更新履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版 | 更新日 | 更新項目 | 更新者 | 備考 |
| (会社名/氏名) |
| 1.0 | 2021/09/30 | 新規作成 | サン・エム・システム  若林 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目次

[1 はじめに 6](#_Toc81598483)

[2 システム構成 7](#_Toc81598484)

[2.1 システム構成図 7](#_Toc81598485)

[2.2 サービス構成 8](#_Toc81598486)

[2.2.1 サービス一覧 8](#_Toc81598487)

[2.2.2 サブスクリプション 9](#_Toc81598488)

[2.2.3 デプロイモデル 10](#_Toc81598489)

[2.2.4 リソースグループ 10](#_Toc81598490)

[2.2.5 リージョン 10](#_Toc81598491)

[2.2.6 サービス管理方式 11](#_Toc81598492)

[2.3 サーバー構成 12](#_Toc81598493)

[2.3.1 APサーバー(Azure Functions) 12](#_Toc81598494)

[2.3.2 DBサーバー(Azure SQL Database) 13](#_Toc81598495)

[2.3.3 ストレージ 17](#_Toc81598496)

[2.4 ソフトウェア構成 22](#_Toc81598497)

[2.5 ネットワーク構成 22](#_Toc81598498)

[2.5.1 VNet(仮想ネットワーク) 22](#_Toc81598499)

[2.5.2 サブネット 23](#_Toc81598500)

[2.5.3 ネットワークセキュリティグループ(NSG) 23](#_Toc81598501)

[2.5.4 ルートテーブル 25](#_Toc81598502)

[2.5.5 名前解決 27](#_Toc81598503)

[3 可用性 28](#_Toc81598504)

[3.1 耐障害性 28](#_Toc81598505)

[3.2 災害対策 28](#_Toc81598506)

[4 拡張性 29](#_Toc81598507)

[4.1 拡張性設計 29](#_Toc81598508)

[5 保守性 30](#_Toc81598509)

[5.1 Application Insights 30](#_Toc81598510)

[5.2 バックアップ・リストア 30](#_Toc81598511)

[5.2.1 バックアップ 30](#_Toc81598512)

[5.2.2 リストア 30](#_Toc81598513)

[5.3 ジョブ管理 30](#_Toc81598514)

[5.3.1 ジョブ一覧 31](#_Toc81598515)

[5.3.2 ジョブ監視 31](#_Toc81598516)

[5.4 URL監視 31](#_Toc81598517)

[5.5 リソース監視 31](#_Toc81598518)

[5.5.1 リソース監視方式 32](#_Toc81598519)

[5.5.2 CloudWatchメトリクス保存期間 32](#_Toc81598520)

[5.5.3 リソース監視状況確認方法 32](#_Toc81598521)

[5.5.4 リソース監視項目 32](#_Toc81598522)

[5.5.5 しきい値監視 60](#_Toc81598523)

[5.6 ログ管理 60](#_Toc81598524)

[5.6.1 ログ一覧 60](#_Toc81598525)

[5.6.2 ログ保存期間 63](#_Toc81598526)

[5.6.3 ログ監視 64](#_Toc81598527)

[5.7 時刻同期 64](#_Toc81598528)

[5.8 ソフトウェアのアップデート 65](#_Toc81598529)

[5.9 アラート通知先 65](#_Toc81598530)

[6 セキュリティ 66](#_Toc81598531)

[6.1 ユーザー管理 66](#_Toc81598532)

[6.2 ロール管理 67](#_Toc81598533)

[6.3 暗号化方針 67](#_Toc81598534)

[6.3.1 WebAPサーバー 67](#_Toc81598535)

[6.3.2 DBサーバー(RDS) 67](#_Toc81598536)

[6.3.3 ストレージ(S3) 67](#_Toc81598537)

[6.3.4 バッチサーバー(CodeBuild) 68](#_Toc81598538)

[6.3.5 ソース管理サーバー(CodeCommit) 68](#_Toc81598539)

[6.3.6 バックアップデータ 68](#_Toc81598540)

[6.4 Webアクセス 69](#_Toc81598541)

[6.4.1 API Management 69](#_Toc81598542)

[6.4.1 Front Door 71](#_Toc81598543)

[6.4.2 Azure Web Application Firewall 76](#_Toc81598544)

# はじめに

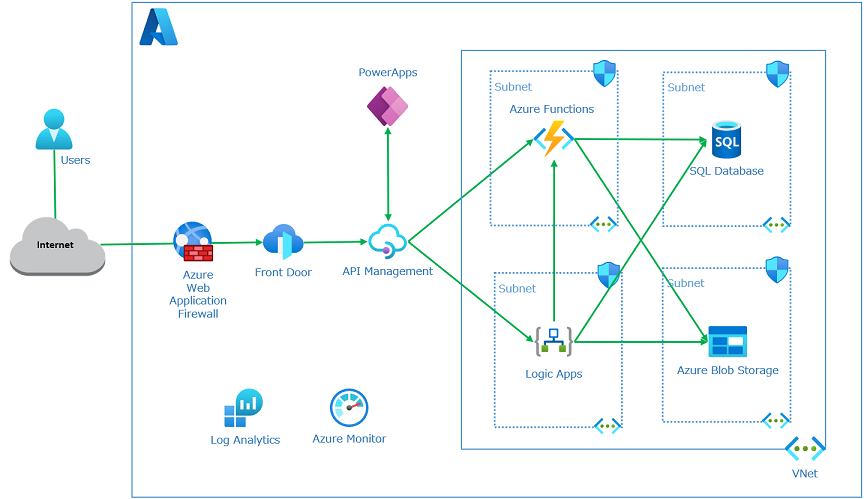
本書はLMS準備システム インフラ環境(以下、本システム)の構成、機能の実現方法、及び運用方式について記載する。

