合にのみ可能) に、このメトリクスを送信する。 |
| - | ResourceCount | アカウントで実行されている指定されたリソースの数。リソースは、メトリクスに関連付けられたディメンションによって定義される。  このメトリクスで最も役に立つ統計は MAXIMUM 。これは、1 分間の期間中に使用されるリソースの最大数を表す。 |

#### KMS

|  |  |
| --- | --- |
| メトリクス | 内容 |
| SecondsUntilKeyMaterialExpiration | インポートしたキーマテリアルの有効期限までの残りの秒数。このメトリックスは、オリジンがEXTERNALキーマテリアルの有効期限が設定された このメトリクスで最も有用な統計は Minimum で、指定した統計期間のすべてのデータポイントの最小残り時間を示す。 |

#### Lambda

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| 呼び出しメトリクス | Invocations | 関数コードが実行された回数(成功した実行や関数エラーが発生した実行を含む)。呼び出しリクエストがスロットリングされた場合、呼び出しは記録されない。それ以外の場合は、呼び出しエラーになる。これは、請求対象リクエストの数に等しくなる。 |
|  | Errors | 関数エラーが発生した呼び出しの数。関数エラーには、コードによってスローされた例外と、Lambda ランタイムによってスローされた例外が含まれる。ランタイムは、タイムアウトや設定エラーなどの問題に対してエラーを返す。エラー率を計算するには、Errors の値を Invocations の値で割る。エラーメトリクスのタイムスタンプは、エラーが発生した時点ではなく、関数が呼び出された時間を反映していることに注意する。 |
|  | DeadLetterErrors | 非同期呼び出しの場合、Lambda がイベントをデッドレターキューに送信しようとしたが、失敗した回数。デッドレターエラーは、アクセス許可エラー、リソースの設定ミス、またはサイズ制限が原因で発生する可能性がある。 |
|  | DestinationDeliveryFailures | 非同期呼び出しの場合、Lambda がイベントを送信先に送信しようとしたが、失敗した回数。配信エラーは、アクセス許可エラー、リソースの設定ミス、またはサイズ制限が原因で発生する可能性がある。 |
|  | Throttles | スロットリングされた呼び出しリクエストの数。すべての関数インスタンスがリクエストを処理していて、スケールアップできる同時実行がない場合、Lambda は TooManyRequestsException を使用して追加のリクエストを拒否する。スロットリングされたリクエストやその他の呼び出しエラーは、Invocations または Errors としてカウントされない。 |
|  | ProvisionedConcurrencyInvocations | プロビジョニングされた同時実行で関数コードが実行される回数。 |
|  | ProvisionedConcurrencySpilloverInvocations | プロビジョニングされたすべての同時実行が使用されているときに、標準同時実行で関数コードが実行される回数。 |
| パフォーマンスメトリクス | Duration | 関数コードがイベントの処理に費やす時間。呼び出しの請求期間は、最も近いミリ秒に切り上げた Duration の値。 |
|  | PostRuntimeExtensionsDuration | 関数コードの完了後、拡張のためにランタイムがコードの実行に費やした累積時間。 |
|  | IteratorAge | ストリームから読み取るイベントソースマッピングの場合、イベントの最後のレコードの所要時間。所要時間は、ストリームがレコードを受信してから、イベントソースマッピングがイベントを関数に送信するまでの時間。 |
| 同時実行メトリクス | ConcurrentExecutions | イベントを処理している関数インスタンスの数。この数値がリージョンの同時実行クォータ、または関数で設定した予約済み同時実行制限に達すると、追加の呼び出しリクエストがスロットリングされる。 |
|  | ProvisionedConcurrentExecutions | プロビジョニングされた同時実行でイベントを処理している関数インスタンスの数。プロビジョニングされた同時実行数を割り当てたエイリアスまたはバージョンの呼び出しごとに、Lambda は現在のカウントを出力する。 |
|  | ProvisionedConcurrencyUtilization | バージョンまたはエイリアスの場合、ProvisionedConcurrentExecutions の値を、割り当て済みのプロビジョニングされた同時実行の合計量で割った値。たとえば、.5 は、割り当て済みのプロビジョニングされた同時実行数の 50% が使用中であることを示す。 |
|  | UnreservedConcurrentExecutions | 同時実行が予約されていない関数によって処理されているイベントの数。 |

