更新履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版 | 更新日 | 更新項目 | 更新者 | 備考 |
| (会社名/氏名) |
| 1.0 | 2021/07/30 | 新規作成 | アイロベックス  若林 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目次

[1 はじめに 6](#_Toc79263295)

[2 システム構成 7](#_Toc79263296)

[2.1 システム構成図 7](#_Toc79263297)

[2.2 サービス構成 8](#_Toc79263298)

[2.2.1 サービス一覧 8](#_Toc79263299)

[2.2.2 リソースグループ 11](#_Toc79263300)

[2.2.3 サービス管理方式 11](#_Toc79263301)

[2.3 サーバー構成 11](#_Toc79263302)

[2.3.1 WebAPサーバー 11](#_Toc79263303)

[2.3.2 DBサーバー(RDS) 20](#_Toc79263304)

[2.3.3 ストレージ(S3) 22](#_Toc79263305)

[2.3.4 バッチサーバー(CodeBuild) 24](#_Toc79263306)

[2.3.5 ソース管理サーバー(CodeCommit) 25](#_Toc79263307)

[2.4 ソフトウェア構成 26](#_Toc79263308)

[2.4.1 WebAPサーバー 26](#_Toc79263309)

[2.4.2 バッチサーバー(CodeBuild) 28](#_Toc79263310)

[2.5 ネットワーク構成 29](#_Toc79263311)

[2.5.1 VPC 29](#_Toc79263312)

[2.5.2 サブネット 30](#_Toc79263313)

[2.5.3 ネットワークACL 31](#_Toc79263314)

[2.5.4 セキュリティグループ 32](#_Toc79263315)

[2.5.5 ルートテーブル 33](#_Toc79263316)

[2.5.6 インターネットゲートウェイ 34](#_Toc79263317)

[2.5.7 NATゲートウェイ 34](#_Toc79263318)

[2.5.8 名前解決 34](#_Toc79263319)

[3 可用性 35](#_Toc79263320)

[3.1 耐障害性 35](#_Toc79263321)

[3.2 災害対策 35](#_Toc79263322)

[4 拡張性 36](#_Toc79263323)

[4.1 拡張性設計 36](#_Toc79263324)

[5 保守性 37](#_Toc79263325)

[5.1 バックアップ・リストア 37](#_Toc79263326)

[5.1.1 バックアップ 37](#_Toc79263327)

[5.1.2 リストア 37](#_Toc79263328)

[5.2 ジョブ管理 37](#_Toc79263329)

[5.2.1 ジョブ一覧 37](#_Toc79263330)

[5.2.2 ジョブ監視 38](#_Toc79263331)

[5.3 URL監視 38](#_Toc79263332)

[5.4 リソース監視 38](#_Toc79263333)

[5.4.1 リソース監視方式 38](#_Toc79263334)

[5.4.2 CloudWatchメトリクス保存期間 39](#_Toc79263335)

[5.4.3 リソース監視状況確認方法 39](#_Toc79263336)

[5.4.4 リソース監視項目 39](#_Toc79263337)

[5.4.5 しきい値監視 66](#_Toc79263338)

[5.5 ログ管理 66](#_Toc79263339)

[5.5.1 ログ一覧 66](#_Toc79263340)

[5.5.2 ログ保存期間 70](#_Toc79263341)

[5.5.3 ログ監視 71](#_Toc79263342)

[5.6 時刻同期 71](#_Toc79263343)

[5.7 ソフトウェアのアップデート 72](#_Toc79263344)

[5.8 アラート通知先 72](#_Toc79263345)

[6 セキュリティ 73](#_Toc79263346)

[6.1 ユーザー管理 73](#_Toc79263347)

[6.2 ロール管理 74](#_Toc79263348)

[6.3 暗号化方針 75](#_Toc79263349)

[6.3.1 WebAPサーバー 75](#_Toc79263350)

[6.3.2 DBサーバー(RDS) 75](#_Toc79263351)

[6.3.3 ストレージ(S3) 75](#_Toc79263352)

[6.3.4 バッチサーバー(CodeBuild) 75](#_Toc79263353)

[6.3.5 ソース管理サーバー(CodeCommit) 75](#_Toc79263354)

[6.3.6 バックアップデータ 76](#_Toc79263355)

[6.4 Webアクセス 76](#_Toc79263356)

[6.4.1 ACM 76](#_Toc79263357)

[6.4.2 AWS WAF 77](#_Toc79263358)

[6.4.3 CloudFront 79](#_Toc79263359)

# はじめに

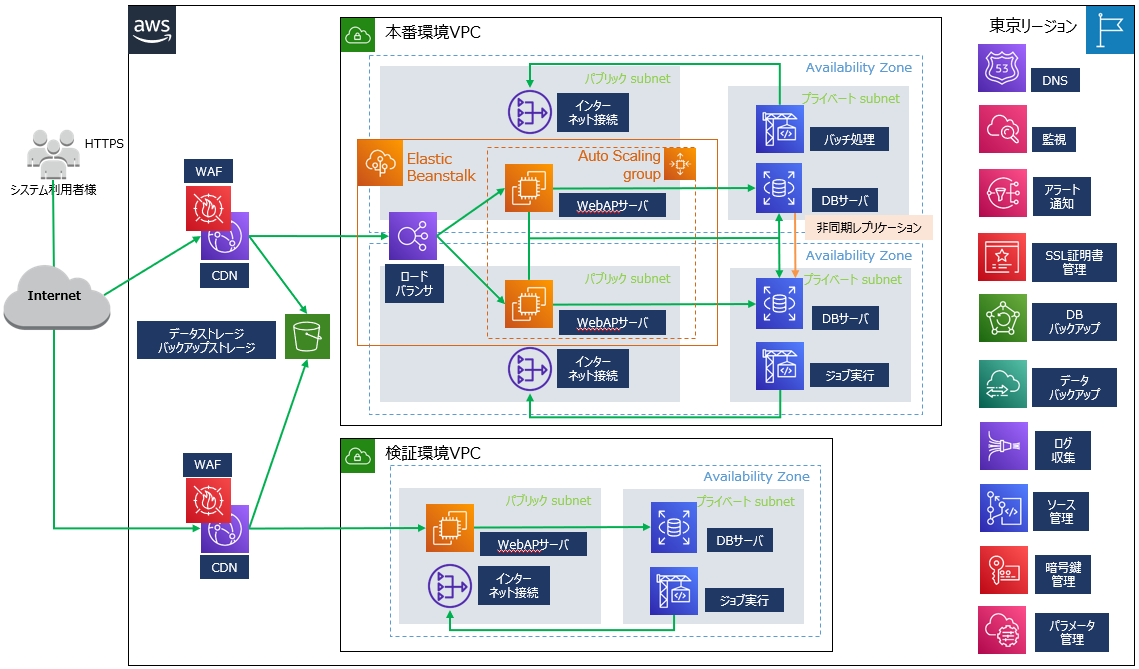
本書はコーポレートサイトシステム インフラ環境(以下、本システム)の構成、機能の実現方法、及び運用方式について記載する。

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。 |
| Auto Scaling group |  | 同左 | Auto Scaling グループと呼ばれる EC2 インスタンスの集合を作成し、アプリケーションの負荷を処理するために適切な数の Amazon EC2 インスタンスを利用できるようにするグループの最小値、最大値を設定し、システムの負荷状況に応じて最小値、最大値の範囲でEC2インスタンスの数を自動で増減する。 |
| AWS Backup |  | DB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 Systems Manager |  | パラメータ管理 | AWS Systems Manager の一機能である Parameter Store は､設定データ管理と機密管理のための安全な階層型ストレージを提供する。パスワード、データベース文字列、Amazon マシンイメージ (AMI) ID、ライセンスコードなどのデータをパラメータ値として保存できる。値はプレーンテキストまたは暗号化されたデータとして保存できます。 |
| 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。 |
| CodeBuild |  | ジョブ実行 | ソースコードをコンパイルし、テストを実行し、デプロイ可能なソフトウェアパッケージを作成できる完全マネージド型のビルドサービス。 |
| CodeCommit |  | ソース管理 | プライベート Git リポジトリをホストする、安全で高度にスケーラブルなマネージド型のソース管理サービス。これにより、チームは、転送中および保存中にコントリビューションを暗号化して、コードの共同作業を安全に行うことが容易になる。 |
| CloudFront |  | 同左 | 低レイテンシーの高速転送により世界中の視聴者に安全に配信する高速コンテンツ配信ネットワーク (CDN) サービス。 |
| 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。 |
| 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。 |
| EC2 |  | WebAPサーバ | プロセッサ、ストレージ、ネットワーキング、オペレーティングシステム、購入モデルを選択できる、幅広く奥の深いコンピューティングプラットフォームを提供する。 |
| Elastic Beanstalk |  | 同左 | Java、.NET、PHP、Node.js、Python、Ruby、Go および Docker を使用して開発されたウェブアプリケーションやサービスを、Apache、Nginx、Passenger、IIS など使い慣れたサーバーでデプロイおよびスケーリングするサービス。 |
| Elastic Load Balancing |  | ロードバランサ | アプリケーションへのトラフィックを複数のターゲット (Amazon EC2 インスタンス、コンテナ、IP アドレス、Lambda 関数、仮想アプライアンスなど) に自動的に分散する。 |
| 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。 |
| NAT Gateway |  | インターネット接続 | ネットワークアドレス変換 (NAT) ゲートウェイを使用して、プライベートサブネットのインスタンスからインターネットや他の AWS サービスに接続できるが、インターネットからはこれらのインスタンスとの接続を開始できないようにすることができる。 |
| 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 |  | 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

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 | AERAS-corporate-site-system-Production | AERAS-corporate-site-system-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 | AERAS-corporate-site-system | |
| 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。