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Microsoft Azure (以下、Azure)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。

|  |  |  |
| --- | --- | --- |
| サービス | システム構成  図内アイコン | 概要 |
| API Management |  | API を保護、発行、分析するためのスケーラブルなマルチクラウド API 管理プラットフォームを提供する。 |
| Azure Blob Storage |  | モバイル、Web、クラウドネイティブ アプリケーション開発者のスケーリング、セキュリティ、可用性のニーズに対応できるストレージ。 |
| Azure Functions |  | 記述するコードと管理するインフラストラクチャを減らし、コストを節約できるサーバーレス ソリューション。 クラウドインフラストラクチャによって、アプリケーションの実行を維持するために必要な最新のリソースがすべて提供されるので、サーバーのデプロイや管理について心配する必要はない。 |
| Azure Monitor |  | クラウドおよびオンプレミス環境のテレメトリを収集、分析し、対応する包括的なソリューションを提供する。 この情報を頼りにアプリケーションの実行状態を把握し、アプリケーションやその依存リソースに影響を及ぼす問題を事前に突き止めることができる。 |
| Azure Web Application Firewall |  | 悪意のある攻撃や一般的な Web 脆弱性 (SQL インジェクション、クロスサイト スクリプティングなど) から Web アプリを保護する。 |
| Front Door |  | Microsoft グローバル エッジ ネットワークを使用して、セキュリティで保護された高速でスケーラビリティの高い Web アプリを作成するためのスケーラブルなグローバル エントリ ポイント。 |
| Log Analytics |  | Azure Monitor ログによって収集されたデータからログ クエリを編集して実行し、その結果を対話形式で分析する Azure portal のツール。 |
| Logic Apps |  | アプリ、データ、サービス、およびシステムを統合する自動化された "ワークフロー" を作成および実行するためのクラウドベースのプラットフォーム。 |
| PowerApps |  | デバイス用のアプリをすばやく構築するためのローコード アプローチが提供され、加えて高度なプロ開発者向け拡張モデルにより Azure ベースのサービスとのシームレスな連携を実現する。 |
| SQL Database |  | クラウド向けに構築されたインテリジェントでスケーラブルなリレーショナル データベース サービス。常に最新の状態に保たれた自動 AI を利用した機能で、パフォーマンスと耐久性を最適化できる。 |
| VNet |  | Azure 内のプライベート ネットワークの基本的な構成要素。 VNet により、Azure Virtual Machines (VM) などのさまざまな種類の Azure リソースが、他の Azure リソース、インターネット、およびオンプレミスのネットワークと安全に通信することができる。 |

### サブスクリプション

サブスクリプションはAzureリソースの論理コンテナーである。

各Azure リソースは、1 つのサブスクリプションだけに関連付けられる。

本システムでは以下のサブスクリプションを使用する。

|  |  |
| --- | --- |
| 項目 | 設定値 |
| サブスクリプション | 確認後記載 |
| Azureプラン | 確認後記載 |

Azureサブスクリプションは以下の目的で使用される。

|  |  |
| --- | --- |
| 目的 | 概要 |
| 法的契約 | 各サブスクリプションは、無料試用版や従量課金制などの Azure プランに関連付けられる。 各プランには固有の料金プラン、特典、使用条件が設定されている。 Azure プランはサブスクリプションを作成するときに選択する。 |
| 支払い契約 | サブスクリプションを作成するときに、そのサブスクリプションの支払い情報 (クレジット カード番号など) を指定する。 そのサブスクリプションにデプロイされたリソースにかかる費用が毎月計算され、指定した支払い方法で請求される。 |
| スケールの境界 | サブスクリプションに対してスケール制限が定義される。 サブスクリプションのリソースは、設定されたスケール制限を超えることはできない。 たとえば、1 つのサブスクリプションで作成できる仮想マシンの数には制限がある。 |
| 管理上の境界 | サブスクリプションは、管理、セキュリティ、ポリシーの境界として機能する。 Azure では、これらのニーズに対応するその他のメカニズムも提供している (管理グループ、リソース グループ、Azure ロールベースのアクセス制御など)。 |

### デプロイモデル

Azureソリューションのデプロイと管理における2種類の異なる方法として、Resource Managerデプロイモデルとクラシックデプロイモデルがある。

これら2つのモデルに互換性はない。リソースのデプロイと管理を簡単にするために、すべてのリソースにResource Managerを利用することが推奨されている。

本システムでは推奨に則り、Resource Managerデプロイモデルを採用する。

|  |  |
| --- | --- |
| 項目 | 設定値 |
| デプロイモデル | Resource Managerデプロイモデル |

### リソースグループ

サブスクリプション内の関連するリソースをグループ化する論理コンテナー。 各リソースが所属できるリソース グループは 1 つに限られる。 リソース グループは、サブスクリプション内でのより詳細なグループ化を可能にする。また、一般に、サブスクリプション内のワークロード、アプリケーション、または特定の機能をサポートするために必要なリソースのコレクションを表すために使用される。

|  |  |
| --- | --- |
| 項目 | 設定値 |
| リソースグループ |  |

### リージョン

リージョンは待ち時間で定義された境界内にデプロイされる Azure データセンターのセットである。

データセンターは、リージョンの待ち時間の短い専用ネットワーク経由で接続される。

多くのAzure リソースは特定の Azure リージョンで実行される。

本システムの利用者の待ち時間を最小化するために利用者の所在地に近いリージョンを選択する。

|  |  |
| --- | --- |
| 項目 | 設定値 |
| リージョン | 東日本 |

### サービス管理方式

Azure Resource Manager は、Azure リソースのデプロイや管理を行うサービスである。Azureアカウント内のリソースを作成、更新、および削除できる管理レイヤーを提供する。本システムでは以下に記載するメリットを得るために、すべてのサービスをAzure Resource Managerで管理する。

|  |
| --- |
| メリット |
| スクリプトではなく宣言型のテンプレートを使用してインフラストラクチャを管理する。 |
| ソリューションのリソースを個別に処理するのではなく、すべてのリソースをグループとしてデプロイ、管理、監視する。 |
| ソリューションを開発のライフサイクル全体で再デプロイする。リソースは、必ず一貫した状態でデプロイされる。 |
| 正しい順序でデプロイされるように、リソース間の依存関係を定義することができる。 |
| Azure ロールベースのアクセス制御 (Azure RBAC) が管理プラットフォームにネイティブ統合されるため、すべてのサービスにアクセス制御を適用できる。 |
| タグをリソースに適用し、サブスクリプションのすべてのリソースを論理的に整理する。 |
| 同じタグを共有するリソース グループのコストを表示することで、組織の課金を分かりやすくする。 |

## サーバー構成

以下に本システムのサーバー構成を示す。

### APサーバー(Azure Functions)

本システムではAPサーバーとしてAzure Functionsサービスを利用する。

以下にAzure Functionsの実行環境であるFunction Appの定義を示す。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 公開 | | ストレージアカウント | OS | プランの種類 | Application Insights | VNet統合  (接続するサブネット) |
| 関数アプリ名 | ランタイムスタック | バージョン | SKUとサイズ |
| 本番環境：  prod-ymhlms-functionapp  検証環境：  stg-ymhlms-functionapp | コード | | 本番環境：  prodYmhlmsStorageaccount | Linux | Functions Standard | いいえ  (Node.jsでは有効にできない) | SQL Database用サブネット  ストレージアカウント用サブネット |
| Node.js | 14LTS | 検証環境：  stgYmhlmsStorageaccount |  | エラスティック Premium EP1 |