#### RDS

|  |  |
| --- | --- |
| メトリクス | 内容 |
| BinLogDiskUsage | プライマリでバイナリログが占有するディスク領域の量。MySQL リードレプリカに適用される。 |
| BlockedRequests | 汎用 SSD (gp2) のバーストバケット I/O クレジットの利用可能パーセント。 |
| CPUUtilization | CPU 使用率。 |
| CPUCreditUsage | (T2 インスタンスの場合)  CPU 使用率に関してインスタンスで消費される CPU クレジットの数。1 CPUクレジットは、1 分間 100％ の使用率で実行される 1 つの vCPU、または vCPU、使用率、時間の同等の組み合わせに相当する。たとえば、2 分間 50％ の使用率で実行されている 1 つの vCPU、または 2 分間 25％ の使用率で実行されている 2 つの vCPU があるとする。  CPU クレジットメトリクスは、5 分間隔でのみ利用可能。5 分を超える期間を指定する場合は、Sum 統計の代わりに Average 統計を使用する。 |
| CPUCreditBalance | (T2 インスタンスの場合)  インスタンスが起動または開始後に蓄積した獲得 CPU クレジットの数。T2 スタンダードの場合、CPUCreditBalance には蓄積された起動クレジットの数も含まれる。  クレジットは、獲得後にクレジット残高に蓄積され、消費されるとクレジット残高から削除される。クレジット残高には、インスタンスサイズによって決まる上限がある。制限に到達すると、獲得された新しいクレジットはすべて破棄される。T2 スタンダードの場合、起動クレジットは制限に対してカウントされない。  CPUCreditBalance のクレジットは、インスタンスがそのベースライン CPU 使用率を超えてバーストするために消費できる。  インスタンスが実行中の場合、CPUCreditBalance のクレジットは期限切れにならない。インスタンスが停止すると、CPUCreditBalance は保持されず、蓄積されたすべてのクレジットが失われる。  CPU クレジットメトリクスは、5 分間隔でのみ利用可能。 |
| DatabaseConnections | 使用中のデータベース接続の数。  メトリクス値には、データベースによってまだクリーンアップされていない、切断されたデータベース接続が含まれていない可能性がある。したがって、データベースによって記録されるデータベース接続の数は、メトリクス値よりも多い可能性がある。 |
| DiskQueueDepth | 未処理のディスク I/O アクセス (読み取り/書き込みリクエスト) の数。 |
| EBSByteBalance% | RDS データベースのバーストバケットに残っているスループットクレジットの割合。このメトリクスは基本モニタリング専用。  このメトリクスをサポートするインスタンスサイズを確認するには、Linux インスタンス用 Amazon EC2 ユーザーガイド の「デフォルトで最適化された EBS」の表で、アスタリスク (\*) の付いたインスタンスサイズを参照する。Sum 統計は、このメトリクスに該当しない。 |
| EBSIOBalance% | RDS データベースのバーストバケットに残っている I/O クレジットの割合。このメトリクスは基本モニタリング専用。  このメトリクスをサポートするインスタンスサイズを確認するには、Linux インスタンス用 Amazon EC2 ユーザーガイド の「デフォルトで最適化された EBS」の表で、アスタリスク (\*) の付いたインスタンスサイズを参照する。Sum 統計は、このメトリクスに該当しない。 |
| FailedSQLServerAgentJobsCount | 直近 1 分間に失敗した Microsoft SQL Server エージェントジョブの数。 |
| FreeableMemory | 使用可能な RAM の容量。  MariaDB、MySQL、Oracle、および PostgreSQL DB インスタンスの場合、このメトリクスは /proc/meminfo の MemAvailable フィールドの値を報告する。 |
| FreeStorageSpace | 使用可能なストレージ領域の容量。 |
| MaximumUsedTransactionIDs | 最大使用済みトランザクション ID 数。PostgreSQL に適用る。 |
| NetworkReceiveThroughput | モニタリングとレプリケーションに使用する顧客データベーストラフィックと Amazon RDS トラフィックの両方を含む、DB インスタンスの受信ネットワークトラフィック。 |
| NetworkTransmitThroughput | モニタリングとレプリケーションに使用する顧客データベーストラフィックと Amazon RDS トラフィックの両方を含む、DB インスタンスの送信ネットワークトラフィック。 |
| OldestReplicationSlotLag | 受信した先行書き込み (WAL) データに関して最も遅延の長いレプリカの遅延サイズ。PostgreSQL に適用される。 |
| ReadIOPS | 1 秒あたりのディスク読み取り I/O 操作の平均回数。 |
| ReadLatency | 1 回のディスク I/O 操作にかかる平均時間。 |
| ReadThroughput | 1 秒あたりのディスクからの平均読み取りバイト数。 |
| ReplicaLag | ソース DB インスタンスからリードレプリカ DB インスタンスまでのラグ。MySQL、MariaDB、Oracle、PostgreSQL、および SQL Server のリードレプリカに適用される。 |
| ReplicationSlotDiskUsage | レプリケーションスロットファイルで使用されているディスク容量。PostgreSQL に適用される。 |
| SwapUsage | DB インスタンスで使用するスワップ領域の量。このメトリクスは SQL Server では利用できない。 |
| TransactionLogsDiskUsage | トランザクションログで使用されているディスク容量。PostgreSQL に適用される。 |
| TransactionLogsGeneration | 1 秒あたりに生成されるトランザクションログのサイズ。PostgreSQL に適用される。 |
| WriteIOPS | 1 秒あたりのディスク書き込み I/O 操作の平均回数。 |
| WriteLatency | 1 回のディスク I/O 操作にかかる平均時間。 |
| WriteThroughput | 1 秒あたりのディスクへの平均書き込みバイト数。 |