### WebAPサーバー

#### 本番環境用WebAPサーバー(Elastic Beanstalk)

本システムでは本番環境用WebサーバーとしてElastic Beanstalkサービスを利用する。

以下にElastic Beanstalkの定義を示す。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | 本番環境 | 備考 |
| アプリケーション名 | | | | | prod-aeras-corporate-site-system-eb-application |  |
| プラットフォーム | | | | |  |  |
|  | プラットフォーム | | | | PHP | 2021年8月時点で最新 |
|  | プラットフォームのブランチ | | | | PHP 7.4 running on 64bit Amazon Linux 2 | PHP 7.4.21 |
|  | プラットフォームのバージョン | | | | 3.3.3 | Apache 2.4.48 |
| ソフトウェア | | | | |  |  |
|  | コンテナオプション | | | |  |  |
|  |  | プロキシサーバー | | | Apache | リバースプロキシとしてnginxかApacheを選択する。現行環境に合わせてApacheとする。 |
|  |  | ドキュメントのルート | | |  | パブリック向けウェブのルートとして機能するプロジェクトの子ディレクトリ |
|  |  | メモリ制限 | | | 256M | PHP 環境に割り当てられたメモリの量 |
|  |  | Zlib出力の圧縮 | | | 無効 | PHP が出力に圧縮を使用するかどうかを指定する。 |
|  |  | URLでfopenを許可 | | | 有効 | PHP のファイル関数がウェブサイトや FTP サーバーなどのリモートロケーションからデータを取得できるかどうかを指定する。 |
|  |  | 表示エラー | | | 無効 | エラーメッセージを出力に含めるかどうかを指定する。 |
|  |  | 最大実行時間(秒) | | | 60 | 環境がスクリプトを終了するまでの最長時間を指定する。 |
|  | AWS X-Ray | | | | 無効 | 分散アプリケーションの分析とデバッグ |
|  | S3 ログストレージ | | | | 更新されたログを Amazon S3 にアップロードするように環境内のインスタンスを設定する。 | |
|  |  | ログのローテーション | | | 有効 | ログローテーションの有効/無効を指定 |
|  | CloudWatchLogsへのインスタンスログのストリーミング | | | | CloudWatch Logs にログをストリーミングするように環境内のインスタンスを設定する。最大10年間までの保持期間と環境終了時のログ削除について設定する。 | |
|  |  | ログのストリーミング | | | 有効 | ログストリーミングの有効/無効を指定 |
|  |  | 保持期間 | | | 5.5.2ログ保存期間を参照 |  |
|  |  | ライフサイクル | | | 環境の終了後にログを保持する |  |
| インスタンス | | | | |  |  |
|  | ルートボリューム(起動デバイス) | | | |  |  |
|  |  | ルートボリュームタイプ | | | コンテナのデフォルト | 起動デバイス |
|  | インスタンスメタデータサービス (IMDS) | | | | 環境のプラットフォームは IMDSv1 と IMDSv2 の両方をサポートしている。IMDSv2 を適用するには、IMDSv1 を無効にする。 | |
|  |  | IMDSv1 を無効化 | | | 無効にチェックを入れない | IMDSv1無効化の有効/無効を指定 |
|  | インスタンスセキュリティグループ | | | |  |  |
|  |  | グループ名 | | | 本番環境用WebAPサーバー用セキュリティ |  |
|  |  | グループID | | | グループを指定 |  |
| 容量 | | | | |  |  |
|  | Auto Scaling グループ | | | |  |  |
|  |  | 環境タイプ | | | 負荷分散 | 単一インスタンス / 負荷分散 |
|  |  |  | | インスタンス最小数 | 1 | 自動拡張するインスタンス数の範囲を指定 |
|  |  |  | | インスタンス最大数 | 4 |
|  |  | フリートの構成 | | | オンデマンドインスタンス | 複数のインスタンスタイプを持つオンデマンドインスタンスとスポットインスタンスの組み合わせを選択する。 |
|  |  | インスタンスタイプ | | | t3.medium | ベースラインレベルの CPU パフォーマンスを提供する次世代のバースト可能な汎用インスタンスタイプ  vCPU：2 / メモリ：4GiB |
|  |  | アベイラビリティゾーン | | | ap-northeast-1a | 使用するアベイラビリティーゾーン (AZ) を指定する。 |
|  |  | | | | ap-northeast-1c |
|  | スケーリングトリガー | | | |  |  |
|  |  | メトリクス | | | NetworkOut | 自動拡張 |
|  |  | 統計 | | | 平均 | パブリック向けウェブのルートとして機能するプロジェクトの子ディレクトリ |
|  |  | 単位 | | | 256M | PHP 環境に割り当てられたメモリの量 |
|  |  | 期間 | | | 5分 | メトリクスの評価間隔 |
|  |  | 超過時間 | | | 5分 | スケーリングオペレーションをトリガーするまでメトリクスがしきい値を超えることができる期間 |
|  |  | 上限しきい値 | | | 6000000バイト | スケールアウトのしきい値 |
|  |  | 下限しきい値 | | | 2000000バイト | スケールインのしきい値 |
| ロードバランサー | | | | |  |  |
|  | ロードバランサーの種類 | | | | Application Load Balancer | アプリケーションレイヤーのロードバランサー — プロトコル、ポート、および環境プロセスへのルートに基づいて HTTP および HTTPS トラフィックをルーティングする。 |
|  | リスナー | | | | ロードバランサーで使用するリスナーを指定。各リスナーは指定されたプロトコルを使用して、指定されたポートの着信クライアントトラフィックを環境プロセスにルーティングする。デフォルトでは、標準の Web サーバーにポート 80 を使用するようにロードバランサーが設定されている。 | |
|  |  | ポート | | | 80 |  |
|  |  | プロトコル | | | HTTP |  |
|  |  | SSL証明書 | | | -- |  |
|  |  | デフォルトプロセス | | | default |  |
|  | プロセス | | | | 各環境プロセスに対して、ロードバランサーがリクエストをプロセスにルーティングするために使用するプロトコルとポートを指定。また、ロードバランサーがプロセスのヘルスチェックを実行する方法も指定。 | |
|  |  | 名前 | | | default |  |
|  |  | ポート | | | 80 |  |
|  |  | プロトコル | | | HTTP |  |
|  |  | HTTPコード | | | default |  |
|  |  | ヘルスチェック | | |  |  |
|  |  |  | HTTPコード | | 200 | 環境内の正常なインスタンスの HTTP ステータスコード。 |
|  |  |  | パス | | / | ロードバランサーが HTTP ヘルスチェックリクエストを送信するパス。 |
|  |  |  | タイムアウト | | 5秒 | ヘルスチェックレスポンスの待機時間 |
|  |  |  | 間隔 | | 15秒 | 個々のインスタンスのヘルスチェックの間隔。間隔はタイムアウトより大きくする必要がある。 |
|  |  |  | 非正常のしきい値 | | 5リクエスト | インスタンスが異常であると結論するまでに必要なヘルスチェックの連続失敗回数。 |
|  |  |  | 正常のしきい値 | | 3リクエスト | インスタンスが正常であると結論するまでに必要なヘルスチェックの連続成功回数。 |
|  |  |  | 登録解除の遅延 | | 20秒 | 登録解除前にアクティブなリクエストが完了するまでの待機時間 |
|  |  | セッション | | | 以下の設定で、ロードバランサーが同一のセッションのリクエストを最小の負荷の Amazon EC2 インスタンスにルーティングするか、常時同じインスタンスにルーティングするかを制御する。 | |
|  |  |  | スティッキーポリシー | | 有効 | ロードバランサーは同一のセッションのリクエストを常時同じインスタンスにルーティングする。 |
|  |  |  | Cookie の維持期間 | | 86400秒 | Amazon EC2 インスタンスとロードバランサーの間のスティッキーセッション Cookie の有効期間。 |
|  | ルール | | | | なし | ロードバランサーは、ルールに基づいて環境プロセスにリクエストをルーティングする。ルールは優先度に基づいて数値の昇順に評価される。  Elastic Beanstalk は、各リスナーにデフォルトのルールを設定する。それぞれのデフォルトのルールは、すべてのトラフィックを各リスナーに関連付けられたデフォルトのプロセスにルーティングし、そのリスナーのすべてのルールの中で最後の優先度を持つ。リクエストが他のルールの条件と一致しない場合、デフォルトのルールはリスナーのデフォルトプロセスにリクエストをルーティングする。 |
|  | ログ設定 | | | | Elastic Load Balancing を設定して、ロードバランサーに送信されたリクエストの詳細情報を含むログを出力する。ログは Amazon S3 に保存する。 | |
|  |  | ログの保存 | | | 有効 | ログ保存の有効/無効を指定 |
|  |  | S3バケット | | | ログストレージ(S3) | ログの保存先を指定 |
|  |  | プレフィックス | | | alb/ | バケットの論理階層。プレフィックスを指定しない場合、Elastic Load Balancing はバケットのルートにアクセスログを保存する。 |
| ローリング更新とデプロイ | | | | |  |  |
|  | アプリケーションのデプロイ | | | |  |  |
|  |  | デプロイメントポリシー | | | 1回にすべて | AWS Elastic Beanstalk がソースコードの変更および設定更新をどのように伝達するかを選択する。 |
|  | 設定の更新 | | | | 仮想マシンの設定および VPC の設定への変更により、環境内でダウンタイムなしにインスタンスを置き換えるローリング更新がトリガーされる。 | |
|  |  | ローリング更新のタイプ | | | ヘルスにもとづくローリング | オンラインでEC2インスタンスのインスタンスタイプを変更可能とする。 |
|  |  | バッチサイズ | | | 1 | 更新の各フェーズで置き換えるインスタンスの最大数。 |
|  |  | 最小容量 | | | 1 | 常にサービス内に保持されるインスタンスの最小数。 |
|  | デプロイの設定 | | | | ヘルスチェックの要件とデプロイメントタイムアウトのカスタマイズ | |
|  |  | ヘルスチェックを無視 | | | False | ヘルスチェックに合格しなくてもデプロイに失敗しない。 |
|  |  | 正常のしきい値 | | | - | 更新またはデプロイ中に、バッチのインスタンスがヘルスチェックにパスするようにしきい値を下げる。 |
|  |  | コマンドタイムアウト | | | 600秒 | AWS Elastic Beanstalk でインスタンスがデプロイメントコマンドを完了する時間を秒単位で変更する。 |
| セキュリティ | | | | |  |  |
|  | サービスロール | | | |  |  |
|  | 仮想マシンアクセス許可 | | | |  |  |
|  |  | EC2キーペア | | | 本番環境用EC2キーペア | 検証環境とは別のキーペアを指定 |
|  |  | IAM インスタンスプロフィール | | | 6.2ロール管理を参照 | IAMロールを指定 |
| モニタリング | | | | |  |  |
|  | ヘルスレポート | | | | 拡張ヘルスレポートは、無料のリアルタイムアプリケーション、および環境内のインスタンスと他のリソースのオペレーティングシステムモニタリングを提供する。EnvironmentHealth カスタムメトリックスは、拡張ヘルスレポートと共に無料で提供される。 | |
|  |  | システム | | | ベーシック | 問題が発生した場合に拡張メトリクスの導入を検討する。 |
|  | ヘルスモニタリングルールのカスタマイズ | | | | 環境のヘルス状態の判断に含まれる HTTP アプリケーションステータスコードとロードバランサーステータスコードを設定する。 | |
|  |  | アプリケーション 4xx を無視 | | | 無効 | アプリケーション4xxエラー設定 |
|  |  | ロードバランサー 4xx を無視 | | | 無効 | ロードバランサー4xxエラー設定 |
|  | CloudWatch Logs へのヘルスイベントのストリーミング | | | | CloudWatch Logs に環境のヘルスイベントをストリーミングするように環境内のインスタンスを設定する。最大10年間までの保持期間と環境終了時のログ削除について設定する。 | |
|  |  | ログのストリーミング | | | 有効 | ログストリーミングの有効/無効を指定 |
|  |  | 保持期間 | | | 5.5.2ログ保存期間を参照 |  |
|  |  | ライフサイクル | | | 環境の終了後にログを保持する |  |
| 管理された更新 | | | | | 管理されたプラットフォームの更新で、選択した週ごとのメンテナンスウィンドウに自動的にプラットフォームの更新を適用する。更新プロセス中も、引き続きアプリケーションを使用可能。 | |
|  | 管理された更新 | | | | 有効 | 管理された更新の有効/無効を指定 |
|  | 週ごとの更新ウィンドウ | | | | 土曜日  開始時刻：18:00(UTC) | 利用可能なマネージドアップデートの更新ウィンドウを指定 |
|  | 更新レベル | | | | パッチのみ | マイナーレベルの更新とセキュリティパッチの更新について指定。セキュリティパッチのみ適用する。 |
|  | インスタンスの置換 | | | | 無効 | 有効にした場合、インスタンスの置換は他の更新が利用可能でない場合にスケジュールされる。 |
| 通知 | | | | | 環境からの重要イベントに関するメール通知の受信先 | |
|  | Eメール | | | | 5.8アラート通知先を参照 |  |
| ネットワーク | | | | |  |  |
|  | VPC | | | | 本番環境用VPC | 環境を起動するVPCを指定 |
|  | ロードバランサーの設定 | | | | アプリケーションを実行する各アベイラビリティーゾーン (AZ) で、ロードバランサーをサブネットに割り当てる。 パブリックアクセス可能なアプリケーションとする場合は、可視性をパブリックに設定し、パブリックサブネットを選択する。 | |
|  |  | 可視性 | | | パブリック | 接続された VPC からのみアプリケーションがリクエストを処理する場合は、ロードバランサーを内部に作成する。 パブリックロードバランサーはインターネットからリクエストを処理する。 |
|  |  | ロードバランサーのサブネット | | | ロードバランサー用サブネット | ロードバランサーを接続するサブネットを指定 |
|  | インスタンスの設定 | | | | アプリケーションを実行するインスタンスの各 AZ のサブネットを選択する。 インスタンスのインターネットへの公開を回避するには、プライベートサブネットのインスタンスとパブリックサブネットのロードバランサーを実行する。 同じパブリックサブネットでロードバランサーとインスタンスを実行するには、インスタンスにパブリック IP アドレスを割り当てる。 | |
|  |  | パブリック IP アドレス | | | 無効 | 環境内の Amazon EC2 インスタンスにパブリック IP アドレスを割り当てる場合は有効とする。 |
|  |  | インスタンスサブネット | | | WebAPサーバー用サブネット | WebAPサーバーを接続するサブネットを指定 |
| データベース | | | | | 開発およびテスト用に、Amazon RDS SQL データベースを環境に追加する。 AWS Elastic Beanstalk はデータベースのホスト名、ユーザー名、パスワード、テーブル名、ポートの環境のプロパティを設定し、インスタンスに接続情報を提供する。 環境にデータベースを追加するときに、ライフサイクルは環境に固定される。  実稼働環境では、インスタンスを外部データベースに接続するよう設定できる。 | |
|  | スナップショットの復元 | | | | RDSを使用するため、データベースは作成しない。 | アカウントの既存のスナップショットを復元するか、新しいデータベースを作成する。 |
|  | データベース設定 | | | | 環境のデータベースのエンジンとインスタンスタイプを選択する。 | |
|  |  | エンジン | | | RDSを使用するため、データベースは作成 |  |
|  |  | エンジンバージョン | | | しない。 |  |
|  |  | インスタンスクラス | | |  |  |
|  |  | ストレージ | | |  | 5 GB ～ 1024 GB を入力する。 |
|  |  | ユーザー名 | | |  |  |
|  |  | パスワード | | |  |  |
|  |  | 保持期間 | | |  | 環境終了時のスナップショット保存について指定 |
|  |  | 可用性 | | |  |  |