各種設定項目の説明を以下に示す。

|  |  |
| --- | --- |
| 設定項目 | 説明 |
| 関数アプリ名 | グローバルに一意の名前を指定する。  有効な文字は以下の通りである。  a-z (大文字と小文字の区別をしない)、0-9、および - |
| 公開 | コード、Dockerコンテナから選択する。コードが推奨される。  Docker コンテナー オプションは、関数アプリが実行される Linux 環境をより詳細に制御する必要がある場合に使用する。 |
| ランタイムスタック | 以下より、関数プログラミング言語をサポートするランタイムを選択する。  .NET / Node.js / Python / Java / PowerShell Core / Custom Handler |
| バージョン | インストールされているランタイムのバージョンをする。 |
| 地域 | ユーザーに近い地域、または関数がアクセスする他のサービスの近くのリージョンを選択する。 |
| ストレージアカウント | グローバルに一意の名前を指定する。  Function App で使用されるストレージ アカウントを作成する。 ストレージ アカウント名は、3 文字から 24 文字までの長さにし、数字と小文字のみを使用する必要がある。 |
| OS | オペレーティング システムは、ランタイム スタックの選択に基づいてあらかじめ選択されますが、必要に応じて設定を変更できる。 ポータルでの編集は Windows でのみサポートされます。 |
| プランの種類 | Function App にどのようにリソースが割り当てられるかを定義するホスティングプランを選択する。  消費量(サーバーレス)：  自動的にスケールし、関数が実行されている際のコンピューティング リソースに対してのみ課金される。Functions ホストのインスタンスは、受信イベントの数に基づいて動的に追加および削除される。  Functions Standard：  説明追記  Functions Premium：  需要に応じて自動的にスケーリングを行いながら、事前ウォーミングされたワーカーを使用して、アイドル状態になっても遅延なくアプリケーションを実行したり、より強力なインスタンスで実行したり、仮想ネットワークに接続したりすることができる。  App Serviceプラン：  App Service プラン内で、Functions を通常の App Service プラン料金で実行する。  サーバーレス コンピューティング環境でステートフル関数を記述できる Azure Functions の拡張機能である、Durable Functions を使用できない、実行時間の長いシナリオに最適。 |
| Application Insights | Azure Functionsのログ、パフォーマンス、およびエラー データを収集する。パフォーマンスの異常が自動的に検出されるほか、強力な分析ツールが特徴となっていて、より簡単に、問題を診断したり、関数がどのように使用されているかを把握することができる。 |

### DBサーバー(Azure SQL Database)

本システムではDBサーバーとしてAzure SQL Databaseサービスを利用する。

Azureは以下3種類のSQLデータベースサービスを提供しており、本システムは新規に開発するシステムであるため、Azure SQL Databaseを採用する。

|  |  |  |  |
| --- | --- | --- | --- |
| サービス | 利用形態 | 用途 | 概要 |
| Azure SQL Database | PaaS | 新規開発向け | クラウド向けに構築されたインテリジェントでスケーラブルなデータベースサービスであり、AI を利用した機能によりピーク パフォーマンスと耐久性を維持する。自動的にスケーリングするハイパースケールのストレージ リソースで、リソース管理を気にすることなくコストを最適化。サーバーレス コンピューティングも可能。 |
| Azure SQL Managed Instance | PaaS | オンプレからの移行 | 幅広い SQL Server エンジンとの互換性と、フル マネージドで最新のサービスとしてのプラットフォームのすべての利点が組み合わさった、インテリジェントでスケーラブルなクラウド データベース サービス。 |
| Azure VM 上の SQL Server | IaaS | OS機能を併用 | Azure VM上でSQL Serverを稼働。SQL Server IaaS Agent 拡張機能を使用して、Azure VM 上の SQL Server の管理固有の管理タスクを自動化することが可能。 |