#### Route53

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| ヘルスチェック | ChildHealthCheckHealthyCount | Route 53 がモニタリングしているヘルスチェック間で正常なヘルスチェックの数。 |
|  | ConnectionTime | Route 53 ヘルスチェッカーがエンドポイントとの TCP 接続を確立するのにかかった平均時間。ヘルスチェックの ConnectionTime は、すべてのリージョンまたは選択した地理的リージョンについて確認できる。 |
|  | HealthCheckPercentageHealthy | Route 53 ヘルスチェッカーが選択したエンドポイントを正常であるとみなす割合。HealthCheckPercentageHealthy は、すべてのリージョンについてのみ確認できる (選択したリージョンについてのデータは表示できない)。 |
|  | HealthCheckStatus | Route53がチェックしているヘルスチェックエンドポイントのステータス。1 は正常、0 は異常を示します。HealthCheckStatus は、すべてのリージョンについてのみ確認できる (選択したリージョンについてのデータは表示できない)。 |
|  | SSLHandshakeTime | Route 53 ヘルスチェッカーが SSL ハンドシェイクを完了するまでにかかった平均時間。ヘルスチェックの SSLHandshakeTime は、すべてのリージョンまたは選択した地理的リージョンについて確認できる。 |
|  | TimeToFirstByte | Route 53 ヘルスチェッカーが HTTP または HTTPS リクエストへの応答の先頭バイトを受け取るまでにかかった平均時間。ヘルスチェックの TimeToFirstByte は、すべてのリージョンまたは選択した地理的リージョンについて確認できる。 |
| ホストゾーン | DNSQueries | ホストゾーン内のすべてのレコードについて、指定された期間に Route 53 が応答する DNS クエリの数。 |
|  | DNSSECInternalFailure | ホストゾーン内のオブジェクトが INTERNAL\_FAILURE 状態の場合、値は 1 。それ以外の場合、値は 0 。 |
|  | DNSSECKeySigningKeysNeedingAction | ACTION\_NEEDED 状態 (KMS の障害のため) を持つキー署名キー (KSKs) の数。 |
|  | DNSSECKeySigningKeyMaxNeedingActionAge | キー署名キー (KSK) が ACTION\_NEEDED 状態に設定されてから経過した時間。 |
|  | DNSSECKeySigningKeyAge | キー署名キー (KSK) が作成されてから経過した時間 (アクティブ化されてからではありません)。 |
| リゾルバーエンドポイント | InboundQueryVolume | インバウンドエンドポイント、またはIPアドレスを対象とし、EndpointId で指定されたエンドポイントを介してネットワークから VPC に転送された DNS クエリの数。 |
|  | OutboundQueryVolume | アウトバウンドエンドポイントを対象とし、EndpointId で指定されたエンドポイントを介して VPC からネットワークに転送された DNS クエリの数。 |
|  | OutboundQueryAggregateVolume | アウトバウンドエンドポイント、またはIPアドレスを対象とし、、Amazon VPC からネットワークに転送された 以下を含むDNS クエリの総数。  ・EndpointId で指定されたエンドポイントを介して VPC からネットワークに転送された DNS クエリの数。  ・現在のアカウントが他のアカウントと リゾルバー ルールを共有する場合、EndpointId によって指定されたエンドポイントを介してネットワークに転送される、他のアカウントによって作成された VPC からのクエリ。 |
| リゾルバー IP アドレス | InboundQueryVolume | インバウンドエンドポイントの IP アドレスごとに、ネットワークから、指定された IP アドレスに転送された DNS クエリの数。各 IP アドレスは、IP アドレス ID で識別されます。この値は Route 53 コンソールを使用して取得できる。該当するエンドポイントのページの [IP アドレス] セクションで、[IP アドレス ID] 列を参照する。また、ListResolverEndpointIpAddresses を使用してプログラムで値を取得することもできる。 |
|  | OutboundQueryAggregateVolume | アウトバウンドエンドポイントの IP アドレスごとに、Amazon VPC からネットワークに転送された 以下を含むDNS クエリの総数。  ・指定された IP アドレスを使用して VPC からネットワークに転送された DNS クエリの数。  ・現在のアカウントが他のアカウントと リゾルバー ルールを共有する場合、指定された IP アドレスを介してネットワークに転送される、他のアカウントによって作成された VPC からのクエリ。  各 IP アドレスは、IP アドレス ID で識別される。この値は Route 53 コンソールを使用して取得できる。該当するエンドポイントのページの [IP アドレス] セクションで、[IP アドレス ID] 列を参照する。また、ListResolverEndpointIpAddresses を使用してプログラムで値を取得することもできる。 |

#### S3

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| 日次ストレージメトリクス | BucketSizeBytes | STANDARD ストレージクラス、INTELLIGENT\_TIERING ストレージクラス、標準低頻度アクセス (STANDARD\_IA) ストレージクラス、OneZone 低頻度アクセス (ONEZONE\_IA)、低冗長化ストレージ (RRS) クラス、ディープアーカイブストレージ (S3 Glacier Deep Archive)、または Glacier (GLACIER) ストレージクラスのバケットに保存されているデータの量 (バイト単位)。この値を計算するには、バケット内のすべてのオブジェクト (最新のオブジェクトと最新でないオブジェクトの両方) のサイズを合計する。これには、バケットに対するすべての不完全なマルチパートアップロードのすべてのパートのサイズも含める。 |
|  | NumberOfObjects | すべてのストレージクラスのバケットに保存されたオブジェクトの総数。この値を計算するには、バケット内のすべてのオブジェクト (最新のオブジェクトと最新でないオブジェクトの両方) と、バケットに対するすべての不完全なマルチパートアップロードの合計パート数をカウントする。 |
| リクエストメトリクス | AllRequests | タイプに関係なく、Amazon S3 バケットに対して行われた HTTP リクエストの総数。フィルタでメトリクス設定を使用している場合、このメトリクスはフィルタの要件を満たすバケット内のオブジェクトに対する HTTP リクエストのみを返す。 |
|  | GetRequests | Amazon S3 バケット内のオブジェクトに対して行われた HTTP GET リクエストの数。これには、リストオペレーションは含まれない。 |
|  | PutRequests | Amazon S3 バケット内のオブジェクトに対して行われた HTTP PUT リクエストの数。 |
|  | DeleteRequests | Amazon S3 バケットのオブジェクトに対して行われた HTTP DELETE リクエストの数。これには、複数オブジェクトの削除リクエストも含まれる。このメトリクスは、削除されるオブジェクトの数ではなくリクエストの数を示す。 |
|  | HeadRequests | Amazon S3 バケットに対して行われた HTTP HEAD リクエストの数。 |
|  | PostRequests | Amazon S3 バケットに対して行われた HTTP POST リクエストの数。 |
|  | SelectRequests | Amazon S3 バケットのオブジェクトに対して行われた Amazon S3 の SELECT Object Content リクエストの数。 |
|  | SelectBytesScanned | Amazon S3 バケットの Amazon S3 の SELECT Object Content リクエストでスキャンされたデータのバイト数。 |
|  | SelectBytesReturned | Amazon S3 バケットの Amazon S3 の SELECT Object Content リクエストで返されたデータのバイト数。 |
|  | ListRequests | バケットの内容をリストする HTTP リクエストの数。 |
|  | BytesDownloaded | Amazon S3 バケットに対する、レスポンスに本文が含まれるリクエストに対してダウンロードしたバイト数。 |
|  | BytesUploaded | Amazon S3 バケットに対する、リクエストボディを含むアップロードしたバイト数。 |
|  | 4xxErrors | Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 4xx クライアントエラーステータスコードリクエストの数。average 統計はエラーレートを示し、sum 統計は各期間中のそのタイプのエラー数を示す。 |
|  | 5xxErrors | Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 5xx サーバーエラーステータスコードリクエストの数。average 統計はエラーレートを示し、sum 統計は各期間中のそのタイプのエラー数を示す。 |
|  | FirstByteLatency | Amazon S3 バケットがリクエスト全体を受信してからレスポンスの返信が開始するまでのリクエストあたりの時間。 |
|  | TotalRequestLatency | 最初のバイトが受信されてから Amazon S3 バケットに最後のバイトが送信されるまでのリクエストあたりの経過時間。これには、FirstByteLatency には含まれない、リクエストボディの受信とレスポンス本文の送信にかかった時間が含まれる。 |
| レプリケーションメトリクス | ReplicationLatency | 特定のレプリケーションルールについて、レプリケート先リージョンがレプリケート元リージョンより遅れる最大秒数。 |
|  | BytesPendingReplication | 特定のレプリケーションルールについて、レプリケーションが保留中のオブジェクトの合計バイト数。 |
|  | OperationsPendingReplication | 特定のレプリケーションルールについて、レプリケーションが保留中のオペレーションの数。 |
| Outpostsメトリクス | OutpostTotalBytes | Outpost のプロビジョニングされた合計キャパシティー (バイト単位)。 |
|  | OutpostFreeBytes | お客様のデータを保存するために Outpost で使用可能な空きバイト数。 |
|  | BucketUsedBytes | 指定されたバケットのすべてのオブジェクトの合計サイズ。 |