#### 検証環境用WebAPサーバー(EC2)

本システムでは検証環境用WebサーバーとしてEC2サービスを利用する。

以下にEC2の定義を示す。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | 検証環境 | 備考 |
| Amazonマシーンイメージ(AMI) | | | Amazon Linux 2 AMI (HVM), SSD Volume Type | ami-06631ebafb3ae5d34 |
| サーバー名 | | | stg-aeras-corporate-site-system-webap01 | ホスト名、タグNameに指定する。 |
| インスタンスタイプの設定 | | | t3.medium | ベースラインレベルの CPU パフォーマンスを提供する次世代のバースト可能な汎用インスタンスタイプ  vCPU：2 / メモリ：4GiB |
| インスタンスの詳細の設定 | | |  |  |
|  | インスタンス数 | | 1 |  |
|  | 購入のオプション | | 無効 | スポットインスタンスをリクエストして、支払い可能なインスタンス時間当たりの最高価格が指定できる。 |
|  | ネットワーク | | 検証環境VPC | インスタンスを作成するVPCを指定 |
|  | サブネット | | WebAPサーバー用サブネット  (2.5.2サブネットを参照) | 異なる EC2 リソースを互いに、またはインターネットから隔離するために使用できる VPC の IP アドレス範囲。 |
|  | 自動割り当てパブリックIP | | 無効化 | 固定IPを割り当てる |
|  | 配置グループ | | 無効 | ワークロードのニーズに対応するための独立したインスタンスのグループ |
|  | キャパシティーの予約 | | なし | キャパシティー予約では、特定のアベイラビリティーゾーンの EC2 インスタンスに対してキャパシティーを予約する。 |
|  | IAMロール | | EC2(WebAPサーバー)用ロール  (6.2ロール管理を参照) | AM ロールはそれを引き受けるリソースに自動的に AWS 認証情報をデプロイする。 |
|  | シャットダウン動作 | | 停止 | OS レベルのシャットダウンが実行された時のインスタンスの動作を指定する。 |
|  | 停止‐休止動作 | | 無効 | 休止動作はインスタンスを停止し、インスタンスの RAM にある情報をルートボリュームに保存する。 |
|  | 終了保護の有効化 | | 有効 | 誤った終了を防止する。 |
|  | モニタリング | | 無効 | CloudWatch 詳細モニタリングを有効化する。(追加料金が適用される。) |
|  | テナンシー | | 共有 | ご利用の目的にあわせて、完全専有の物理サーバーでインスタンスを実行することができる。 |
|  | Elastic Inference | | 無効 | 深層学習による推論におけるコスト効率に優れたハードウェアアクセラレーションを提供する。 |
|  | クレジット仕様 | | standard | クレジット仕様で無制限を選択すると、いつでも必要な分だけ、アプリケーションがベースラインを超えてバースト可能になる。 |
|  | ファイルシステム | | - | インスタンスにマウントする Amazon EFS ファイルシステムを指定する。 |
| ストレージの追加 | | |  |  |
|  | ボリュームタイプ | | ルート | インスタンスを起動し実行するためのOSが割り当てられているAmazon EBSのボリューム。 |
|  |  | デバイス | /dev/xvda | ボリュームで使用可能なデバイス名。 |
|  |  | サイズ | 30 GiB | ストレージ容量 |
|  |  | ボリュームタイプ | 汎用SSD (gp2) | 汎用 (SSD) ボリュームは、3000 IOPS までのバーストが可能で、1 GiB あたり 3 IOPS の一貫したベースラインで機能する。 |
|  |  | 終了時に削除 | 有効 | EBS ボリュームは、EC2 インスタンスの運用状況から独立した永続性を持つ。ただし、関連付けられたインスタンスが終了されたときに EBS ボリュームが自動的に削除されるように選択することができる。 |
|  |  | 暗号化 | 6.3暗号化方針を参照 |  |
| セキュリティグループの設定 | | | WebAPサーバー用セキュリティグループ  (2.5.4セキュリティグループを参照) | インスタンスのトラフィックを制御するファイアウォールのルールセット |

### DBサーバー(RDS)

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-aeras-corporate-site-system-rds | stg-aeras-corporate-site-system-rds | AWSリージョン内で一意の名称を指定 |
| アベイラビリティゾーン | | - | ap-northeast-1a |  |
| 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.m5.xlarge | db.m5.xlarge | 最新世代のメモリ最適化インスタンス |
|  | vCPU | 4 | 4 |  |
|  | メモリ | 16 GiB | 16 GiB |  |
| バージョン | | MySQL 8.0.25 | MySQL 8.0.25 | 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 | 500 GiB | 20 GiB | 本番環境は現行環境と同様の値を指定  検証環境は最小値を指定 |
|  | ストレージの自動スケーリング | 有効 | 無効 |  |
|  | 最大ストレージしきい値 | 1000 GiB | - | 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 | 2.5ネットワーク構成を参照 | 2.5ネットワーク構成を参照 |  |
|  | サブネットグループ | 2.5ネットワーク構成を参照 | 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 | 2.5ネットワーク構成を参照 | 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。 |
| データベース名 | | aerascorporatesitedb | aerascorporatesitedb |  |
| 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 | | 有効 | 有効 |  |
| 暗号化 | | 6.3暗号化方針を参照 | 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 | | 監査ログ  エラーログ  全般ログ  スロークエリログ | 監査ログ  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 | | 5.7ソフトウェアのアップデートを参照 | 5.7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)

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

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| バケット名 | | 本番環境：prod-aeras-corporate-site-system-data  検証環境：stg-aeras-corporate-site-system-data |  |
| アクセス設定 | | パブリックアクセスをすべて許可 | インターネットから接続可とする。 |
| バケットポリシー | |  |  |
|  | プリンシパル | WordPress用CloudFrontディストリビューション | WordPress用CloudFrontからのみアクセス可とする。 |
|  | 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 | | 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 | dataacclog/ |  |

#### 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-aeras-corporate-site-system-app  検証環境：stg-aeras-corporate-site-system-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 | | 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/ |  |
| ライフサイクルルール | | バッチサーバーのキャッシュ保存期間を30日に設定 | オブジェクトの現行バージョンの有効期限を設定し、有効期限が切れたオブジェクトを完全に削除する。 |

#### 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-aeras-corporate-site-system-backup  検証環境：stg-aeras-corporate-site-system-backup |  |
| 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 | | 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/ |  |
| ライフサイクルルール | | データストレージ(S3)バックアップの保存期間を設定  5.1.1バックアップを参照 | オブジェクトの現行バージョンの有効期限を設定し、有効期限が切れたオブジェクトを完全に削除する。 |

#### ログストレージ

|  |  |  |
| --- | --- | --- |
| 項目 | 設定値 | 備考 |
| バケット名 | 本番環境：prod-aeras-corporate-site-system-log  検証環境：stg-aeras-corporate-site-system-log |  |
| 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 | 6.3暗号化方針を参照 |  |
| ライフサイクルルール | 5.5.2ログ保存期間を参照 | オブジェクトの現行バージョンの有効期限を設定し、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-aeras-corporate-site-system-cloudtrail  検証環境：stg-aeras-corporate-site-system-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 | | 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 | | 5.5.2ログ保存期間を参照 | オブジェクトの現行バージョンの有効期限を設定し、有効期限が切れたオブジェクトを完全に削除する。 |

### バッチサーバー(CodeBuild)

本システムではスクリプトによるジョブ実行のため、CodeBuildを利用する。

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 設定値 | 備考 |
| プロジェクト名 | | 本番環境：  prod-aeras-corporate-site-system-ImportBatch  検証環境：  stg-aeras-corporate-site-system-ImportBatch | プロジェクト名は 2～255 文字にする必要がある。アルファベット (A～Z、a～z)、番号 (0～9)、特殊文字 (- と \_) を含めることができる。 |
| ソース | |  |  |
|  | ソースプロバイダ | Amazon S3 | ビルドするソースコードの場所を指定 |
|  | リポジトリ | アプリケーションストレージ(S3) |  |
| 環境 | |  |  |
|  | 環境イメージ | マネージド型イメージ | コードを実行する環境を指定 |
|  | オペレーティングシステム | Amazon Linux 2 |  |
|  | ランタイム | Standard |  |
|  | イメージ | aws/codebuild/amazonlinux2-x86\_64-standard:3.0 |  |
|  | イメージのバージョン | 最新のイメージ |  |
|  | 環境タイプ | Linux |  |
|  | 特権付与 | 無効 | Docker イメージを構築するか、ビルドで昇格されたアクセス権限を取得するには、このフラグを有効にする |
| サービスロール | | EC2(WebAPサーバー)用ロール  (6.2ロール管理を参照) | 権限 |
| タイムアウト | | テスト実行後記載 | デフォルトのタイムアウトは1時間 |
| VPC | | 本番環境：本番環境VPC  検証環境：検証環境VPC | 接続先のVPC |
| サブネット | | バッチサーバー用サブネット |  |
| セキュリティグループ | | バッチサーバー用セキュリティグループ |  |
| ビルド仕様 | | buildspec ファイルを使用する | buildspec.ymlを使用してビルドする |
| キャッシュ | |  |  |
|  | キャッシュタイプ | S3 | キャッシュを作成し、ビルド時間を短縮する。 |
|  | キャッシュバケット | アプリケーションストレージ(S3) |  |
| ログ | |  |  |
|  | CloudWatch Logs | 有効 | ログ出力設定 |
|  | S3 | 有効 |  |

### ソース管理サーバー(CodeCommit)

本システムではソースコード管理のため、CodeCommitを利用する。

|  |  |  |
| --- | --- | --- |
| 項目 | 設定値 | 備考 |
| リポジトリ名 | aeras-corporate-site-system-codecommit-repo | 本番環境 / 検証環境 共通で使用する。 |

## ソフトウェア構成

### WebAPサーバー

本システムではWebサービスのコンテンツ管理ソフトウェアとしてWordPressを使用する。

#### インストールパッケージ

構築時点で最新のバージョンをインストールする。

|  |  |  |  |
| --- | --- | --- | --- |
| インストールソフトウェア | バージョン | パッケージファイル | 備考 |
| WordPress | 5.8 | - | 以下からダウンロード  http://wordpress.org/latest.tar.gz |
| php | 7.4.21 | libzip.x86\_64 0:1.3.2-1.amzn2.0.1 | WordPressを利用するため |
|  |  | php-7.4.21-1.amzn2.x86\_64 |  |
|  |  | php-cli.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-common.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-fpm.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-json.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-mysqlnd.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-pdo.x86\_64 0:7.4.21-1.amzn2 |  |
| httpd | 2.4.48 | apr-util-bdb.x86\_64 0:1.6.1-5.amzn2.0.2 |  |
| (自動起動) |  | apr-util.x86\_64 0:1.6.1-5.amzn2.0.2 |  |
|  |  | apr.x86\_64 0:1.6.3-5.amzn2.0.2 |  |
|  |  | generic-logos-httpd.noarch 0:18.0.0-4.amzn2 |  |
|  |  | httpd-filesystem.noarch 0:2.4.48-2.amzn2 |  |
|  |  | httpd-tools.x86\_64 0:2.4.48-2.amzn2 |  |
|  |  | httpd.x86\_64 0:2.4.48-2.amzn2 |  |
|  |  | mailcap.noarch 0:2.1.41-2.amzn2 |  |
|  |  | mod\_http2.x86\_64 0:1.15.19-1.amzn2.0.1 |  |
| mysql-community-client | 8.0.26 | mariadb-libs.x86\_64 1:5.5.68-1.amzn2 | DB接続のため |
|  |  | mysql-community-client-plugins.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-client.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-common.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-libs-compat.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-libs.x86\_64 0:8.0.26-1.el7 |  |
|  |  | ncurses-compat-libs.x86\_64 0:6.0-8.20170212.amzn2.1.3 |  |
| php-xml | 7.4.21 | libxslt.x86\_64 0:1.1.28-6.amzn2 | WP Offload Media Liteプライグインを使用するため |
|  |  | php-xml.x86\_64 0:7.4.21-1.amzn2 |
| php-gd | 7.4.21 | php-gd.x86\_64 0:7.4.21-1.amzn2 |  |
| amazon-cloudwatch-agent  (自動起動) | 1.247347.4 | amazon-cloudwatch-agent.x86\_64 0:1.247347.4-1.amzn2 | CloudWatchによるメトリクス、ログ収集のため |