以下にAzure SQL Databaseの設定値を示す。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | 本番環境 | 検証環境 | 備考 |
| データベースの詳細 | | | 論理サーバーの選択や、コンピューティング リソースとストレージ リソースの構成など、このデータベースに必要な設定を入力する。 | | |
|  | データベース名 | |  |  |  |
|  | サーバー | | 接続文字列と資格情報は、サーバーに基づいて使用される。 | | |
|  |  | サーバー名 |  |  |  |
|  |  | サーバー管理者ログイン |  |  |  |
|  |  | パスワード |  |  |  |
|  | SQL エラスティック プール | | いいえ | いいえ | エラスティック プールは、決まった予算内で複数のデータベースのパフォーマンスを管理するためのシンプルかつコスト効率の良いソリューションを提供する。 |
|  | コンピューティングとストレージ | | ワークロードのニーズに基づいて、使用可能なレベルを選択する。仮想コアモデルでは、さまざまな構成コントロールが提供され、ワークロードのニーズに基づいてデータベースを自動的にスケーリングするための Hyperscale とサーバーレス機能が提供される。また、DTU モデルでは、価格とパフォーマンス パッケージを選択して、構成を簡単に行うことができる。 | | |
|  |  | サービスレベル | 汎用目的(スケーラブルな計算とストレージのオプション) | 汎用目的(スケーラブルな計算とストレージのオプション) | 汎用目的：  予算重視のワークロード向け。  ビジネスに不可欠：  障害に対する高い回復性と高速フェールオーバーを使用する、低待機時間のワークロード向け。  Hyperscale：  拡張性の高いストレージ、読み取りスケールアウト、およびデータベースの高速復元機能を提供する。 |
|  |  | コンピューティングレベル | プロビジョニング済み | サーバーレス  検証実施時のみにサーバーを使用する。検証を実施していない間は自動でサーバーを停止する。 | プロビジョニング済み：コンピューティング リソースは事前に割り当てられる。 構成されている仮想コアに基づいて、1 時間単位で課金される。  サーバーレス：コンピューティング リソースは自動でスケーリングされる。 使用されている仮想コアに基づいて、1 秒単位で課金される。 |
|  |  | ハードウェア構成 | 第5世代 | 第5世代 | ワークロード要件に基づいてハードウェア構成を選択する。 |
|  |  | ハイブリッド特典 | いいえ | いいえ | 既に所有しているライセンスがあれば最大55%の利用費を節約できる。  サーバーレス構成の場合は利用不可。 |
|  |  | 仮想コア | 4仮想コア | 2仮想コア | 使用する仮想コア数を指定。 |
|  |  | データの最大サイズ | 検証完了後に記載 | 32 GB | データ ストレージの最大容量を指定。 |
|  |  | 冗長性 | はい | いいえ | 1 つのリージョン内の複数の可用性ゾーンにレプリカを広げ、可用性を高める。 |
|  | バックアップ ストレージの冗長性 | | ゾーン冗長バックアップ ストレージ | ローカル冗長バックアップ ストレージ | PITR と LTR のバックアップをレプリケートする方法を選択する。リージョンの障害から回復するための機能である geo リストアは、geo 冗長ストレージが選択されている場合にのみ使用できる。 |
| ネットワーク | | | サーバーのネットワーク アクセスと接続を構成する。 | | |
|  | ネットワーク接続 | | プライベート エンドポイント | プライベート エンドポイント | パブリック エンドポイントまたはプライベート エンドポイントを使用してサーバーへの接続を構成するためのオプションを選択する。 |
|  | 接続ポリシー | | デフォルト  待機時間を短縮し、スループットを向上するためにAzure内部からの接続ポリシーをリダイレクトとする。 | デフォルト  待機時間を短縮し、スループットを向上するためにAzure内部からの接続ポリシーをリダイレクトとする。 | リダイレクト (推奨): クライアントは、データベースをホストしているノードへの直接接続を確立する。これにより、待機時間が短縮され、スループットが向上する。  プロキシ：このモードでは、すべての接続が Azure SQL Database ゲートウェイ経由でプロキシ化されるため、待機時間が長くなり、スループットが低下する。  デフォルト：Azureの内部からの (たとえば、Azure 仮想マシンからの) すべてのクライアント接続の既定のポリシーは Redirect であり、外部からのすべてのクライアント接続 (たとえば、ローカル ワークステーションからの接続) の既定のポリシーは Proxy。 |
|  | 暗号化接続 TLSの最小バージョン | | TLS 1.2 | TLS 1.2 | 現在、TLS 1.0、1.1、1.2 がサポートされている。 最小 TLS バージョンを設定すると、それより新しい TLS バージョンは確実にサポートされる。アプリケーションでサポートされているかどうかをテストした後、最小 TLS バージョンを 1.2 に設定することが推奨されている。 |
| セキュリティ | | | セキュリティを構成する。 | | |
|  | Azure Defender for SQL | | 有効 | 有効 | Azure Defender により、SQL 脆弱性の評価、Advanced Threat Protection などの高度な SQL セキュリティ機能のセットが提供されます。 |
|  |  | Advanced Threat Protection  アラートの送信先 |  |  | Advanced Threat Protectionにより、データベースへのアクセスや悪用を試みる、通常とは異なる、害を及ぼす可能性がある異常なアクティビティが検出できる。 Advanced Threat Protection によって、SQL インジェクションの可能性、通常とは異なる場所またはデータ センターからのアクセス、通常とは異なるプリンシパルまたは有害な可能性があるアプリケーションからのアクセス、SQL 資格情報に対するブルート フォース攻撃 を特定できる。 |
| 追加設定 | | | 照合順序データやサンプル データなどの追加の構成パラメーターをカスタマイズする。 | | |
|  | データソース | | なし | なし | 空のデータベースで開始し、バックアップから復元するか、新しいデータベースに設定するためのサンプル データを選択する。 |
|  | データベース照合順序 | | SQL\_Latin1\_General\_CP1\_CI\_AS | SQL\_Latin1\_General\_CP1\_CI\_AS | データベースの照合順序は、データの並べ替えと比較に使用する規則を定義したものであり、データベースの作成後は変更できない。既定の照合順序は、SQL\_Latin1\_General\_CP1\_CI\_AS。 |
|  | メンテナンス期間 | | システムの既定値  確認後記載 | システムの既定値  確認後記載 | メンテナンス イベントの実行中、Azure SQL Database は完全に使用とアクセスが可能だが、メンテナンス更新プログラムを適用するために Azure で短時間 SQL DB インスタンスがオフラインにされるため、一部のメンテナンス更新プログラムでフェールオーバーが必要になる。データベースがエラスティック プールの一部である場合は、エラスティック プールのメンテナンス構成が適用される。 |