#### SNS

|  |  |
| --- | --- |
| メトリクス | 内容 |
| NumberOfMessagesPublished | Amazon SNS トピックに対して発行されたメッセージ数 |
| NumberOfNotificationsDelivered | Amazon SNS トピックからそのトピックにサブスクライブしているエンドポイントに正常に配信されたメッセージ数。  配信の試行が成功するには、エンドポイントのサブスクリプションでメッセージが許可されている必要がある。サブスクリプションは、メッセージを受け入れます。フィルタポリシーがないか、b.) そのフィルタポリシーには、メッセージに割り当てられた属性と一致する属性が含まれている。サブスクリプションでメッセージが拒否された場合、配信の試行はこのメトリクスに対してカウントされない。 |
| NumberOfNotificationsFailed | Amazon SNS が配信に失敗したメッセージの数。  Amazon SQS、E メール、SMS、またはモバイルプッシュエンドポイントの場合、Amazon SNS がメッセージ配信の試行を停止すると、このメトリクスが 1 増分される。HTTP または HTTPS エンドポイントの場合、失敗した配信の試行がすべて、初回試行に続く再試行を含め、このメトリクスに対してカウントされる。その他のすべてのエンドポイントの場合、メッセージが配信されないと、カウントが 1 増加する (試行回数には関係ありません)。  サブスクリプションフィルタポリシーによって拒否されたメッセージは、このメトリクスに対してカウントされない。 |
| NumberOfNotificationsFilteredOut | サブスクリプションフィルタポリシーによって拒否されたメッセージの数。メッセージの属性がポリシーの属性と一致しない場合、フィルタポリシーによってメッセージは拒否される。 |
| NumberOfNotificationsFilteredOut-InvalidAttributes | メッセージの属性が無効であるため、たとえば属性の JSON 形式が正しくないため、サブスクリプションフィルタポリシーによって拒否されたメッセージの数 |
| NumberOfNotificationsFilteredOut-NoMessageAttributes | メッセージに属性がないため、サブスクリプションフィルタポリシーによって拒否されたメッセージの数 |
| NumberOfNotificationsRedrivenToDlq | デッドレターキューに移動されたメッセージの数 |
| NumberOfNotificationsFailedToRedriveToDlq | デッドレターキューに移動できなかったメッセージの数 |
| PublishSize | 発行されたメッセージのサイズ |
| SMSMonthToDateSpentUSD | 今月の始めから今日までの SMS メッセージの送信料金。  今月の始めから今日までの料金がアカウントの毎月の SMS 使用限度に近付いたことがわかるように、このメトリクスにアラームを設定できる。Amazon SNS が、SMS メッセージを送信するとこの限度を超えるコストが発生すると判断した場合、数分以内に SMS メッセージの発行が停止される。 |
| SMSSuccessRate | 正常な SMS メッセージ配信のレート。 |

### しきい値監視

本システムは以下のリソースについてしきい値監視を行う。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サービス | リソース | しきい値 | しきい値超過時のアクション | メトリクス |
| Elasticsearch  データノード | プライマリシャードとそのレプリカ | 1回以上ノードに割り当てられていない状況が1分 | メールによるアラート通知 | ClusterStatus.red |
|  | レプリカシャード | 1回以上ノードに割り当てられていない状況が1分 |  | ClusterStatus.yellow |
|  | データノードのストレージ容量 | 空き容量が2GB以下  (自動拡張しきい値以下を指定) |  | FreeStorageSpace |
|  | 書き込みリクエストのブロック | 1回以上が5分 |  | ClusterIndexWritesBlocked |
|  | データノード数 | 3ノード以下が1日 |  | Nodes |
|  | 自動スナップショットの失敗 | 1回以上 |  | AutomatedSnapshotFailure |
|  | CPU使用率 | 80%以上が15分、3回連続 |  | CPUUtilization または  WarmCPUUtilizationmaximum |
|  | メモリ使用率 | 80%以上が5分、3回連続 |  | JVMMemoryPressure または  WarmJVMMemoryPressuremaximum is |
|  | KMS 暗号化キーエラー | 1回以上 |  | KMSKeyError |
|  | KMS 暗号化キーアクセス不可 | 1回以上 |  | KMSKeyInaccessible |
| Elasticsearch マスターノード | CPU使用率 | 50%以上が15分、3回連続 |  | MasterCPUUtilization |
| メモリ使用率 | 85%以上が15分 |  | MasterJVMMemoryPressure |
| RDS | CPU使用率 | 80%以上が15分、3回連続 |  | CPUUtilization |
| メモリ使用率 | 80%以上が5分、3回連続 |  | FreeableMemory |
| ストレージ容量 | 空き容量が2GB以下  (自動拡張しきい値以下を指定) |  | FreeStorageSpace |

以下のメールアドレスに対してアラート通知を行う。

|  |
| --- |
| 通知先メールアドレス |
| d-suzuki@cstnet.co.jp |
| y-chida@cstnet.co.jp |
| t-gotoh@cstnet.co.jp |