#### WordPress設定

画像や動画をデータストレージ(S3)に格納し、WebAPサーバーのローカルストレージ使用量の増加を防ぐ。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項目 | | | 設定値 | 備考 |
| ユーザー名 | | | パスワード一覧を参照 |  |
| パスワード | | | パスワード一覧を参照 |  |
| 一般設定 | | |  |  |
|  | WordPress アドレス (URL) | | http://www.<ドメイン名> |  |
|  | サイトアドレス (URL) | | http://www.<ドメイン名> |  |
| wp-config.php | | |  |  |
|  | ブラウザクッキーに対する暗号化レイヤー | | 設定する | 以下よりキーセット値を取得  https://api.wordpress.org/secret-key/1.1/salt/ |
|  | httpsリダイレクト設定 | | 設定する | 「/\* Add any custom values between this line and the "stop editing" line. \*/」下に以下を追記  define('WP\_SITEURL', 'https://' . $\_SERVER['HTTP\_HOST'] . '/');  define('WP\_HOME', 'https://' . $\_SERVER['HTTP\_HOST'] . '/');  if (strpos($\_SERVER['HTTP\_CLOUDFRONT\_FORWARDED\_PROTO'], 'https') !== false) {  $\_SERVER['HTTPS'] = 'on';  } |
| プラグイン | | |  |  |
|  | WP Offload Media Lite for Amazon S3, DigitalOcean Spaces, and Google Cloud Storage | | 設定する | メディアファイルをデータストレージ(S3)に格納する |
|  |  | ストレージ | データストレージ(S3) | メディアファイルをデータストレージ(S3)に格納する。 |
|  |  | ストレージ接続方式 | IAM Role |  |
|  |  | ファイルをバケットにコピーする | 有効 |  |
|  |  | パス | wp-content/uploads/ |  |
|  |  | 年/月 | 有効 | メディアファイルを指定したパス配下の年/月フォルダに格納する |
|  |  | バージョニング | 無効 | メディア格納パスにタイムスタンプを追加する |
|  |  | プロバイダー | Amazon CloudFront | サイトの速度向上のため、CloudFrontを利用する |
|  |  | カスタムドメイン | www.<ドメイン名> |  |
|  |  | HTTPS強制 | 無効 | オリジンへはhttp接続を利用する |
|  |  | サーバからファイルを削除する | 有効 | S3への転送後、サーバからファイルを削除し、サーバのストレージ使用量増加を防ぐ |
| セキュリティ設定 | | | .htaccessファイルによりアクセス制御を設定する | |
|  | CloudFront経由のみのリクエストをWebアクセス許可する | | 有効 |  |
|  | wp-config.phpへのアクセス | | 拒否 |  |
|  | IPアドレスによる管理画面のアクセス制限 | | |  |
|  |  | 許可IPアドレス | 121.3.87.196 | アエラス様 |
|  |  |  |  | H2O様 |

### バッチサーバー(CodeBuild)

本システムではバッチ処理を実行するサーバーとしてPHP実行環境、及びMySQLクライアント環境を構築する。

#### インストールパッケージ

構築時点で最新のバージョンをインストールする。

|  |  |  |  |
| --- | --- | --- | --- |
| インストールソフトウェア | バージョン | パッケージファイル | 備考 |
| php | 7.4.21 | libzip.x86\_64 0:1.3.2-1.amzn2.0.1 | PHPを実行するため |
|  |  | php-7.4.21-1.amzn2.x86\_64 |  |
|  |  | php-cli.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-common.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-fpm.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-json.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-mysqlnd.x86\_64 0:7.4.21-1.amzn2 |  |
|  |  | php-pdo.x86\_64 0:7.4.21-1.amzn2 |  |
| mysql-community-client | 8.0.26 | mariadb-libs.x86\_64 1:5.5.68-1.amzn2 | DB接続のため |
|  |  | mysql-community-client-plugins.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-client.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-common.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-libs-compat.x86\_64 0:8.0.26-1.el7 |  |
|  |  | mysql-community-libs.x86\_64 0:8.0.26-1.el7 |  |
|  |  | ncurses-compat-libs.x86\_64 0:6.0-8.20170212.amzn2.1.3 |  |

## 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

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-aeras-corporate-site-system-vpc | stg-aeras-corporate-site-system-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 | 172.29.0.0/16 | 172.30.0.0/16 | /16 ネットマスク（65,536 個の IP アドレス）から /28 ネットマスク（16 個の IP アドレス）の間でCIDRブロックを指定する。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。 |

なお、IPv4でVPCを作成する場合、以下の通りRFC 1918 の範囲でCIDRブロックを指定することが推奨されている。

|  |  |
| --- | --- |
| RFC 1918 の範囲 | CIDR ブロックの例 |
| 10.0.0.0 - 10.255.255.255 (10/8 プレフィックス) | VPC は /16 以下 (10.0.0.0/16 など) にする必要がある。 |
| 172.16.0.0 - 172.31.255.255 (172.16/12 プレフィックス) | VPC は /16 以下 (172.31.0.0/16 など) にする必要がある。 |
| 192.168.0.0 - 192.168.255.255 (192.168/16 プレフィックス) | VPC を小さく (192.168.0.0/20 などに) することができる。 |

### サブネット

VPCのネットワーク範囲を区切るサブネットを作成する。

/28 ネットマスクから /16 ネットマスクの間のブロックサイズでIPアドレスの範囲を指定する必要がある。

本システムでは、インターネットに接続するパブリックサブネットと、インターネットに接続しないプライベートサブネットを作成する。

#### 本番環境用サブネット

|  |  |  |  |
| --- | --- | --- | --- |
| パブリックサブネット | サブネット名 | アベイラビリティゾーン | IPv4 CIDRブロック |
| バッチサーバー用サブネット | prod-aeras-corporate-site-system-batch-public-subnet01 | ap-northeast-1a | 172.29.0.0/24 |
|  | prod-aeras-corporate-site-system-batch-public-subnet02 | ap-northeast-1c | 172.29.1.0/24 |
| ロードバランサー用サブネット | prod-aeras-corporate-site-system-lb-public-subnet01 | ap-northeast-1a | 172.29.16.0/20 |
|  | prod-aeras-corporate-site-system-lb-public-subnet02 | ap-northeast-1c | 172.29.32.0/20 |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| WebAPサーバー用サブネット | prod-aeras-corporate-site-system-webap-private-subnet01 | ap-northeast-1a | 172.29.48.0/20 |
|  | prod-aeras-corporate-site-system-webap-private-subnet02 | ap-northeast-1c | 172.29.64.0/20 |
| RDS用サブネット | prod-aeras-corporate-site-system-rds-private-subnet01 | ap-northeast-1a | 172.29.80.0/28 |
|  | prod-aeras-corporate-site-system-rds-private-subnet02 | ap-northeast-1c | 172.29.80.16/28 |

#### 検証環境用サブネット

|  |  |  |  |
| --- | --- | --- | --- |
| パブリックサブネット | サブネット名 | アベイラビリティゾーン | IPv4 CIDRブロック |
| NAT Gateway用サブネット | stg-aeras-corporate-site-system-natgateway-public-subnet01 | ap-northeast-1a | 172.30.0.0/20 |
| WebAPサーバー用サブネット | stg-aeras-corporate-site-system-webap-public-subnet01 |  | 172.30.16.0/20 |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| バッチサーバー用サブネット | stg-aeras-corporate-site-system-batch-private-subnet01 | ap-northeast-1a | 172.30.32.0/20 |
| RDS用サブネット | stg-aeras-corporate-site-system-rds-private-subnet01 | ap-northeast-1a | 172.30.48.0/28 |
|  | stg-aeras-corporate-site-system-rds-private-subnet02 | ap-northeast-1c | 172.30.48.16/28 |

### ネットワークACL

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 |
| NATゲートウェイ用NACL | prod-aeras-corporate-site-system-natgateway-nacl | stg-aeras-corporate-site-system-natgateway-nacl | NATゲートウェイ用サブネット | すべて | すべて |
| WebAPサーバー用NACL | prod-aeras-corporate-site-system-webap-nacl | stg-aeras-corporate-site-system-webap-nacl | WebAPサーバー用サブネット | すべて | すべて |
| RDS用NACL | prod-aeras-corporate-site-system-rds-nacl | stg-aeras-corporate-site-system-rds-nacl | RDS用サブネット | バッチサーバー用サブネット | バッチサーバー用サブネット |
|  |  |  |  | WebAPサーバー用サブネット | WebAPサーバー用サブネット |
| バッチサーバー用NACL | prod-aeras-corporate-site-system-batch-nacl | stg-aeras-corporate-site-system-batch-nacl | バッチサーバー用サブネット | すべて | すべて |

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

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。

#### 本番環境用セキュリティグループ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | 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 | セキュリティグループ名 | 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 | 備考 |
| バッチサーバー用セキュリティグループ | prod-aeras-corporate-site-system-batch-sg | - | - | すべて：すべて | 0.0.0.0/0 |  |
| WebAPサーバー用セキュリティグループ | prod-aeras-corporate-site-system-webap-sg | TCP：443 | 0.0.0.0/0 | すべて：すべて | 0.0.0.0/0 | HTTPS接続を許可 |
| RDS用セキュリティグループ | prod-aeras-corporate-site-system-rds-sg | TCP：3306 | バッチサーバー用セキュリティグループ | すべて：すべて | 0.0.0.0/0 |  |
|  |  |  | WebAPサーバー用セキュリティグループ |  |  |  |

#### 検証環境用セキュリティグループ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | 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 | セキュリティグループ名 | 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 | 備考 |
| バッチサーバー用セキュリティグループ | stg-aeras-corporate-site-system-batch-sg | - | - | すべて：すべて | 0.0.0.0/0 |  |
| WebAPサーバー用セキュリティグループ | stg-aeras-corporate-site-system-webap-sg | TCP：22 | 0.0.0.0/0 | すべて：すべて | 0.0.0.0/0 | SSH接続を許可 |
| TCP:80 |  |  | HTTP接続を許可 |
| RDS用セキュリティグループ | stg-aeras-corporate-site-system-rds-sg | TCP：3306 | バッチサーバー用セキュリティグループ | すべて：すべて | 0.0.0.0/0 |  |
|  |  |  | WebAPサーバー用セキュリティグループ |  |  |  |

### ルートテーブル

#### パブリックサブネット用ルートテーブル

パブリックサブネット用に以下のルートテーブルを作成する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 | 備考 |
| ルートテーブル名 | | prod-aeras-corporate-site-system-public-rt | stg-aeras-corporate-site-system-public-rt |  |
| 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 |  |
| ルート | |  |  |  |
|  | 送信先 | 0.0.0.0/0 | 0.0.0.0/0 |  |
|  | ターゲット | インターネットゲートウェイ | インターネットゲートウェイ |  |
| サブネットの関連付け | | WebAPサーバー用サブネット | WebAPサーバー用サブネット |  |
|  | | NAT Gateway用サブネット | NAT Gateway用サブネット |  |

#### プライベートサブネット用ルートテーブル

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-aeras-corporate-site-system-private-rt | stg-aeras-corporate-site-system-private-rt |  |
| 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 |  |
| ルート | |  |  |  |
|  | 送信先 | 0.0.0.0/0 | 0.0.0.0/0 |  |
|  | ターゲット | NATゲートウェイ | NATゲートウェイ |  |
| サブネットの関連付け | | バッチサーバー用サブネット | バッチサーバー用サブネット |  |
|  | | RDS用サブネット | RDS用サブネット |  |

### インターネットゲートウェイ

VPCをインターネットに接続する要件がある場合、インターネットゲートウェイを作成する。

本システムでは検証環境のWebAPサーバーにインターネットからSSH接続する必要があるため、インターネットゲートウェイを作成する。

|  |  |  |
| --- | --- | --- |
|  | 本番環境 | 検証環境 |
| インターネットゲートウェイ | prod-aeras-corporate-site-system-igw | stg-aeras-corporate-site-system-igw |

### NATゲートウェイ

プライベートサブネットからインターネットに接続する要件がある場合、NATゲートウェイを作成する。

本システムではプライベートサブネットにあるバッチサーバーからインターネットに接続する必要があるため、NATゲートウェイを作成する。

|  |  |  |
| --- | --- | --- |
|  | 本番環境 | 検証環境 |
| NATゲートウェイ | prod-aeras-corporate-site-system-ngw | stg-aeras-corporate-site-system-ngw |

### 名前解決

本システムでは、DNSサーバーとしてRoute53を利用する。

# 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% | Elastic Load Balancing / Kinesis Data Firehose |
| 99.95% | API Gateway / AWS WAF / RDS |
| 99.9% | ACM / AWS Backup / AWS Systems Manager / CodeBuild / CodeCommit / CloudFront / CloudTrail / CloudWatch / Cognito / DataSync / EC2 / KMS / NAT Gateway / 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