### ストレージ

本システムではストレージとしてAzure Stogaeサービスを使用する。

Azure Storageは高可用性、セキュリティ、耐久性、スケーラビリティ、冗長性を備えたクラウドストレージを提供する Microsoft が管理するサービスである。以下にストレージアカウントの定義を示す。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | 本番環境 | 検証環境 | 備考 |
| インスタンスの詳細 | | | | |  | | |
|  | | ストレージアカウント名 | | | prodymhlmsstorageaccount | stgymhlmsstorageaccount |  |
|  | | パフォーマンス | | | Standard | Standard | Storage：ほとんどのシナリオに対して推奨される  Premium：低遅延が必要な場合に使用する |
|  | | 冗長性 | | | ゾーン冗長ストレージ(ZRS) | ローカル冗長ストレージ(LRS) | ローカル冗長ストレージ(LRS)：  サーバーラックとドライブの障害に対する基本的な保護を含む最低コストのオプション。  geo冗長ストレージ(GRS)：  セカンダリリージョンのフェイルオーバー機能を含む。  ゾーン冗長ストレージ(ZRS)：  データセンターレベルの障害に対する保護を含む。  ｇeoゾーン冗長ストレージ(GZRS)：  GRSとZRSの両方のオファリングを含む最適なデータ保護ソリューション。 |
| セキュリティ | | | | | ストレージアカウントに影響を与えるセキュリティ設定を構成する。 | | |
|  | REST API操作の安全な転送を必須にする | | | | 有効 | 有効 | 安全な転送オプションを使用すると、ストレージアカウント上でHTTPSを使用したRESTAPI操作のみを許可することによって、ストレージアカウントのセキュリティが強化される。この設定が有効の場合、HTTPを使用する要求はすべて拒否される。 |
|  | インフラストラクチャ暗号化を有効にする | | | | 無効 | 無効 | 既定では、Azureはストレージアカウントの保存データを暗号化する。インフラストラクチャ暗号化により、ストレージアカウントのデータに2番目の暗号化レイヤーが追加される。データのセキュリティ保護について高いレベルの保証が必要な場合に有効化する。 |
|  | BLOB パブリック アクセスを有効にする | | | | 無効 | 無効 | BLOBパブリックアクセスが有効な場合、ストレージアカウント内のBLOBへの匿名アクセスを許可するようにコンテナーACLを構成することが許可される。無効にすると、基になっているACL構成に関わらず、ストレージアカウント内のBLOBへの匿名アクセスは許可されない。 |
|  | ストレージ アカウント キーへのアクセスを有効にする | | | | 有効 | 有効 | ストレージアカウントキーへのアクセスが無効になっている場合、Shared Access Signature (SAS)などの共有キーによって認可されているアカウントに対する要求はすべて拒否される。現在共有キーを使用してストレージアカウントにアクセスしているクライアントアプリケーションは動作しなくなる。 |
|  | Azure portal で Azure Active Directory の承認を既定にする | | | | 無効 | 無効 | このプロパティを有効にすると、Azure portalでは既定でAzure Active Directoryを使用してBLOB、キュー、テーブルへの要求が承認される。 |
|  | TLSの最小バージョン | | | | バージョン 1.2 | バージョン 1.2 | ストレージアカウントのデータを使用するアプリケーションに必要な最小TLS バージョンを設定する。 |
| Data Lake Storage Gen2 | | | | |  |  |  |
|  | 階層型名前空間を有効にする | | | | 無効 | 無効 | Data Lake Storage Gen2 の階層型名前空間は、ビッグ データの分析ワークロードを高速化し、ファイル レベルのアクセス制御リスト (ACL) を有効にする。 |
| BLOBストレージ | | | | |  |  |  |
|  | ネットワークファイル共有v3を有効にする | | | | 無効 | 無効 | NFSv3を有効にするには、「階層型名前空間」を有効にする必要がある。 |
|  | クロステナントレプリケーションを許可する | | | | 無効 | 無効 | オブジェクトのレプリケーションで、別の Azure Active Directory (Azure AD) テナントの宛先アカウントに BLOB をコピーできるようにする。 |
|  | アクセス層 | | | | ホット | ホット | ホット：アクセス頻度の高いデータと日常的な使用のシナリオ  クール：アクセス頻度の低いデータとバックアップのシナリオ |
| Azure Files | | | | |  |  |  |
|  | 大きいファイルの共有を有効にする | | | | 無効 | 無効 | 最大100TiBのファイル共有をサポーする。大きいファイルの共有ストレージアカウントはgeo冗長ストレージオファリングに変換する機能を備えておらず、アップグレードは永続的である。 |
| テーブルとキュー | | | | |  |  |  |
|  | |  | | カスタマーマネージドキーのサポートを有効にする | 無効 | 無効 | 有効にすると、カスタマー マネージド キー (CMK) を使用したテーブルとキューの暗号化のサポートが有効になる。 |
| ネットワーク接続 | | | | | ストレージアカウントはパブリックIPアドレスまたはサービス エンドポイント経由で公的に接続することも、プライベートエンドポイントを使用してプライベートに接続することもできる。 | | |
|  | 接続方法 | | | | プライベートエンドポイント | プライベートエンドポイント | 仮想ネットワーク内からのみアクセス可能とする。 |
| プライベートエンドポイント | | | | | このリソースへのプライベート接続を許可するには、プライベートエンドポイントを作成する。 | | |
|  | | 名前 | | |  |  | プライベートエンドポイント名 |
|  | | ストレージのサブリソース | | | blob | blob | このプライベート エンドポイントがアクセスできる特定のサブリソース |
|  | | 仮想ネットワーク | | | 本番環境VNet | 検証環境VNet | ストレージアカウントを接続する仮想ネットワーク |
|  | | サブネット | | | ストレージアカウント用サブネット | ストレージアカウント用サブネット | ストレージアカウントを接続するサブネット |
|  | | プライベートDNSと統合 | | |  |  |  |
|  | |  | プライベートDNSゾーンと統合する | | はい | はい | プライベートエンドポイントとプライベートに接続するには、DNS レコードが必要。プライベートエンドポイントをプライベートDNSゾーンと統合することが推奨される。 |
|  | |  | プライベートDNSゾーン | |  |  | 仮想ネットワークと同じリソース グループにあるプライベートDNSゾーンを使用することが推奨される。 |
| ネットワーク ルーティング | | | | | トラフィックがソースから Azureエンドポイントに移動するときに、トラフィックをルーティングする方法を決定する。Microsoft ネットワーク ルーティングが推奨されている。 | | |
|  | | ルーティングの優先順位 | | | Microsoftネットワークルーティング | Microsoftネットワークルーティング | Microsoftネットワークルーティングでは、トラフィックができるだけ早くソースからMicrosoftクラウドに入るようにする。インターネットルーティングでは、トラフィックがAzureエンドポイントにより近い位置でMicrosoftクラウドに入るようにする。 |
| 復旧 | | | | | 偶発的または誤った削除または変更からデータを保護する。 | | |
|  | | コンテナーのポイントインタイム リストアを有効にする | | | 無効 | 無効 | ポイントインタイム リストアを使用して、1 つまたは複数のコンテナーを以前の状態に復元する。ポイントインタイム リストアを有効にする場合は、バージョン管理、変更フィード、BLOB の論理的な削除も有効にする必要がある。 |
|  | | BLOB の論理的な削除を有効にする | | | 有効  削除されたBLOBを保持する日数：7日 | 有効  削除されたBLOBを保持する日数：7日 | 論理的な削除では、上書きされた BLOB を含め、以前に削除とマークされた BLOB を回復することができる。 |
|  | | コンテナーの論理的な削除を有効にする | | | 有効  削除されたコンテナーを保持する日数：7日 | 有効  削除されたコンテナーを保持する日数：7日 | 論理的な削除では、以前に削除とマークされたコンテナーを回復することができる。 |
|  | | ファイル共有の論理的な削除を有効にする | | | 有効  削除されたファイル共有を保持する日数：7日 | 有効  削除されたファイル共有を保持する日数：7日 | 論理的な削除では、以前に削除とマークされたファイル共有を回復することができる。 |
| 追跡 | | | | | バージョンを管理し、BLOB データに加えられた変更を追跡する。 | | |
|  | | BLOB のバージョン管理を有効にする | | | 無効 | 無効 | バージョン管理を使用すると、以前のバージョンの BLOB を復旧と復元のために自動的に管理できる。 |
|  | | BLOB の変更フィードを有効にする | | | 無効 | 無効 | 自分のアカウントでの BLOB の作成、変更、削除の変更内容を追跡する。 |