## ログ管理

本システムのログはCloudWatch Logs、S3により管理する。

### ログ一覧

本システムのログ一覧を管理方式別に示す。

#### CloudWatch Logs管理ログ

CloudWatch Logsにより以下のログを管理する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ログ確認方法 | AWSマネジメントコンソールCloudWatchページ | | | |
| 対象サービス | 対象ログ | ロググループ | リージョン | 備考 |
| API Gateway | アクセスログ | 本番環境：/aws/apigateway/northface/prod/acclog  検証環境：/aws/apigateway/northface/stag/acclog | 東京 |  |
|  | 実行ログ | API-Gateway-Execution-Logs\_<文字列>/<ステージ名> |  | 自動作成される。ロググループ名変更不可。 |
| Lambda |  | /aws/lambda/<Lambda関数名> |  |
| DataSync |  | 本番環境：/aws/datasync/northface/prod/synclog  検証環境：/aws/datasync/northface/stag/synclog |  |  |
| Elasticsearch | スローログ | 本番環境：  /aws/aes/domains/northface/prod/<ドメイン名>/slowlog  検証環境：  /aws/aes/domains/northface/stag/<ドメイン名>/slowlog |  |  |
|  | インデックススローログ | 本番環境：  /aws/aes/domains/northface/prod/<ドメイン名>/indexslowlog  検証環境：  /aws/aes/domains/northface/stag/<ドメイン名>/indexslowlog |  | インデックス作成のスローログ |
|  | エラーログ | 本番環境：  /aws/aes/domains/northface/prod/<ドメイン名>/errorlog  検証環境：  /aws/aes/domains/northface/stag/<ドメイン名>/errorlog |  |  |
| RDS | 監査ログ | 本番環境：  /aws/rds/instance/northface/prod/<インスタンス名>/auditlog  検証環境：  /aws/rds/instance/northface/stag/<インスタンス名>/auditlog |  |  |
|  | 全般ログ | 本番環境：  /aws/rds/instance/northface/prod/<インスタンス名>/generallog  検証環境：  /aws/rds/instance/northface/stag/<インスタンス名>/generallog |  |  |
|  | スロークエリログ | 本番環境：  /aws/rds/instance/northface/prod/<インスタンス名>/slowquerylog  検証環境：  /aws/rds/instance/northface/stag/<インスタンス名>/slowquerylog |  |  |
| Route53 | 以下の情報を含むパブリック DNS クエリログ  ・リクエストされたドメインまたはサブドメイン  ・リクエストの日付と時刻  ・DNS レコードタイプ (A や AAAA など)  ・DNS クエリに応答した Route 53 エッジロケーション  ・DNS レスポンスコード (NoError や ServFail など) | 本番環境：/aws/route53/northface/prod/dnsquerylog  検証環境：/aws/route53/northface/stag/dnsquerylog | バージニア北部 | ロググループは、米国東部（バージニア北部） リージョンにある必要がある。 |
| AWS Systems Manager | エージェントログ | 本番環境：/aws/ssm/northface/prod/agentlog  検証環境：/aws/ssm/northface/stag/agentlog | 東京 |  |
| ACM  API Gateway  AWS Backup  AWS WAF  CloudWatch  Cognito  Data Pipeline  DataSync  ElasticSearch  Kinesis Data Firehose  KMS  Lambda  RDS  Route53  S3  SNS  VPC | 操作ログ(90日以上前のログ) | 本番環境：/aws/cloudtrail/northface/prod/operationlog  検証環境：/aws/cloudtrail/northface/stag/operationlog |  |  |

#### CloudTrail管理ログ

CloudTrailにより以下のログを管理する。

|  |  |
| --- | --- |
| ログ確認方法 | AWSマネジメントコンソールCloudTrailページ |
| 対象サービス | 対象ログ |
| ACM  API Gateway  AWS Backup  AWS WAF  CloudWatch  Cognito  Data Pipeline  DataSync  ElasticSearch  Kinesis Data Firehose  KMS  Lambda  RDS  Route53  S3  SNS  VPC | 操作ログ  (90日前までのログ) |

#### ログストレージ(S3)管理ログ

S3により以下のログを管理する。

|  |  |  |  |
| --- | --- | --- | --- |
| ログ確認方法 | AWSマネジメントコンソールS3ページのS3 Selectクエリ | | |
| 対象サービス | 対象ログ | プレフィクス | 備考 |
| AWS WAF | 以下の情報を含むWebACLトラフィック情報のログ  ・リクエストを受信した時間  ・リクエストの詳細  ・リクエストが一致したルールのアクション | awswaf/ | Kinesis Data Firehoseでログ収集する。 |
| Data Pipeline | 実行ログ | datapipeline/<テーブル名> |  |
| S3 | アクセスログ | 2.3.4ストレージ(S3)参照 | バケットに対するリクエストの詳細 |

### ログ保存期間

IPAが発表した企業における情報システムのログ管理に関する実態調査によると、一般的にはログの保存期間は1年程度が妥当である。

本システムではログの保存期間を以下とする。

|  |  |  |
| --- | --- | --- |
| ログ格納先 | ログ保存期間 | 備考 |
| CloudWatch Logs | 12ヶ月(365日) |  |
| S3 | 5年(1827日) | 2年目以降はS3 Glacierに保存 |

### ログ監視

本システムのログ監視については、運用上問題が発生した場合に実施を検討する。

## 時刻同期

本システムが利用する各種サービスはAWSグローバルインフラストラクチャにより時刻同期する。

## ソフトウェアのアップデート

各種サービスのアップデート方針を示す。

|  |  |  |
| --- | --- | --- |
| サービス | セキュリティアップデート | 機能追加やバージョンアップグレード |
| Elasticsearch | 自動適用する。 | 自動適用しない。  アプリケーション要件等で適用が必要な場合は検証環境に適用し、問題がないことを確認した後に本番環境に適用する。 |
| DBサーバー |