本システムの拡張性についてサーバー別に記載する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | 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 |
| WebAPサーバー | ストレージ容量 | ストレージ容量の手動追加 | 不要 | 必要 |
| 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 |
| DBサーバー | ストレージ容量 | [本番環境]  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自動で拡張する。  ・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。 | 不要 |  |
|  |  | [検証環境]  ストレージ容量の手動拡張 |  |  |
|  | 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 | ストレージ容量 | 自動拡張 | 不要 |  |
| バッチサーバー | ストレージ容量 | インスタンスタイプの変更 | 必要 |  |
|  | 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 |  |
| ソース管理サーバー | ストレージ容量 | 自動拡張 | 不要 |  |
|  | CPU | 自動拡張 | 不要 |  |
|  | メモリ | 自動拡張 | 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 対象 | 保存期間 | スケジュール | バックアップ方式 | 暗号化 | バックアップ保存先 |
| データベース(RDS) | 35日 | 連続 | 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 |
| データストレージ(S3) |  | 日次 3:00 | 増分バックアップ |
| 検証環境WebAPサーバー(EC2) | 任意 | 任意 | 完全バックアップ |

### リストア

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。

|  |  |  |  |
| --- | --- | --- | --- |
| 対象 | リストア方式 | 復旧時点 | 復旧時間 |
| 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。 | 保存期間内の任意の時点 | 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 |
| 検証環境用WebAPサーバー(EC2) | AWSマネジメントコンソールより、WebAPサーバー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

本システムの本番環境では以下のジョブを実行する。

検証環境においてはジョブを実行しない。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 種別 | ジョブ | 内容 | 成功時 | 失敗時 |
| バッチ処理 | 物件情報インポート | バッチサーバーでレンターズの物件情報システムの情報を取得し、本システムにインポートする。 | ・ログ出力 | ・ログ出力  ・メールによる |
|  | DB最適化 実行時間 | DBテーブルの断片化を解消し、最適化する。 |  | アラート通知 |
| バックアップ | 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。 |  |  |

### ジョブ監視

本システムでは本番環境で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。

アラートの通知先は5.8アラート通知先を参照する。

検証環境についてはアラート通知は行わない。

## URL監視

本システムではCloudWatchにより本番環境のURLを監視し、URL監視が失敗した際にメールによるアラート通知を行う。

検証環境については業務影響がないためURL監視は実施しない。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | スクリーンショット | タイムアウト | データ保持 | | メール通知ルール | |
| 対象 | スケジュール | 監視実行データ保存先 | 障害データ | 成功データ | 期間 | 失敗回数 |
| 本番環境URL | 取得しない | 1分 | 31日 | 31日 | 1時間 | 2回 |
| 10分おき | ログストレージ(S3) |

メール通知ルールの期間は1時間 / 6時間 / 1日間 から選択する。

## 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。 |

#### Auto Scaling group

|  |  |
| --- | --- |
| メトリクス | 内容 |
| GroupMinSize | Auto Scaling グループの最小サイズ。 |
| GroupMaxSize | Auto Scaling グループの最大サイズ。 |
| GroupDesiredCapacity | Auto Scaling グループが保持しようとするインスタンスの数。 |
| GroupInServiceInstances | Auto Scaling グループの一部として実行するインスタンスの数。このメトリクスには保留中もしくは終了処理中のインスタンスは含まれない。 |
| GroupPendingInstances | 保留中のインスタンスの数。保留中のインスタンスは、稼働状態ではない。このメトリクスには稼働中もしくは終了処理中のインスタンスは含まれない。 |
| GroupStandbyInstances | Standby 状態にあるインスタンスの数。この状態のインスタンスはまだ実行中だが、実際には使用されていない。 |
| GroupTerminatingInstances | 終了処理中のインスタンスの数。このメトリクスには稼働中もしくは保留中のインスタンスは含まれない。 |
| GroupTotalInstances | Auto Scaling グループに含まれるインスタンスの合計数。このメトリクスは稼働中、保留中、および終了処理中のインスタンスの数を特定する。 |

#### 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 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。 |

#### CloudFront

デフォルトのメトリクスを監視対象とする。

追加のメトリクスとして以下が監視可能であるが、追加料金が必要となるためパフォーマンスに問題が生じた場合に監視の実施を検討する。

・キャッシュヒット率 / オリジンのレイテンシー / ステータスコード別のエラー率

|  |  |
| --- | --- |
| メトリクス | 内容 |
| Requests | すべての HTTP メソッド、および HTTP リクエストと HTTPS リクエストの両方について CloudFront が受信したビューワーリクエストの総数。 |
| Bytes downloaded | GET リクエスト、HEAD リクエスト、および OPTIONS リクエストに対してビューワーがダウンロードしたバイト総数 |
| Bytes uploaded | POST リクエストと PUT リクエストを使用して CloudFront でビューワーがオリジンにアップロードしたバイト総数 |
| 4xx error rate | レスポンスの HTTP ステータスコードが 4xx であるすべてのビューワーリクエストの割合 |
| 5xx error rate | レスポンスの HTTP ステータスコードが 5xx であるすべてのビューワーリクエストの割合 |
| Total error rate | レスポンスの HTTP ステータスコードが 4xx または 5xx であるすべてのビューワーリクエストの割合 |

#### CodeBuild

|  |  |
| --- | --- |
| メトリクス | 内容 |
| SucceededBuilds | 成功したビルドの数 |
| FailedBuilds | 失敗したビルドの数 |
| Builds | ビルドの合計数 |
| Duration | ビルドの所要時間 |

#### 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。 |

#### EC2

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| CloudWatchエージェント不要で | CPUUtilization | CPU 使用率 |
| 収集できるメトリクス | NetworkIn | インバウンド ネットワーク使用率 |
|  | NetworkOut | アウトバウンド ネットワーク使用率 |
|  | DiskReadOps | ディスク読み取りパフォーマンス |
|  | DiskWriteOps | ディスク書き込みパフォーマンス |
|  | DiskReadBytes | ディスク読み取りバイト数 |
|  | DiskWriteBytes | ディスク書き込みバイト数 |
| CloudWatchエージェントが収集するメトリクス | cpu\_time\_active | 任意の容量で CPU がアクティブになっている時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_guest | ゲストオペレーティングシステムで CPU が仮想 CPU を実行している時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_guest\_nice | 優先度が低く、他のプロセスにより中断される場合がある、ゲストオペレーティングシステムの仮想 CPU を CPU で実行している時間。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_idle | CPU がアイドル状態の時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_iowait | CPU が I/O 操作の完了を待機している時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_irq | CPU が中断を処理している時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_nice | プロセスの優先度が低く、優先度の高いプロセスによって簡単に中断される場合がある、ユーザーモードになっている CPU の時間。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_softirq | CPU がソフトウェアの中断を処理している時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_steal | CPU が盗まれた時間になっている時間の長さ。これは、仮想化環境で他のオペレーティングシステムに費やされる時間です。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_system | CPU がシステムモードになっている時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_time\_user | CPU がユーザーモードになっている時間の長さ。このメトリクスは、1/100 秒単位で測定される。 |
|  | cpu\_usage\_active | 任意の容量で CPU がアクティブになっている時間の割合。 |
|  | cpu\_usage\_guest | ゲストオペレーティングシステムで CPU が仮想 CPU を実行している時間の割合。 |
|  | cpu\_usage\_guest\_nice | 優先度が低く、他のプロセスにより中断される場合がある、ゲストオペレーティングシステムの仮想 CPU を CPU で実行している時間の割合。 |
|  | cpu\_usage\_idle | CPU がアイドル状態の時間の割合。 |
|  | cpu\_usage\_iowait | CPU が I/O 操作の完了を待機している時間の割合。 |
|  | cpu\_usage\_irq | CPU が中断を処理している時間の割合。 |
|  | cpu\_usage\_nice | プロセスの優先度が低く、優先度の高いプロセスによって簡単に中断される場合がある、ユーザーモードになっている CPU の時間の割合。 |
|  | cpu\_usage\_softirq | CPU がソフトウェアの中断を処理している時間の割合。 |
|  | cpu\_usage\_steal | CPU が盗まれた時間になっている時間の割合。つまり、仮想化環境で他のオペレーティングシステムに費やされる時間。 |
|  | cpu\_usage\_system | CPU がシステムモードになっている時間の割合。 |
|  | cpu\_usage\_user | CPU がユーザーモードになっている時間の割合。 |
|  | disk\_free | ディスクの空き容量。 |
|  | disk\_inodes\_free | ディスクで使用可能なインデックスノードの数。 |
|  | disk\_inodes\_total | ディスクで予約されているインデックスノードの合計数。 |
|  | disk\_inodes\_used | ディスクで使用されているインデックスノードの数。 |
|  | disk\_total | 使用済み容量と空き容量を含む、ディスクの合計容量。 |
|  | disk\_used | ディスクの使用済み容量。 |
|  | disk\_used\_percent | ディスクスペース合計に対する使用済みの割合。 |
|  | diskio\_iops\_in\_progress | デバイスドライバーに発行されたがまだ完了していない I/O リクエストの数。 |
|  | diskio\_io\_time | ディスクが I/O リクエストをキューに入れている時間の長さ。 |
|  | diskio\_reads | ディスク読み取り操作の回数。 |
|  | diskio\_read\_bytes | ディスクから読み込まれたバイト数。 |
|  | diskio\_read\_time | 読み取りリクエストがディスクで待機した時間の長さ。複数の読み込みリクエストが同時に待機している場合、その分数値が増える。たとえば、5 つのリクエストが平均 100 ミリ秒待機している場合、500 と報告される。 |
|  | diskio\_writes | ディスク書き込み操作の回数。 |
|  | diskio\_write\_bytes | ディスクへの書き込みバイト数。 |
|  | diskio\_write\_time | 書き込みリクエストがディスクで待機した時間の長さ。複数の書き込みリクエストが同時に待機している場合、その分数値が増える。たとえば、8 つのリクエストが平均 1000 ミリ秒待機している場合、8000 と報告される。 |
|  | ethtool\_bw\_in\_allowance\_exceeded | インバウンド集計の帯域幅がインスタンスの最大値を超えたために、キューおよび (または) ドロップされたパケットの数。  このメトリクスは、CloudWatch エージェント設定ファイルの metrics\_collected セクションの ethtool サブセクションにリストされている場合にのみ収集される。 |
|  | ethtool\_bw\_out\_allowance\_exceeded | アウトバウンド集計の帯域幅がインスタンスの最大値を超えたために、キューおよび (または) ドロップされたパケットの数。  このメトリクスは、CloudWatch エージェント設定ファイルの metrics\_collected セクションの ethtool サブセクションにリストされている場合にのみ収集される。 |
|  | ethtool\_conntrack\_allowance\_exceeded | 接続トラッキングがインスタンスの最大数を超え、新しい接続を確立できなかったためにドロップされたパケットの数。これにより、インスタンスとの間で送受信されるトラフィックのパケット損失が発生する可能性がある。  このメトリクスは、CloudWatch エージェント設定ファイルの metrics\_collected セクションの ethtool サブセクションにリストされている場合にのみ収集される。 |
|  | ethtool\_linklocal\_allowance\_exceeded | ローカルプロキシサービスへのトラフィックの PPS がネットワークインターフェイスの最大値を超えたためにドロップされたパケットの数。これは、DNS サービス、インスタンスメタデータサービス、および Amazon Time Sync Service へのトラフィックに影響する。  このメトリクスは、CloudWatch エージェント設定ファイルの metrics\_collected セクションの ethtool サブセクションにリストされている場合にのみ収集される。 |
|  | ethtool\_pps\_allowance\_exceeded | 双方向 PPS がインスタンスの最大値を超えたために、キューおよび (または) ドロップされたパケットの数。  このメトリクスは、CloudWatch エージェント設定ファイルの metrics\_collected セクションの ethtool サブセクションにリストされている場合にのみ収集される。 |
|  | mem\_active | 最後のサンプル期間中に何らかの方法で使用されたメモリの量。 |
|  | mem\_available | すぐにプロセスに渡すことができる使用可能なメモリの量。 |
|  | mem\_available\_percent | すぐにプロセスに渡すことができる使用可能なメモリの割合。 |
|  | mem\_buffered | バッファに使用されているメモリの量。 |
|  | mem\_cached | ファイルキャッシュに使用されているメモリの量。 |
|  | mem\_free | 使用されていないメモリの量。 |
|  | mem\_inactive | 最後のサンプル期間中に何らかの方法で使用されていないメモリの量。 |
|  | mem\_total | メモリの合計量。 |
|  | mem\_used | 現在使用中のメモリの量。 |
|  | mem\_used\_percent | 現在使用中のメモリの割合。 |
|  | net\_bytes\_recv | ネットワークインターフェイスで受信されたバイトの数。 |
|  | net\_bytes\_sent | ネットワークインターフェイスで送信されたバイトの数。 |
|  | net\_drop\_in | このネットワークインターフェイスで受信されたパケットのうち、削除されたものの数。 |
|  | net\_drop\_out | このネットワークインターフェイスで送信されたパケットのうち、削除されたものの数。 |
|  | net\_err\_in | このネットワークインターフェイスによって検出された受信エラーの数。 |
|  | net\_err\_out | このネットワークインターフェイスによって検出された送信エラーの数。 |
|  | net\_packets\_sent | このネットワークインターフェイスで送信されたパケットの数。 |
|  | net\_packets\_recv | このネットワークインターフェイスで受信されたパケットの数。 |
|  | netstat\_tcp\_close | 状態のない TCP 接続の数。 |
|  | netstat\_tcp\_close\_wait | クライアントからの終了リクエストを待機している TCP 接続の数。 |
|  | netstat\_tcp\_closing | クライアントからの確認付き終了リクエストを待機している TCP 接続の数。 |
|  | netstat\_tcp\_established | 確立された TCP 接続の数。 |
|  | netstat\_tcp\_fin\_wait1 | 接続の終了プロセス時に FIN\_WAIT1 状態になっている TCP 接続の数。 |
|  | netstat\_tcp\_fin\_wait2 | 接続の終了プロセス時に FIN\_WAIT2 状態になっている TCP 接続の数。 |
|  | netstat\_tcp\_last\_ack | クライアントが接続終了メッセージの確認を送信するのを待機している TCP 接続の数。これは、接続が終了する直前の最後の状態。 |
|  | netstat\_tcp\_listen | 現在接続リクエストをリッスンしている TCP ポートの数。 |
|  | netstat\_tcp\_none | 非アクティブなクライアントを持つ TCP 接続の数。 |
|  | netstat\_tcp\_syn\_sent | 接続リクエストを送信したあとに一致する接続リクエストを待機している TCP 接続の数。 |
|  | netstat\_tcp\_syn\_recv | 接続リクエストを送受信したあとに接続リクエスト確認を待機している TCP 接続の数。 |
|  | netstat\_tcp\_time\_wait | クライアントが接続終了リクエストの確認を受信したことが確認されるのを現在待機している TCP 接続の数。 |
|  | netstat\_udp\_socket | 現在の UDP 接続の数。 |
|  | processes\_blocked | ブロックされているプロセスの数。 |
|  | processes\_dead | 「dead」となっているプロセスの数。Linux では、X 状態コードにより示される。 |
|  | processes\_idle | アイドル状態になっているプロセスの数 (20 秒以上スリープ状態)。FreeBSD インスタンスでのみ使用できる。 |
|  | processes\_paging | 「paging」となっているプロセスの数。Linux では、W 状態コードにより示される。 |
|  | processes\_running | 実行されているプロセスの数。R 状態コードにより示される。 |
|  | processes\_sleeping | スリープ状態になっているプロセスの数。S 状態コードにより示される。 |
|  | processes\_stopped | 停止されているプロセスの数。T 状態コードにより示される。 |
|  | processes\_total | インスタンス上でのプロセスの合計数。 |
|  | processes\_total\_threads | プロセスを構成するスレッドの合計数。このメトリクスは、Linux インスタンスでのみ有効。 |
|  | processes\_wait | ページングしているプロセスの数。FreeBSD インスタンスでは、W 状態コードにより示されます。このメトリクスは FreeBSD インスタンスでのみ使用でき、Linux、Windows サーバー、macOS インスタンスでは使用できない。 |
|  | processes\_zombies | ゾンビ状態のプロセスの数。Z 状態コードにより示される。 |
|  | swap\_free | 使用されていないスワップスペースの量。 |
|  | swap\_used | 現在使用中のスワップスペースの量。 |
|  | swap\_used\_percent | 現在使用中のスワップスペースの割合。 |