#### コンテナー

|  |  |  |
| --- | --- | --- |
| コンテナー名 | パブリックアクセスレベル | 用途 |
| 本番環境：prod-ymhlms-data  検証環境：stg-ymhlms-data | プライベート | 画像データ、CSVファイル等を格納 |
| azure-webjobs-hosts | プライベート | Azure Functions用 |
| azure-webjobs-secrets | プライベート | Azure Functions作成時に自動で作成される。 |

#### ファイル共有

|  |  |
| --- | --- |
| ファイル共有名 | 用途 |
| 本番環境：prod-ymhlms-functionapp  検証環境：stg-ymhlms-functionapp | Azure Functions用  Azure Functions作成時に自動で作成される。 |

## ソフトウェア構成

本システムのソフトウェアは全てAzure管理のソフトウェアを利用する。

ユーザー管理の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。

### VNet(仮想ネットワーク)

本システムではAzure内のプライベートネットワークの基本的な構成要素であるVNetを構成する。VNetにより、さまざまな種類のAzureリソースが、他のAzureリソース、インターネット、およびオンプレミスのネットワークと安全に通信することが可能となる。

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、本番環境用VNetと検証環境用VNetを作成する。

以下にVNetの定義を示す。

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | 本番環境 | 検証環境 | 備考 |
| VNet名 | prod-ymhlms-vnet | stg-ymhlms-vnet | 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VNetを分ける。 |
| IPv4 アドレス空間 | 172.16.0.0/16 | 172.17.0.0/16 | CIDR 表記の 1 つまたは複数のアドレス プレフィックスとして指定された、仮想ネットワークのアドレス空間。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アドレス空間の追加 | 無効  (既存の関連システムがIPv6を使用していないため無効とする。) | | IPv6 アドレス空間を追加して、デュアルスタック (IPv4 と IPv6 に対応) の仮想ネットワークを作成できる。仮想ネットワークの作成後に、後で IPv6 サポートを追加することも可能。 |
| サブネット | 以下参照 | 以下参照 | CIDR 表記のサブネットのアドレス範囲。仮想ネットワークのアドレス空間に含まれている必要がある。 |
| BastionHost | 無効化  (仮想マシンを使用しないため無効とする。) | | 仮想ネットワーク内でプロビジョニングされるフルプラットフォームマネージドPaaSサービス。Azure Portalで直接、仮想マシンへの安全でシームレスなRDP/SSH接続をSSL経由で提供する。 |
| DDoS Protection Standard | Basic  (著しくDDos攻撃を受けた場合に有効化を検討する。) | | DDoS保護プランは有償サービスで、仮想ネットワーク内の保護対象リソースすべてに対するDDoS攻撃による影響から保護するための高度なDDoS軽減機能が提供される。基本的なDDoS保護は、既定でAzureプラットフォームに統合され、無償で利用できる。 |
| ファイアウォール | 無効化 | | Azure Virtual Network リソースを保護するクラウド ベースのマネージド ネットワーク セキュリティ サービス。 |

なお、IPv4でVNet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 |
| 10.0.0.0 - 10.255.255.255 (10/8 プレフィックス) |
| 172.16.0.0 - 172.31.255.255 (172.16/12 プレフィックス) |
| 192.168.0.0 - 192.168.255.255 (192.168/16 プレフィックス) |

### サブネット

VNetのネットワーク範囲を区切るサブネットを作成する。

#### 本番環境用サブネット

|  |  |  |  |
| --- | --- | --- | --- |
| サブネット | サブネット名 | IPv4 CIDRブロック | サービスエンドポイント |
| FunctionApp用サブネット | prod-ymhlms-functionapp-subnet | 172.16.0.0/24 | - |
| SQL Database用サブネット | prod-ymhlms-sqldatabase-subnet | 172.16.1.0/27 | - |
| ストレージアカウント用サブネット | prod-ymhlms-storageaccount-subnet | 172.16.1.32/27 | - |

#### 検証環境用サブネット

|  |  |  |  |
| --- | --- | --- | --- |
| サブネット | サブネット名 | IPv4 CIDRブロック | サービスエンドポイント |
| FunctionApp用サブネット | stg-ymhlms-functionapp-subnet | 172.17.0.0/24 | - |
| SQL Database用サブネット | stg-ymhlms-sqldatabase-subnet | 172.17.1.0/27 | - |
| ストレージアカウント用サブネット | stg-ymhlms-storageaccount-subnet | 172.17.1.32/27 | - |

### ネットワークセキュリティグループ(NSG)

Azureサブネットへの承諾されていないトラフィックを防ぐため、ネットワークセキュリティグループを使用する。

ネットワークセキュリティグループはシンプルなステートフルパケットインスペクションデバイスであり、5タプルアプローチ(発信元IP、発信元ポート、接続先IP、接続先ポート、およびレイヤー4プロトコル)を使用して、ネットワークトラフィックに対する許可/拒否ルールを作成する。許可または拒否の対象は、単一のIPアドレス、複数のIPアドレス、またはサブネット全体との間のトラフィックとなる。

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 |

#### 本番環境用NSG

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | FunctionApp用NSG | | | | | |
| NSG名 | prod-ymhlms-functionapp-nsg | | | | | |
| 割当先サブネット | FunctionApp用サブネット | | | | | |
| 受信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |
| 送信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | SQL Database用NSG | | | | | |
| NSG名 | prod-ymhlms-sqldatabase-nsg | | | | | |
| 割当先サブネット | SQL Database用サブネット | | | | | |
| 受信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |
| 送信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | ストレージアカウント用NSG | | | | | |
| NSG名 | prod-ymhlms-storageaccount-nsg | | | | | |
| 割当先サブネット | ストレージアカウント用サブネット | | | | | |
| 受信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |
| 送信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |

#### 検証環境用NSG

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | FunctionApp用NSG | | | | | |
| NSG名 | stg-ymhlms-functionapp-nsg | | | | | |
| 割当先サブネット | FunctionApp用サブネット | | | | | |
| 受信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |
| 送信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | SQL Database用NSG | | | | | |
| NSG名 | stg-ymhlms-sqldatabase-nsg | | | | | |
| 割当先サブネット | SQL Database用サブネット | | | | | |
| 受信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |
| 送信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | ストレージアカウント用NSG | | | | | |
| NSG名 | stg-ymhlms-storageaccount-nsg | | | | | |
| 割当先サブネット | ストレージアカウント用サブネット | | | | | |
| 受信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |
| 送信セキュリティ規則  (追加分) | 優先度 | ポート | プロトコル | ソース | 宛先 | アクション |
| - | - | - | - | - | - |