# セキュリティ

## ユーザー管理

以下のユーザーを作成する。

|  |  |  |  |
| --- | --- | --- | --- |
| ユーザー | 管理ポリシー | 権限 | 備考 |
| northface-cfnuser | AmazonAPIGatewayAdministrator | API Gateway管理 |  |
| (CloudFormation管理ユーザー) | - | Elasticsearch管理 | 以下の操作を許可  es:CreateElasticsearchDomain  es:DescribeElasticsearchDomain |
|  | AmazonKinesisFirehoseFullAcces | ログ収集管理 |  |
|  | AmazonRDSFullAccess | RDS管理 |  |
|  | AmazonRoute53FullAccess | Route53管理 |  |
|  | AmazonS3FullAccess | S3管理 |  |
|  | AWSBackupFullAccess | バックアップ管理 |  |
|  | AWSCertificateManagerFullAccess | ACM管理 |  |
|  | AWSCloudFormationFullAccess | CloudFormation管理 |  |
|  | AWSCloudTrail\_FullAccess | CloudTrail管理 |  |
|  | AWSDataSyncFullAccess | データストレージバックアップ管理 |  |
|  | AWSLambda\_FullAccess | Lambda管理 |  |
|  | AmazonVPCFullAccess | VPC管理 |  |
|  | AWSWAFFullAccess | AWS WAF管理 |  |
|  | CloudFrontFullAccess | CloudFront管理 |  |
|  | CloudWatchFullAccess | CloudWatch管理 |  |
|  | IAMFullAccess | 権限管理 |  |
| northface-operator | AmazonS3FullAccess | ログ確認、データストレージリストア | リソースグループのタグにより対象のリソースを限定する。 |
| (運用ユーザー) | AWSBackupOperatorAccess | バックアップ運用 |
|  | AWSCloudTrail\_FullAccess | ログ確認 |
|  | CloudWatchFullAccess |  |
|  | AWSDataSyncFullAccess | データストレージバックアップ |
| northface-developer  (アプリケーション開発ユーザー) | AmazonS3FullAccess | Lambdaコード管理 |

## ロール管理

各種サービスに以下のロールを付与する。

|  |  |  |
| --- | --- | --- |
| サービス | 権限 | 備考 |
| Lambda | Elasticsearch接続 |  |
|  | RDS接続 |  |
|  | CloudWatchLogs書き込み権限 | ログをCloudWatch Logsに書き込むため |
| API Gateway | CloudWatchLogs書き込み権限 | ログをCloudWatch Logsに書き込むため |
| CloudTrail | CloudWatchLogs書き込み権限 | ログをCloudWatch Logsに書き込むため。  AWSマネジメントコンソールによるCloudTrail作成時に自動で付与される。 |

## 暗号化方針

本システムの暗号化方針について記載する。

### Elasticsearch

|  |  |  |  |
| --- | --- | --- | --- |
| 暗号化 | 項目 | 設定値 | 備考 |
| 有効 | ドメインへのすべてのトラフィックに HTTPS を要求する | 有効 | 機密データが含まれるため暗号化する。 |
|  | ノード間の暗号化 | 有効 |
|  | 保管時のデータの暗号化の有効化 | 有効 |
|  | KMSマスターキー | (デフォルト)aws/es |

### DBサーバー(RDS)

|  |  |
| --- | --- |
| 暗号化 | 備考 |
| 有効 | 機密データが含まれるため暗号化する。 |

### ストレージ(S3)

|  |  |  |  |
| --- | --- | --- | --- |
| ストレージ種別 | 暗号化 | 暗号化キータイプ | 備考 |
| データストレージ01 | 有効 | Amazon S3 キー (SSE-S3) | 機密データが含まれるため暗号化する。 |
| データストレージ02 |  |  |  |
| データストレージ03 |  |  |  |
| データストレージ04 |  |  |  |
| アプリケーションストレージ | 無効 | - | 機密データが含まれないため暗号化不要。 |
| バックアップストレージ | 有効 | Amazon S3 キー (SSE-S3) | 機密データが含まれるため暗号化する。 |
| ログストレージ |  |  |  |
| CloudTrailログストレージ |  |  |  |

### 認証基盤(Cognito)

|  |  |
| --- | --- |
| 暗号化 | 備考 |
| 有効 | 機密データが含まれるため暗号化する。  デフォルトで暗号化される。 |

### バックアップデータ

|  |  |  |
| --- | --- | --- |
| 対象 | 暗号化 | 備考 |
| Elasticsearchデータ | 有効 | 機密データが含まれるため暗号化する。 |
| データベース(RDS) | 有効 |  |
| データストレージ(S3) | 有効 |  |

## Webアクセス

本システムでは以下のサービスを利用し、セキュアなWebアクセス環境を提供する。

### ACM

本システムではACMサービスにより以下のSSL証明書を発行する。

|  |  |
| --- | --- |
| 項目 | 設定値 |
| 証明書のタイプ | パブリック証明書 |
| ドメイン名 | 本番環境：northface.cstnet.co.jp  検証環境：northface-stag.cstnet.co.jp |

ACMにより以下の特性を持つACM証明書を発行する。

|  |  |
| --- | --- |
| 特性 | 内容 |
| ドメイン検証 (DV) | ACM 証明書はドメイン検証される。 |
| 有効期間 | ACM 証明書の有効期間は 13 ヶ月 (395 日) |
| マネージド型更新とデプロイ | ACM は、ACM 証明書の更新プロセスと、更新後の証明書のプロビジョニングを管理し、証明書の設定ミス、失効、期限切れによるダウンタイムを防止する。 |
| ブラウザとアプリケーショントラスト | ACM証明書は、Google Chrome、Microsoft Internet Explorer と Microsoft Edge、そして Mozilla Firefox および Apple Safari を含むすべての主要なブラウザから信頼されている。 |
| 複数のドメイン名 | 各 ACM 証明書には、少なくとも 1 つの完全修飾ドメイン名 (FQDN) が含まれる必要があり、必要に応じて追加の名前を付け加えることができる。  (例) 「www.example.com」のACM 証明書に「example.com」 を追加 |
| ワイルドカード名 | ドメイン名にアスタリスク (\*) を使うことで、同じドメイン内の複数のサイトを保護できるワイルドカード名を含む ACM 証明書を作成することができる。 |
| アルゴリズム | 以下のパブリックキーアルゴリズムが ACM でサポートされている。  ・2048 ビット RSA (RSA\_2048)  ・4096 ビット RSA (RSA\_4096)  ・Elliptic Prime Curve 256 ビット (EC\_prime256v1)  ・Elliptic Prime Curve 384 ビット (EC\_secp384r1) |