#### Elastic Beanstalk

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| Webサーバーのメトリクス | RequestCount | 直前の 10 秒間にウェブサーバーによって処理されたリクエストの 1 秒あたりの数。EB CLI と r/sec に表示される平均 環境の状態ページ (1 秒ごとのリクエスト)。 |
|  | Status2xx | 直前の 10 秒間に各タイプのステータスコードが返されたリクエストの数。たとえば、正常なリクエストには 200 OK、リダイレクトには 301 が返され、アプリケーション内のどのリソースとも一致しない URL が入力された場合は 404 が返される。  EB CLI と 環境の状態ページ は、インスタンスへのリクエスト未処理数、そして環境内の総体的なリクエストのパーセンテージとしてこれらのメトリクスを示す。 |
|  | Status3xx |
|  | Status4xx |
|  | Status5xx |
|  | p99.9 | 最近 10 秒間で最も遅かったリクエストの x パーセントの平均レイテンシー。x はこの数値と 100 との差異。たとえば、p99 1.403 は、直前の 10 秒間に応答が返るのが最も遅かったリクエストの 1% の平均レイテンシーが 1.403 秒であったことを示す。 |
|  | p99 |
|  | p95 |
|  | p90 |
|  | p85 |
|  | p75 |
|  | p50 |
|  | p10 |
| OSのメトリクス | Running | インスタンスが起動してから経過した時間。 |
|  | Load 1 | 直前の 1 分間と 5 分間の平均負荷。この期間に実行されていたプロセスの平均数を小数値で示す。表示された数が使用可能な vCPU（スレッド）の数よりも多い場合、余りは待機中だったプロセスの平均数。  たとえば、インスタンスタイプが 4 vCPU であり、負荷が 4.5 である場合、その期間において、平均で .5 のプロセスが待機していたことになり、その期間の 50% にわたって 1 つのプロセスが待機していたことを意味する。 |
|  | Load 5 |
|  | User % | 過去 10 秒間に CPU が各状態で費やした時間のパーセンテージ。 |
|  | Nice % |
|  | System % |
|  | Idle % |
|  | I/O Wait % |

#### Elastic Load Balancing

|  |  |  |
| --- | --- | --- |
| 種別 | メトリクス | 内容 |
| ロードバランサーのメトリクス | ActiveConnectionCount | クライアントからロードバランサーへ、およびロードバランサーからターゲットへの、アクティブな同時 TCP 接続の総数。 |
|  | ClientTLSNegotiationErrorCount | クライアントにより開始され、TLS エラーのためにロードバランサーとのセッションを確立しなかった、TLS 接続の数。考えられる原因としては、暗号やプロトコルの不一致、クライアントがサーバー証明書を検証できないため接続を閉じるなどがある。 |
|  | ConsumedLCUs | ロードバランサーが使用するロードバランサーキャパシティーユニット (LCU) の数。1 時間当たりで使用する LCU 数の料金がかかる。 |
|  | DesyncMitigationMode\_NonCompliant\_Request\_Count | RFC 7230 に準拠していないリクエストの数。 |
|  | DroppedInvalidHeaderRequestCount | リクエストをルーティングする前に、ロードバランサーが無効なヘッダーフィールドを持つ HTTP ヘッダーを削除したリクエストの数。ロードバランサーは、routing.http.drop\_invalid\_header\_fields.enabled 属性が true に設定されている場合にのみこれらのヘッダーを削除する。 |
|  | ForwardedInvalidHeaderRequestCount | 無効なヘッダーフィールドを持つ HTTP ヘッダーがあるロードバランサーによってルーティングされたリクエストの数。ロードバランサーは、routing.http.drop\_invalid\_header\_fields.enabled 属性が false に設定されている場合にのみ、これらのヘッダーを使用してリクエストを転送する。 |
|  | GrpcRequestCount | IPv4 および IPv6 経由で処理された gRPC リクエストの数。 |
|  | HTTP\_Fixed\_Response\_Count | 成功した固定レスポンスアクションの数。 |
|  | HTTP\_Redirect\_Count | 成功したリダイレクトアクションの数。 |
|  | HTTP\_Redirect\_Url\_Limit\_Exceeded\_Count | レスポンスの Location ヘッダーの URL が 8K を超えているために、リダイレクトアクションを完了できなかった数。 |
|  | HTTPCode\_ELB\_3XX\_Count | ロードバランサーから送信された HTTP 3XX リダイレクトコードの数。この数には、ターゲットによって生成される応答コードは含まれない。 |
|  | HTTPCode\_ELB\_4XX\_Count | ロードバランサーから送信される HTTP 4XX クライアントエラーコードの数。この数には、ターゲットによって生成される応答コードは含まれない。  リクエストの形式が不正な場合、または不完全な場合は、クライアントエラーが生成される。ロードバランサーが HTTP 460 エラーコードを返す場合を除き、これらのリクエストはターゲットで受信されない。この数には、ターゲットによって生成される応答コードは含まれない。 |
|  | HTTPCode\_ELB\_5XX\_Count | ロードバランサーから送信される HTTP 5XX サーバーエラーコードの数。この数には、ターゲットによって生成される応答コードは含まれない。 |
|  | HTTPCode\_ELB\_500\_Count | ロードバランサーから送信される HTTP 500 エラーコードの数。 |
|  | HTTPCode\_ELB\_502\_Count | ロードバランサーから送信される HTTP 502 エラーコードの数。 |
|  | HTTPCode\_ELB\_503\_Count | ロードバランサーから送信される HTTP 503 エラーコードの数。 |
|  | HTTPCode\_ELB\_504\_Count | ロードバランサーから送信される HTTP 504 エラーコードの数。 |
|  | IPv6ProcessedBytes | IPv6 を使用したロードバランサーによって処理される総バイト数。この数は ProcessedBytes に含まれている。 |
|  | IPv6RequestCount | ロードバランサーによって受信された IPv6 リクエストの数。 |
|  | NewConnectionCount | クライアントからロードバランサーへ、およびロードバランサーからターゲットへの、新たに確立された TCP 接続の総数。 |
|  | NonStickyRequestCount | 既存のスティッキーセッションを使用できなかったために、ロードバランサーが新しいターゲットを選択したリクエストの数。たとえば、リクエストが新しいクライアントから最初のリクエストで、維持 Cookie が提示されなかった、維持 Cookie が提示されたが、このターゲットグループに登録されたターゲットを指定しなかった、維持 Cookie の形式が誤っているか期限切れであった、内部エラーによりロードバランサーは維持 Cookie を読み取れなかったなど。 |
|  | ProcessedBytes | IPv4 および IPv6 を使用したロードバランサーによって処理される総バイト数。この数には、クライアントとの間および Lambda 関数との間で送受信されるトラフィックに加えて、ユーザー認証が有効な場合は ID プロバイダー (IdP) からのトラフィックが含まれる。 |
|  | RejectedConnectionCount | ロードバランサーが接続の最大数に達したため、拒否された接続の数。 |
|  | RequestCount | IPv4 および IPv6 経由で正常に処理されたリクエストの数。このメトリクスは、ロードバランサーノードがターゲットを選択できたリクエストに対してのみ増分される。ターゲットが選択される前に拒否された要求 (HTTP460、HTTP400、HTTP503 および 500 など) は、このメトリクスには反映されない。 |
|  | RuleEvaluations | 1 時間の平均リクエスト頻度に基づいてロードバランサーによって処理されるルールの数。 |
| ターゲットのメトリクス | HealthyHostCount | 正常と見なされるターゲットの数。 |
|  | HTTPCode\_Target\_2XX\_Count | ターゲットによって生成された HTTP 応答コードの数。これには、ロードバランサーによって生成される応答コードは含まれない。 |
|  | HTTPCode\_Target\_3XX\_Count |
|  | HTTPCode\_Target\_4XX\_Count |
|  | HTTPCode\_Target\_5XX\_Count |
|  | RequestCountPerTarget | ターゲットグループ内の各ターゲットによって受信されたリクエストの平均数。TargetGroup ディメンションを使用してターゲットグループを指定する必要がある。ターゲットが Lambda 関数である場合、このメトリクスは適用されない。 |
|  | TargetConnectionErrorCount | ロードバランサーとターゲット間で正常に確立されなかった接続数。ターゲットが Lambda 関数である場合、このメトリクスは適用されない。 |
|  | TargetResponseTime | リクエストがロードバランサーから送信され、ターゲットからの応答を受信するまでの経過時間 (秒)。これは、アクセスログの target\_processing\_time フィールドに相当する。 |
|  | TargetTLSNegotiationErrorCount | ロードバランサーにより開始され、ターゲットとのセッションを確立しなかった、TLS 接続の数。暗号化またはプロトコルの不一致が原因である場合がある。ターゲットが Lambda 関数である場合、このメトリクスは適用されない。 |
|  | UnHealthyHostCount | 異常と見なされるターゲットの数。 |