### ルートテーブル

Azureでは、Azure仮想ネットワークのサブネットごとにルートテーブルが自動的に作成され、既定のシステムルートがテーブルに追加される。Azureのシステムルートをカスタムルートでオーバーライドし、カスタムルートをルートテーブルに追加できる。サブネットのルートテーブルのルートに基づいて、サブネットからの送信トラフィックがルーティングされる。

#### システムルート

Azureでは、システムルートが自動的に作成され、仮想ネットワークの各サブネットに割り当てられる。

|  |  |  |
| --- | --- | --- |
| ルート | |  |
|  | アドレスプレフィックス | 仮想ネットワークに固有 |
|  | 次ホップの種類 | 仮想ネットワーク |
| ルート | |  |
|  | アドレスプレフィックス | 0.0.0.0/0 |
|  | 次ホップの種類 | インターネット |
| ルート | |  |
|  | アドレスプレフィックス | 10.0.0.0/8 |
|  | 次ホップの種類 | なし |
| ルート | |  |
|  | アドレスプレフィックス | 192.168.0.0/16 |
|  | 次ホップの種類 | なし |
| ルート | |  |
|  | アドレスプレフィックス | 100.64.0.0/10 |
|  | 次ホップの種類 | なし |

#### Function App用カスタムルート

以下のルートテーブルを作成し、関連付けるサブネットをインターネットから接続不可とする。

仮想ネットワーク外からの通信を遮断するため、「ゲートウェイのルートを伝達する」を「いいえ」とする。

|  |  |  |  |
| --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 |
| ルートテーブル名 | | prod-ymhlms-functionapp-rt | stg-ymhlms-functionapp-rt |
| ゲートウェイのルートを伝達する | | いいえ | いいえ |
| ルート | |  |  |
|  | アドレスプレフィックス | (本番環境VNetのIPv4 アドレス空間) | (検証環境VNetのIPv4 アドレス空間) |
|  | 次ホップの種類 | なし | なし |
|  | アドレスプレフィックス | 0.0.0.0/0 | 0.0.0.0/0 |
|  | 次ホップの種類 | なし | なし |
| サブネットの関連付け | | FunctionApp用サブネット | FunctionApp用サブネット |

#### ストレージアカウント用カスタムルート

以下のルートテーブルを作成し、関連付けるサブネットをインターネットから接続不可とする。

仮想ネットワーク外からの通信を遮断するため、「ゲートウェイのルートを伝達する」を「いいえ」とする。

|  |  |  |  |
| --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 |
| ルートテーブル名 | | prod-ymhlms-storageaccount-rt | stg-ymhlms-storageaccount-rt |
| ゲートウェイのルートを伝達する | | いいえ | いいえ |
| ルート | |  |  |
|  | アドレスプレフィックス | (本番環境VNetのIPv4 アドレス空間) | (検証環境VNetのIPv4 アドレス空間) |
|  | 次ホップの種類 | なし | なし |
|  | アドレスプレフィックス | 0.0.0.0/0 | 0.0.0.0/0 |
|  | 次ホップの種類 | なし | なし |
|  | アドレスプレフィックス | (SQL DatabaseのIPV4アドレス)/32 | (SQL DatabaseのIPV4アドレス)/32 |
|  | 次ホップの種類 | なし | なし |
| サブネットの関連付け | | ストレージアカウント用サブネット | ストレージアカウント用サブネット |

#### SQL Database用カスタムルート

|  |  |  |  |
| --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 |
| ルートテーブル名 | | prod-ymhlms-sqldatabase-rt | stg-ymhlms-sqldatabase-rt |
| ゲートウェイのルートを伝達する | | いいえ | いいえ |
| ルート | |  |  |
|  | アドレスプレフィックス | (本番環境VNetのIPv4 アドレス空間) | (検証環境VNetのIPv4 アドレス空間) |
|  | 次ホップの種類 | なし | なし |
|  | アドレスプレフィックス | 0.0.0.0/0 | 0.0.0.0/0 |
|  | 次ホップの種類 | なし | なし |
|  | アドレスプレフィックス | (ストレージアカウントのIPV4アドレス)/32 | (ストレージアカウントのIPV4アドレス)/32 |
|  | 次ホップの種類 | なし | なし |
| サブネットの関連付け | | FunctionApp用サブネット | FunctionApp用サブネット |

### 名前解決

本システムでは、DNSサーバーとしてAzure DNS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 / Lambda / RDS |
| 99.9% | ACM / AWS Backup / AWS Systems Manager / CodeCommit / CloudFront / CloudTrail / CloudWatch / CodeBuild / Cognito / DataSync / EC2 / ElasticSearch / 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 | 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

## Application Insights

## 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5.9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5.9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  (access\_log / access\_log / error\_log) | 本番環境：/aws/elasticbeanstalk/ymhlms/prod/webaplog  検証環境：/aws/ec2/ymhlms/stg/webaplog | 東京 | ログ監視を実施する |
| RDS | 監査ログ | 本番環境：  /aws/rds/instance/ymhlms/prod/<インスタンス名>/auditlog  検証環境：  /aws/rds/instance/ymhlms/stg/<インスタンス名>/auditlog |  |  |
|  | 全般ログ | 本番環境：  /aws/rds/instance/ymhlms/prod/<インスタンス名>/generallog  検証環境：  /aws/rds/instance/ymhlms/stg/<インスタンス名>/generallog |  |  |
|  | スロークエリログ | 本番環境：  /aws/rds/instance/ymhlms/prod/<インスタンス名>/slowquerylog  検証環境：  /aws/rds/instance/ymhlms/stg/<インスタンス名>/slowquerylog |  |  |
| バッチサーバー | ビルド出力ログ | 本番環境：  /aws/codebuild/ymhlms/prod/<プロジェクト名>/buildoutputlog  検証環境：  /aws/codebuild/ymhlms/stg/<プロジェクト名>/buildoutputlog |  |  |
| DataSync | 実行ログ | 本番環境：/aws/datasync/ymhlms/prod/synclog  検証環境：/aws/datasync/ymhlms/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/ymhlms/prod/dnsquerylog  検証環境：/aws/route53/ymhlms/stg/dnsquerylog |  |  |
| 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/ymhlms/prod/operationlog  検証環境：/aws/cloudtrail/ymhlms/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  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。 |
| ELB | リクエストログ | alb/ |  |
| CodeBuild | ビルドログ | codebuildlog/ |  |
| Data Pipeline | 実行ログ | datapipeline/<テーブル名> |  |
| S3 | アクセスログ | 2.3.3ストレージ参照 | 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 | 5.9アラート通知先を参照する。) |  |
|  |  | failed |  |  |
|  |  | notice |  |  |