### AWS WAF作成済み

AWS WAFを利用し、アプリケーションの可用性、セキュリティの侵害、リソースの過剰な消費などに影響を与えかねない一般的なウェブの弱点からシステムを保護する。本システムでは、絶えず変化する脅威に対して迅速な対応をとるためにAWSマネージドルールを適用する。

AWSマネージドルールでは新しい脆弱性と脅威が発生した場合、AWSによりルールグループが自動的に更新される。

検証環境ではAWSマネージドルールに一致するリクエストをカウント(監視)するのみとし、ブロックは行わない。

本番環境ではAWSマネージドルールに一致するリクエストをブロックする。

本番環境で正常なリクエストが意図せずブロックされた場合は検証環境でルールの調整と動作検証を行い、本番環境のルールを調整する。

ルールの優先順位についてはIPアドレスによるルール等、限定的な範囲に及ぶルールを優先とし、より低コストで攻撃をブロック可能とする。

|  |  |  |
| --- | --- | --- |
| 優先順位 | ルールグループ | 説明 |
| 1 | IP 評価ルールグループ | ボットトラフィック等、接続元に基づいてリクエストをブロックする。 |
| 2 | AWS WAF ボットコントロールルールグループ | 一般的なボットを分類して識別し、一般的に望ましいボットを検証し、ボットの信頼度の高い署名を検出することで、サイトに対するボットのアクティビティを管理する。 |
| 3 | ユースケース固有のルールグループ | さまざまな AWS WAF ユースケースに対して段階的な保護を提供する。 |
| 4 | ベースラインルールグループ | さまざまな一般的な脅威に対する一般的な保護を提供する |

AWSマネージドルールは以下の通り構成する。

|  |  |  |  |
| --- | --- | --- | --- |
| ルールグループ | ルールセット | 適用(優先順位) | 説明 |
| ベースラインルールグループ | コアルールセット | ○(6) | Webアプリケーションに一般的に適用すべきルールセット。高リスクの脆弱性や一般的な脆弱性など、幅広い脆弱性の悪用に対する保護が提供される。 |
|  | 管理者保護 | ×  サードパーティーのソフトウェアを実行しないため | 公開されている管理ページへの外部アクセスをブロックするためのルールセット。サードパーティーのソフトウェアを実行している場合や、悪意のある攻撃者がアプリケーションへの管理アクセスを得るリスクを軽減したい場合に適用する。 |
|  | 既知の不正な入力 | ○(5) | 無効であることがわかっており脆弱性の悪用または発見に関連するリクエストパターンをブロックするためのルールセット。悪意のある攻撃者が脆弱なアプリケーションを発見するリスクを軽減する。 |
| ユースケース固有のルールグループ | SQL データベース | ○(4)  RDSを使うため適用する | SQL インジェクション攻撃などの SQL データベースの悪用に関連するリクエストパターンをブロックするルールセット。これにより、不正なクエリのリモートインジェクションを防ぐことができる。アプリケーションが SQL データベースにアクセスする場合に適用する。 |
|  | Linux オペレーティングシステム | ×  LinuxOSを使用しないため | Linux 固有のローカルファイルインクルージョン (LFI) 攻撃など、Linux 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことができる。 |
|  | POSIX オペレーティングシステム | ×  POSIXOSを使用しないため | POSIX および POSIX と同等のオペレーティングシステムに固有の脆弱性の悪用 (ローカルファイルインクルージョン (LFI) 攻撃など) に関連するリクエストパターンをブロックするルールセット。攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことができる。 |
|  | Windows オペレーティングシステム | ×  WindowsOSを使用しないため | PowerShell コマンドのリモート実行など、Windows 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。攻撃者が不正なコマンドを実行したり、悪意のあるコードを実行したりする脆弱性の悪用を防ぐことができる。 |
|  | PHP アプリケーション | ×  PHPを使用しないため | 安全でない PHP 関数のインジェクションなど、PHP プログラミング言語の使用に固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。 |
|  | WordPress アプリケーション | ×  WordPressを使用しないため | WordPress サイト固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールセット。 |
| IP 評価ルールグループ | Amazon IP 評価リスト | ○(1) | Amazon 内部脅威インテリジェンスに基づくルールセット。ボットやその他の脅威に関連付けられている IP アドレスをブロックすることでボットを軽減し、悪意のある攻撃者が脆弱なアプリケーションを発見するリスクを軽減する。 |
|  | 匿名 IP リスト | ○(2) | VPN、プロキシ、Tor ノード、ホスティングプロバイダー (AWS を含む)など、ビューワーIDの難読化を許可するサービスからのリクエストをブロックするルールセット。アプリケーションから ID を隠そうとするビューワーをブロックし、ボットの軽減や地理的制限を回避する。 |
| AWS WAF ボットコントロールルールグループ | AWS WAF ボットコントロール | ○(3) | ボットからのリクエストをブロックして管理するルール。このルールグループを使用する場合は追加料金が必要となる。 |