#### 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。 |

#### NAT Gateway

|  |  |
| --- | --- |
| メトリクス | 内容 |
| ActiveConnectionCount | NAT ゲートウェイ経由の同時アクティブ TCP 接続の合計数。 |
| BytesInFromDestination | NAT ゲートウェイによって受信された送信先からのバイト数。  BytesOutToSource の値が BytesInFromDestination の値より少ない場合、NAT ゲートウェイの処理中、またはトラフィックが NAT ゲートウェイによりアクティブにブロックされている間に、データ損失が発生する可能性がある。 |
| BytesInFromSource | VPC 内のクライアントから NAT ゲートウェイによって受信されたバイト数。  BytesOutToDestination の値が BytesInFromSource の値よりも小さい場合、NAT ゲートウェイの処理中にデータ損失が発生する可能性がある。 |
| BytesOutToDestination | NAT ゲートウェイ経由で送信先に送信されたバイト数。  値が 0 より大きい場合は、NAT ゲートウェイの背後にあるクライアントからインターネットへのトラフィックがあることを示す。BytesOutToDestination の値が BytesInFromSource の値よりも小さい場合、NAT ゲートウェイの処理中にデータ損失が発生する可能性がある。 |
| BytesOutToSource | VPC 内の NAT ゲートウェイ経由でクライアントに送信されたバイト数。  値が 0 より大きい場合は、インターネットから NAT ゲートウェイの背後にあるクライアントへのトラフィックがあることを示す。BytesOutToSource の値が BytesInFromDestination の値より少ない場合、NAT ゲートウェイの処理中、またはトラフィックが NAT ゲートウェイによりアクティブにブロックされている間に、データ損失が発生する可能性がある。 |
| ConnectionAttemptCount | NAT ゲートウェイ経由で行われた接続試行の回数。  ConnectionEstablishedCount の値が ConnectionAttemptCount の値よりも小さい場合は、NAT ゲートウェイの背後にあるクライアントが応答のない新しい接続を確立しようとしたことを示す。 |
| ConnectionEstablishedCount | NAT ゲートウェイ経由で確立された接続の数。  ConnectionEstablishedCount の値が ConnectionAttemptCount の値よりも小さい場合は、NAT ゲートウェイの背後にあるクライアントが応答のない新しい接続を確立しようとしたことを示す。 |
| ErrorPortAllocation | NAT ゲートウェイが送信元ポートを割り当てられなかった回数。  値が 0 より大きい場合は、NAT ゲートウェイ経由の同時接続数が多すぎることを示す。 |
| IdleTimeoutCount | アクティブな状態からアイドル状態に移行した接続の数。適切に閉じられなかった場合や、直前の 350 秒間にアクティビティがなかった場合、アクティブな接続はアイドル状態に移行する。  値が 0 より大きい場合は、アイドル状態に移行した接続があることを示す。IdleTimeoutCount の値が増加する場合は、NAT ゲートウェイの背後にあるクライアントが無効な接続を再使用している可能性がある。 |
| PacketsDropCount | NAT ゲートウェイによって破棄されたパケットの数。  値が 0 より大きい場合は、NAT ゲートウェイで進行中の一時的な問題を示している可能性がある。 |
| PacketsInFromDestination | NAT ゲートウェイによって受信された送信先からのパケット数。  PacketsOutToSource の値が PacketsInFromDestination の値より少ない場合、NAT ゲートウェイの処理中、またはトラフィックが NAT ゲートウェイによりアクティブにブロックされている間に、データ損失が発生する可能性がある。 |
| PacketsInFromSource | VPC 内のクライアントから NAT ゲートウェイによって受信されたパケット数。  PacketsOutToDestination の値が PacketsInFromSource の値よりも小さい場合、NAT ゲートウェイの処理中にデータ損失が発生する可能性がある。 |
| PacketsOutToDestination | NAT ゲートウェイ経由で送信先に送信されたパケット数。  値が 0 より大きい場合は、NAT ゲートウェイの背後にあるクライアントからインターネットへのトラフィックがあることを示す。PacketsOutToDestination の値が PacketsInFromSource の値よりも小さい場合、NAT ゲートウェイの処理中にデータ損失が発生する可能性がある。 |
| PacketsOutToSource | VPC 内の NAT ゲートウェイ経由でクライアントに送信されたパケット数。  値が 0 より大きい場合は、インターネットから NAT ゲートウェイの背後にあるクライアントへのトラフィックがあることを示す。PacketsOutToSource の値が PacketsInFromDestination の値より少ない場合、NAT ゲートウェイの処理中、またはトラフィックが NAT ゲートウェイによりアクティブにブロックされている間に、データ損失が発生する可能性がある。 |

#### 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。

本番環境でしきい値を超過した場合はアラートによる通知を行う。

検証環境についてはアラート通知を行わない。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サーバー | リソース | しきい値 | しきい値超過時の処理 | メトリクス |
| WebAPサーバー | CPU使用率 | 80%以上が15分、3回連続 | メールによるアラート通知 | CPUUtilization |
|  | メモリ使用率 | 80%以上が5分、3回連続 | アラートの通知先は5.8アラート通知先を参照する。 | FreeableMemory |
| DBサーバー | 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 |
| バッチサーバー | 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 |

## 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 |
| WebAPサーバー  (Elastic Beanstlak / EC2) | ・OSログ  ・Apacheログ  (ssl\_access\_log / access\_log / error\_log) | 本番環境：/aws/elasticbeanstalk/aeras-corporate-site-system/prod/webaplog  検証環境：/aws/ec2/aeras-corporate-site-system/stg/webaplog | 東京 | ログ監視を実施する |
| RDS | 監査ログ | /aws/rds/instance/<インスタンス名>/audit |  |  |
|  | エラーログ | /aws/rds/instance/<インスタンス名>/error |  |  |
|  | 全般ログ | /aws/rds/instance/<インスタンス名>/general |  |  |
|  | スロークエリログ | /aws/rds/instance/<インスタンス名>/slowquery |  |  |
| バッチサーバー | ビルド出力ログ | 本番環境：  /aws/codebuild/aeras-corporate-site-system/prod/<プロジェクト名>/buildoutputlog  検証環境：  /aws/codebuild/aeras-corporate-site-system/stg/<プロジェクト名>/buildoutputlog |  |  |
| DataSync | 実行ログ | 本番環境：/aws/datasync/aeras-corporate-site-system/prod/synclog  検証環境：/aws/datasync/aeras-corporate-site-system/stg/synclog |  |  |
| Kinesis Data Firehose | S3データ配信エラー | 検証環境：/aws/kinesisfirehose/manabiplus/prod/s3error  本番環境：/aws/kinesisfirehose/manabiplus/stg/s3error | 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。 |
| 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/aeras-corporate-site-system/prod/dnsquerylog  検証環境：/aws/route53/aeras-corporate-site-system/stg/dnsquerylog |  |  |
| ACM  Auto Scaling group  AWS Backup  AWS Systems Manager  AWS WAF  CodeBuild  CodeCommit  CloudFront  CloudTrail  CloudWatch  DataSync  EC2  Elastic Beanstalk  Elastic Load Balancing  IAM  Kinesis Data Firehose  KMS  NAT Gateway  RDS  Route53  S3  SNS  VPC | 操作ログ(90日以上前のログ) | 本番環境：/aws/cloudtrail/aeras-corporate-site-system/prod/operationlog  検証環境：/aws/cloudtrail/aeras-corporate-site-system/stg/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  Auto Scaling group  AWS Backup  AWS Systems Manager  AWS WAF  CodeBuild  CodeCommit  CloudFront  CloudTrail  CloudWatch  DataSync  EC2  Elastic Beanstalk  Elastic Load Balancing  IAM  Kinesis Data Firehose  KMS  NAT Gateway  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。 |
| ELB | リクエストログ | alb/ |  |
| CloudFront | アクセスログ | 6.4.3CloudFrontを参照 |  |
| CodeBuild | ビルドログ | codebuildlog/ |  |
| S3 | アクセスログ | 2.3.3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 |
| CloudWatch Logs | 12ヶ月(365日) |
| S3 | 12ヶ月(365日) |

### ログ監視

本システムは以下についてログ監視を行う。

本番環境で監視文字列を検知した場合はアラートによる通知を行う。

検証環境についてはアラート通知を行わない。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 対象サービス | 対象ログ | 監視文字列 | 監視文字列検知時の処理 | 備考 |
| WebAPサーバー  (Elastic Beanstlak / EC2) | OSログ  Apacheログ | ERROR | メールによるアラート通知 | 以下のフィルタパターンを適用する。 |
| Error | (アラートの通知先は | ?ERROR ?Error ?error |
|  |  | error | 5.8アラート通知先を参照する。) |  |
|  |  | failed |  |  |
| バッチサーバー | ビルド出力ログ | ERROR |  | 以下のフィルタパターンを適用する。 |
|  |  | Error |  | ?ERROR ?Error ?error |
|  |  | error |  |  |
|  |  | failed |  |  |

## 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

各種サーバーのアップデート方針を示す。

|  |  |  |  |
| --- | --- | --- | --- |
| サーバー | 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 | 備考 |
| 本番環境 WebAPサーバー | 自動適用する。 | 自動適用しない。 |  |
| 検証環境 WebAPサーバー |  | 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のうえ本番環境に適用する。 | cronで実行する。 |
| WordPress |  |  |
| DBサーバー |  |  |
| バッチサーバー |  |  |
| ソース管理サーバー |  | 自動適用する。 | AWSマネージドサービスのため、AWSがソフトウェアのアップデートを実施する。 |
| ストレージ |  |  |

## アラート通知先

本システムでは以下のメールアドレスに対して各種監視のアラートを通知する。

|  |  |
| --- | --- |
| 通知先メールアドレス | 備考 |
| honbu-aeras@aeras-group.co.jp | アエラス様 |
| k-otsuki@aeras-group.co.jp |  |
|  | アイロベックス保守窓口 |
|  | サンエム保守窓口 |

# 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 |
| aeras-corporate-site-system-cfnuser | AWSCertificateManagerFullAccess | SSL証明書管理 |  |
| (CloudFormation管理ユーザー) | AWSCloudFormationFullAccess | CloudFormation管理 | 作成するスタックにowner=ユーザー名のタグを付与し、他ユーザーによるスタックの更新を拒否する。 |
|  | AWSCloudTrail\_FullAccess | CloudTrail管理 |  |
|  | AWSCodeBuildAdminAccess | バッチサーバー管理 |  |
|  | AWSCodeCommitFullAccess | ソース管理サーバー管理 |  |
|  | AWSDataSyncFullAccess | S3バケットバックアップ管理 |  |
|  | AWSKeyManagementServicePowerUser | 暗号鍵管理 |  |
|  | AWSWAFFullAccess | WAF管理 |  |
|  | AdministratorAccess-AWSElasticBeanstalk | Elastic Beanstalk管理 |  |
|  | AmazonEC2FullAccess | EC2管理 |  |
|  | AmazonKinesisFirehoseFullAccess | Kinesis Firehose管理 |  |
|  | AmazonRDSFullAccess | DBサーバー管理 |  |
|  | AmazonRoute53FullAccess | DNS管理 |  |
|  | AmazonS3FullAccess | ストレージ管理 |  |
|  | AmazonSSMFullAccess | パラメータストア管理 |  |
|  | AmazonVPCFullAccess | ネットワーク構成管理 |  |
|  | CloudFrontFullAccess | CloudFront管理 |  |
|  | CloudWatchFullAccess | CloudWatch管理 |  |
|  | CloudWatchLogsFullAccess | CloudWatch Logs管理 |  |
|  | IAMFullAccess | IAM管理 |  |
|  | ResourceGroupsandTagEditorFullAccess | リソースグループ管理 |  |
| aeras-corporate-site-system-operator | カスタムポリシー | アプリケーションストレージ管理 |  |
|  | バックアップストレージ管理 |  |
| (運用ユーザー) |  | ログストレージ管理 |  |
|  |  | CloudTrailログストレージ管理 |  |
|  |  | データストレージ管理 |  |
|  |  | CloudTrailログ表示 |  |
|  |  | CloudWatchメトリクス表示 |  |
|  |  | CloudWatch Logs表示 |  |
|  |  | データストレージバックアップ |  |
| aeras-corporate-site-system-developer | AWSCodeBuildAdminAccess | バッチサーバー管理 |  |
| (アプリケーション開発ユーザー) | AWSCodeCommitFullAccess | ソース管理サーバー管理 |  |
|  | カスタムポリシー | アプリケーションストレージ管理 |  |
|  |  | ログストレージ管理 |  |
|  |  | CloudWatchメトリクス表示 |  |
|  |  | CloudWatch Logs表示 |  |
|  |  | 検証環境WebAPサーバー起動停止 |  |
|  |  | 検証環境DBサーバー起動停止 |  |

## 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 |
| EC2 | CloudWatchLogs書き込み権限 |  |
| (WebAPサーバー) | RDS接続 |  |
| 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。

### WebAPサーバー

#### 本番環境WebAPサーバー(Elastic Beanstalk)

#### 検証環境WebAPサーバー(EC2)

|  |  |  |  |
| --- | --- | --- | --- |
| ボリュームタイプ | 暗号化 | 暗号化手法 | 備考 |
| ルート | 有効 | aws/ebs | 機密データが含まれるため暗号化する。 |

### 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 | 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。 |
| 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 |  |  |  |

### バッチサーバー(CodeBuild)

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

### ソース管理サーバー(CodeCommit)

|  |  |
| --- | --- |
| 暗号化 | 備考 |
| 有効 | 保存中に自動的に暗号化される。 |

### バックアップデータ

|  |  |  |
| --- | --- | --- |
| 対象 | 暗号化 | 備考 |
| WebAPサーバー | 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：aeras-group.jp  検証環境：stg-aeras-group.com |

ACMサービスにより発行したSSL証明書の特性を記載する。

|  |  |
| --- | --- |
| 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

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 | ○(8) | 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 | ○(7) | 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 | ○(6)  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 | ×  本番環境ではPaaS (Elastic Beanstalk)を利用するため適用しない | 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 | ○(5)  PHPを使用するため適用する | 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 | ○(4)  WordPressを使用するため適用する | 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。 |

### CloudFront

CDN(コンテンツデリバリーネットワーク)としてCloudFrontを利用することにより、キャッシュ機能によるオリジンサーバー（CloudFront がコンテンツを取得する元のウェブサーバー）の負荷軽減とコンテンツ配信のパフォーマンス向上を実現する。また、CloudFront はAWS Shield によるDDoS 保護機能が有効化されており、ネットワーク層およびトランスポート層のDDoS 攻撃に対する緩和が自動的に行われる。

本システムではWordPressサーバー向けのCloudFrontディストリビューションを作成し、CloudFrontディストリビューションを経由したリクエストのみno

Webアクセスを許可する。

各ディストリビューションへはACMで管理するACM証明書、及びAWS WAFで作成したWebACLを設定する。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | 設定値 | |  |  |
| 項目 | | | 本番環境 | | 検証環境 | 備考 |
| ディストリビューション設定 | | |  | | |  |
|  | 価格クラス | | 全てのエッジロケーション | | | CloudFront サービスに支払う上限価格に対応する価格クラスを選択する。 |
|  | AWS WAF ウェブACL | | AWS WAFで作成したWebACL | | | AWS WAF を使用して、指定した条件に基づいてリクエストを許可したりブロックしたりする場合は、このディストリビューションに関連付けられたウェブ ACL を選択する。 |
|  | 代替ドメイン名 (CNAME) | | (ドメイン名) | | | ディストリビューションを作成するときに CloudFront が割り当てるドメイン名ではなく、オブジェクトの URL に使用する 1 つ以上のドメイン名を指定する。 |
|  | SSL証明書 | | ACMで作成したSSL証明書 | | | ディストリビューションで使用する代替ドメイン名を指定した場合は、[Custom SSL Certificate (カスタム SSL 証明書)] を選択してこの代替ドメイン名を使用する許可を検証し、これを対象とする証明書選択する。 |
|  | セキュリティポリシー | | TLSv1.2\_2021 (recommended) | | | CloudFront がビューワー (クライアント) との HTTPS 接続に使用するセキュリティポリシーを指定する。 |
|  | サポートされる HTTP バージョン | | HTTP/2 | | | ビューワーが CloudFront と通信するときにディストリビューションでサポートする HTTP バージョンを選択する。 |
|  | デフォルトのルートオブジェクト | | (空白) | | | ビューワーがディストリビューション内のオブジェクト (http://www.example.com/product-description.html) ではなくディストリビューションのルート URL (http://www.example.com/) をリクエストするときに、CloudFront がリクエストする、オリジンからのオブジェクト (index.html など)。 |
|  | ログ記録 | | 有効 | | | CloudFront がオブジェクトに対する各リクエストの情報をログに記録し、ログファイルを Amazon S3 バケットに保存する。 |
|  | ログ用のバケット | | S3(ログストレージ) | | | ログ記録を有効にした場合にCloudFront がアクセスログを保存する Amazon S3 バケット |
|  | ログのプレフィックス | | cf-webap/ | | | ログ記録を有効した場合にこのディストリビューションのアクセスログファイル名の先頭に CloudFront が追加する文字列 (ある場合) を指定する。 (例: exampleprefix/)。末尾のスラッシュ (/) はオプションだが、ログファイルの参照を容易にするためにこれを使用することが推奨される。 |
|  | Cookie のログ作成 | | 無効 | | | CloudFront で Cookie をアクセスログに含めるようにするには、有効を選択する。Amazon S3 は Cookie を処理しないため、S3がオリジンである場合は無効にする。 |
|  | IPv6 を有効にする | | 有効 | | | 一般的に、IPv6 ネットワークのユーザーがいてコンテンツにアクセスする場合は、IPv6 を有効にする必要がある。ただし、コンテンツへのアクセスを制限するために署名付き URL または署名付き Cookie を使用していて、コンテンツへのアクセスが可能な IP アドレスを制限する IP アドレスを含む IpAddress パラメータを使用している場合、IPv6 は有効にしない。 |
| オリジンの設定 | | |  | | |  |
|  | オリジンドメイン名 | |  | WebAPサーバー  プライベート IPv4 DNS | | CloudFront がこのオリジンのオブジェクトの取得先としている Amazon S3 バケットまたは HTTP サーバーの DNS ドメイン名。 |
|  |  | プロトコル |  | HTTP only | | CloudFront がオリジンに接続するときに使用するプロトコル (HTTP または HTTPS) |
|  |  | ポート番号 |  | 80 | | CloudFront がオリジンに接続するときに使用するポート番号 |
|  |  | SSLプロトコル |  | TLS v1 | | CloudFront がオリジンへの HTTPS 接続を確立するときに使用する最小 SSL/TLS プロトコル |
|  | オリジンのパス | | (空白) | | | CloudFront で AWS リソースまたはカスタムオリジンのディレクトリにコンテンツがリクエストされるようにするには、スラッシュ (/) から始まるディレクトリパスを入力する。 |
|  | オリジンカスタムヘッダー | |  | X-Cf-Secret-Key: T@\/\_Bf1iS^Q9ubaga\*@5K7$ | | リクエストをオリジンに転送するときに CloudFront が常にカスタムヘッダーを追加するようにする。  CloudFront経由のみWebアクセスを許可する。 |
|  | オリジンシールド | | 無効 | | | オリジンの前に追加されるキャッシュレイヤー。「異なる地理的リージョンにビューワーが分散している場合」のユースケースに該当しないため無効にする。 |
|  | オリジンへの接続試行回数 | | 3 | | | CloudFront がオリジンへの接続を試行する回数。 |
|  | オリジンへの接続タイムアウト | | 10 | | | オリジンへの接続を確立しようとするときに CloudFront が待機する秒数。 |
| オリジンの設定 | | |  | | |  |
|  | オリジンドメイン名 | | データストレージ(S3) | | | CloudFront がこのオリジンのオブジェクトの取得先としている Amazon S3 バケットまたは HTTP サーバーの DNS ドメイン名。 |
|  | オリジンのパス | | (空白) | | | CloudFront で AWS リソースまたはカスタムオリジンのディレクトリにコンテンツがリクエストされるようにするには、スラッシュ (/) から始まるディレクトリパスを入力する。 |
|  | S3バケットアクセス | | origin access identity (OAI)を使用する | | | OAIを使用してS3バケットへのアクセスをCloudFrontからのみに制限する。 |
|  | オリジンカスタムヘッダー | | (空白) | | | リクエストをオリジンに転送するときに CloudFront が常にカスタムヘッダーを追加するようにする。 |
|  | オリジンシールド | | 無効 | | | オリジンの前に追加されるキャッシュレイヤー。「異なる地理的リージョンにビューワーが分散している場合」のユースケースに該当しないため無効にする。 |
|  | オリジンへの接続試行回数 | | 3 | | | CloudFront がオリジンへの接続を試行する回数。 |
|  | オリジンへの接続タイムアウト | | 10 | | | オリジンへの接続を確立しようとするときに CloudFront が待機する秒数。 |
| キャッシュ動作の設定 0 | | |  | | |  |
|  | パスパターン | | /wp-content/uploads/\* | | | パスパターン (例: images/\*.jpg) を使用して、このキャッシュ動作をどのリクエストに割り当てるかを指定する。 |
|  | 自動圧縮 | | 有効 | | | CloudFront は、ビューワーリクエストの Accept-Encoding ヘッダーで指定されたとおり、ビューアがサポートする場合にのみファイルを圧縮する。 |
|  | ビューワープロトコルポリシー | | Redirect HTTP to HTTPS | | | CloudFront エッジロケーションのコンテンツへのアクセスに使用するビューワーのプロトコルポリシーを選択する。 |
|  | 許可される HTTP メソッド | | GET, HEAD | | | CloudFront が処理してオリジンに転送する HTTP メソッドを指定する。 |
|  | ビューワーのアクセス制限 (署名付き URL の使用) | | 無効 | | | このキャッシュ動作の PathPattern に一致するオブジェクトのリクエストで署名付き URL を使用する場合、[Yes (はい)] を選択する。 |
|  | キャッシュされる HTTP メソッド | | GET, HEAD | | | ビューワーから OPTIONS リクエストが送信されたときに、オリジンからの応答を CloudFront でキャッシュするかどうかを指定する。 |
|  | キャッシュポリシー | | CachingOptimized  (Recommended for S3 origins) | | | CloudFront がコンテンツをキャッシュする方法を管理する。オリジンで再検証する前にオブジェクトをキャッシュする時間の設定（TTL）、CloudFront が HTTP ヘッダー、クエリ文字列パラメータおよび Cookie のパラメータによって変わるコンテンツをキャッシュする方法、および CloudFront が圧縮されたコンテンツをキャッシュする方法を制御する |
|  | オリジンリクエストポリシー | | (空白) | | | オリジンへのリクエストが行われたとき（キャッシュミスまたは再検証）に CloudFront がリクエストタイムメタデータをオリジンに送信する方法を管理する、CloudFront がオリジンに送信するヘッダー、クエリ文字列パラメータ、Cookie を設定できる。 |
|  | スムーズストリーミング | | 無効 | | | Microsoft Smooth Streaming 形式のメディアファイルを配信するが、IIS サーバーがない場合は、[Yes (はい)] を選択する。 |
|  | フィールドレベル暗号化の設定 | | (空白) | | | 特定のデータフィールドにフィールドレベル暗号化を適用する場合は、フィールドレベル暗号化の設定を選択する。 |
|  | リアルタイムログ | | 無効 | | | ディストリビューションに対するリクエストの情報をリアルタイムで取得する |
| キャッシュ動作の設定 1 | | |  | | |  |
|  | パスパターン | | デフォルト | | | パスパターン (例: images/\*.jpg) を使用して、このキャッシュ動作をどのリクエストに割り当てるかを指定する。 |
|  | 自動圧縮 | | 無効 | | | CloudFront は、ビューワーリクエストの Accept-Encoding ヘッダーで指定されたとおり、ビューアがサポートする場合にのみファイルを圧縮する。 |
|  | ビューワープロトコルポリシー | | Redirect HTTP to HTTPS | | | CloudFront エッジロケーションのコンテンツへのアクセスに使用するビューワーのプロトコルポリシーを選択する。 |
|  | 許可される HTTP メソッド | | GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE | | | CloudFront が処理してオリジンに転送する HTTP メソッドを指定する。 |
|  | ビューワーのアクセス制限 (署名付き URL の使用) | | 無効 | | | このキャッシュ動作の PathPattern に一致するオブジェクトのリクエストで署名付き URL を使用する場合、[Yes (はい)] を選択する。 |
|  | キャッシュされる HTTP メソッド | | GET, HEAD | | | オリジンからの応答を CloudFront でキャッシュするかどうかを指定する。 |
|  | レガシーキャッシュ設定 | | HTTPヘッダー：All  クエリ文字列パラメータ：All  Cookieのパラメータ：All | | | CloudFront がコンテンツをキャッシュする方法を管理する。HTTP ヘッダー、クエリ文字列パラメータおよび Cookie のパラメータ別にCloudFrontがオリジンに転送する種別を制御する。 |
|  | スムーズストリーミング | | 無効 | | | Microsoft Smooth Streaming 形式のメディアファイルを配信するが、IIS サーバーがない場合は、[Yes (はい)] を選択する。 |
|  | フィールドレベル暗号化の設定 | | (空白) | | | 特定のデータフィールドにフィールドレベル暗号化を適用する場合は、フィールドレベル暗号化の設定を選択する。 |
|  | リアルタイムログ | | 無効 | | | ディストリビューションに対するリクエストの情報をリアルタイムで取得する |