### API Gateway

本システムでは、API の作成、公開、保守、モニタリング、保護のためにAPI Gatewayサービスを利用する。

以下にAPI Gatewayの非機能要件関連の定義を示す。

機能要件についてはAPI一覧を参照する。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 項目 | | | | | | 設定値 | 備考 |
| API | | | | | |  |  |
|  | | APIタイプ | | | | REST API |  |
|  | | API名 | | | | 本番環境：prod-northface-api  検証環境：stag-northface-api |  |
|  | | エンドポイントタイプ | | | | リージョン | インターネットからアクセス可能とする。 |
|  | | ステージ名 | | | | 本番環境：prod  検証環境：stag |  |
|  | |  | キャッシュ設定 | | | 無効 | パフォーマンスに問題が生じた場合に有効化を検討する。 |
|  | |  | デフォルトのメソッドスロットリング | | | 有効 | スループット向上のため、APIに対するリクエストのレートを制限する。 |
|  | |  |  | レート | | 10000 リクエスト数/秒 | リクエストの送信数がリクエストの定常レートおよびバーストを超えると、API Gateway は制限を超えたリクエストを失敗させ、クライアントに 429 Too Many Requests エラーレスポンスを返す。 |
|  | |  |  | バースト | | 5000 リクエスト数 |
|  | |  | ウェブアプリケーションファイアウォール (WAF) ウェブACL | | | AWS WAF WebACL |  |
|  | |  | クライアント証明書 | | | なし  (バックエンドポイントとしてLambda関数のみを使用するため、クライアント証明書は不要) | API Gateway を使用して SSL 証明書を生成し、バックエンドでそのパブリックキーを使用して、バックエンドシステムへの HTTP リクエストが API Gateway からのものであることを確認する。 |
|  |  | | ログ/トレース | | |  |  |
|  | |  | CloudWatch設定 | | |  |  |
|  | |  |  | CloudWatchログを有効化 | | 有効 | 実行ログを取得する。 |
|  | |  |  |  | ログレベル | エラー | 情報レベルのログは取得しない。 |
|  | |  |  |  | リクエスト/レスポンスをすべてログ | 無効 | このログは API のトラブルシューティングに役立つが、機密データが記録される可能性があるため無効を推奨。 |
|  | |  |  | 詳細 CloudWatch メトリクスを有効化 | | 有効 | API Gatewayの監視を有効化する。 |
|  | |  | カスタムアクセスのログ記録 | | |  |  |
|  | |  |  | アクセスログの有効化 | | 有効 | API Gatewayのアクセスログを取得する。 |
|  | |  |  | Access Log Destination ARN | | ClouodWatchグループ |  |
|  | |  |  | ログの形式 | | CLF |  |
|  | |  | X-Ray トレース | | | 無効 | REST API から基盤となるサービスへのユーザーリクエストの流れをトレースして分析する |
|  |  | | ステージ変数 | | |  |  |
|  | |  | 名前 | | | ステージ変数なし |  |
|  | |  | 値 | | |  |  |
| オーソライザー | | | | | | Cognito | Amazon Cognito ユーザープールまたは Lambda 関数を使用して API へのアクセスを制御する。  ※アプリケーション要件確定後記載 |
|  | | トークンのソース | | | |  |
|  | | トークンの検証 | | | |  |
| ゲートウェイのレスポンス | | | | | |  |  |
|  | | アクセスが拒否されました | | | | レスポンスのステータスコード：403 |  |
|  | | API 設定エラー | | | | レスポンスのステータスコード：500 |  |
|  | | オーソライザー設定エラー | | | | レスポンスのステータスコード：500 |  |
|  | | オーソライザーエラー | | | | レスポンスのステータスコード：500 |  |
|  | | リクエスト本文が不正です | | | | レスポンスのステータスコード：400 |  |
|  | | リクエストパラメータが不正です | | | | レスポンスのステータスコード：400 |  |
|  | | DEFAULT 4XX | | | | - |  |
|  | | DEFAULT 5XX | | | | - |  |
|  | | 期限切れのトークン | | | | レスポンスのステータスコード：403 |  |
|  | | 統合の失敗 | | | | レスポンスのステータスコード：504 |  |
|  | | 統合のタイムアウト | | | | レスポンスのステータスコード：504 |  |
|  | | 無効な API キー | | | | レスポンスのステータスコード：403 |  |
|  | | 無効な署名 | | | | レスポンスのステータスコード：403 |  |
|  | | 認証トークンが見つかりません | | | | レスポンスのステータスコード：403 |  |
|  | | クォータを超過しました | | | | レスポンスのステータスコード：429 |  |
|  | | リクエストが大きすぎます | | | | レスポンスのステータスコード：413 |  |
|  | | リソースは存在しません | | | | レスポンスのステータスコード：404 |  |
|  | | スロットル済み | | | | レスポンスのステータスコード：429 |  |
|  | | 権限がありません | | | | レスポンスのステータスコード：401 |  |
|  | | サポートされていないメディアタイプ | | | | レスポンスのステータスコード：415 |  |
|  | | WAF フィルター | | | | レスポンスのステータスコード：403 |  |
| カスタムドメイン名 | | | | | | 設定する | ドメイン名によるAPI Gatewayへのアクセスを可能とする。 |
|  | | TLS の最小バージョン | | | | TLS 1.2 (推奨) | Transport Layer Security (TLS) により、クライアントとサーバー間の転送中のデータを保護する。 |
|  | | 相互 TLS 認証 | | | | 無効 | クライアントは X.509 証明書を提示して、API にアクセスするためのアイデンティティを検証する。 |
|  | | エンドポイントタイプ | | | | リージョン | このカスタムドメイン名を特定の AWS リージョンに関連付けて、リージョン内レイテンシーを最適化する。 |
|  | | ACM証明書 | | | | 設定する |  |
| VPCリンク | | | | | | 設定しない | VPC 内のプライベートリソースに接続する場合設定する。 |

## ウィルス対策

本システムではデータストレージ(S3)にファイルをアップロードする際にアンチウィルスソフト(ClamAV)によるウィルススキャンを実施し、ウィルスチェックで正常判定が出るまで、オブジェクトを読み取り不可とする。ウィルスチェックで感染判定が出た場合は、ウィルスチェック完了後もオブジェクトを読み取り不可とし、判定結果の書き換えを禁止する。なお、オブジェクトの削除は許可する。

アンチウィルスソフト(ClamAV)の定義ファイルは1日に1回更新する。

修正すること：

RDSの DataPipeline：

1. インターネット向けは必要、NATGatewayの使用は要検討です。
2. インターネット向けなので、RDSのNACLを修正します。
3. DataPipeline専用セキュリティグループの作成、RDSセキュリティグループのソースに追加します。
4. DataPipeline詳細設定はサブネットとセキュリティグループを指定します。