## 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 |
| ymhlms-cfnuser | AmazonKinesisFirehoseFullAcces | ログ収集管理 |  |
| (CloudFormation管理ユーザー) | 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 | 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 |  |
|  | 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 |  |
| ymhlms-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 |
| ymhlms-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 |
| 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。

### API Management

Azure API Management は、API を保護、発行、分析するためのスケーラブルなAPI 管理プラットフォームを提供する。

本システムではAPI Managementを使用してFunction AppをAPIから呼び出す構成とする。

また、セキュリティのため、インターネットから直接のAPI Managementへのアクセスは禁止とし、Front Doorからのアクセスのみを許可する。

以下にAPI Managenemtの定義を示す。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | 本番環境 | 検証環境 | 備考 |
| インスタンスの詳細 | | |  | | |
|  | リソース名 | | prod-ymhlms-apim | stg-ymhlms-apim | API Managementサービスの一意の名前。 この名前を後から変更することはできない。  サービスの名前は「<API Managementサービス名>.azure-api.net」の形式で既定のドメイン名を生成するために使用される。カスタムドメイン名を使用することも可能。 |
|  | 組織名 | |  |  | 組織の名前。 この名前は、開発者ポータルのタイトルや通知用電子メールの送信者など、さまざまな場所に使用される。 |
|  | 管理者メールアドレス | |  |  | API Managementからのすべての通知が送信されるメールアドレス。 |
| 価格レベル | | |  | | |
|  | 価格レベル | | Consumption | Consumption | SLAや拡張可能なユニット最大数に応じて価格レベルを選択する。  Consumption：SLA99.95%、自動スケーリング |
| 監視 | | |  | | |
|  | Application Insights | | 有効 | 有効 | 複数のプラットフォームでアプリを構築し、管理するWeb開発者向けの拡張可能なサービスであるAzure Application Insightsと統合できる。 |
|  |  | Application Insights名 |  |  |  |
| 拡張 | | |  | | |
|  | ユニット | | -  (価格レベルConsumptionの場合は指定不可) | -  (価格レベルConsumptionの場合は指定不可) | ユニットは専用のAzureリソースで構成され、1 か月あたりの API 呼び出しの数として表される特定の耐荷容量がある。 この数値は呼び出しの制限を表しているのではなく、大まかな容量計画を行うための最大スループット値である。 実際のスループットと待ち時間は、コンカレント接続の数とレート、構成されたポリシーの種類と数、要求のサイズと応答のサイズ、バックエンドの待ち時間などの多くの要因によって、大幅に異なる。 |
| 管理ID | | | マネージドID により、開発者は資格情報を管理する必要がなくなる。たとえば、アプリケーションはマネージドIDを使用することで、開発者が安全に資格情報を格納できるAzureキーコンテナーなどのリソースにアクセスしたり、ストレージアカウントにアクセスしたりできるようになる。 | | |
|  | システム割り当てマネージドID | | オフ | オフ | システム割り当てマネージドID：  サービスインスタンスのライフサイクルに関連付けられたIDがAzure ADに作成される。したがって、リソースが削除されると、そのIDもAzureによって自動的に削除される。  ユーザー割り当てマネージドID：  ユーザー割り当てマネージドIDを作成して、Azureサービスの1つまたは複数のインスタンスに割り当てることができる。ユーザー割り当てマネージドIDの場合、IDはそれを使用するリソースとは別に管理される。 |
| 仮想ネットワーク | | | API ManagementをVNetの内部にデプロイし、ネットワーク内でバックエンドサービスにアクセスすることができる。 | | |
|  | タイプ | | External | External | External：パブリック インターネットから外部ロード バランサーを使用してアクセス可能とする。  Internal：VNet内から内部ロードバランサーを使用してのみアクセス可能とする。 |
|  |  | 仮想ネットワーク | 本番環境VNet | 検証環境VNet | API Managementが接続する仮想ネットワークを指定 |
|  |  | サブネット | API Management用サブネット | API Management用サブネット | API Managementが接続するサブネットを指定 |
| プロトコル設定 | | | API トラフィックをセキュリティで保護するために、API ゲートウェイのプロトコル構成を管理する。 | | |
|  | 暗号化 | |  |  |  |
|  |  | 3DES | 無効 | 無効 | 3DESの有効 / 無効を指定 |
|  | クライアント側プロトコル | |  |  |  |
|  |  | HTTP/2 | 無効 | 無効 | HTTP/2の有効 / 無効を指定 |
|  | クライアント側転送セキュリティ | | |  |  |
|  |  | TLS 1.1 | 無効 | 無効 | TLS 1.1の有効 / 無効を指定 |
|  |  | TLS 1.0 | 無効 | 無効 | TLS 1.0の有効 / 無効を指定 |
|  |  | SSL 3.0 | 無効 | 無効 | SSL 3.0の有効 / 無効を指定 |
|  | バックエンド側転送セキュリティ | | |  |  |
|  |  | TLS 1.1 | 無効 | 無効 | TLS 1.1の有効 / 無効を指定 |
|  |  | TLS 1.0 | 無効 | 無効 | TLS 1.0の有効 / 無効を指定 |
|  |  | SSL 3.0 | 無効 | 無効 | SSL 3.0の有効 / 無効を指定 |
| インバウンドポリシー | | | インバウンドポリシーでHTTP ヘッダーを確認し、Front Door以外からのアクセスを拒否する。 | | |
|  | value | | ZDe~PmzcZE00BsQV\eC}K5NPD:uqFV\_6 | [gK7=0s6:.}RoNfwo=4FW+v5D#\F$7.K | Front DoorでHTTPヘッダーに追加する文字列 |
|  | ポリシーステートメント | | <check-header name="Authorization" failed-check-httpcode="401" failed-check-error-message="Not authorized" ignore-case="false">  <value>”value”</value>  </check-header> | | |

### Front Door

本システムではCDNとしてFront Doorを使用する。

Front DoorではWebアプリケーションファイアウォール機能を有効化し、Webアプリケーションの脆弱性を狙った攻撃からシステムを保護する。

以下にFront Doorの定義を示す。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | 本番環境 | 検証環境 | 備考 |
| フロントエンドまたはドメイン | | | | フロントエンドホストはazurefd.net など Front Doorの既定のドメイン上の目的のサブドメインを指定して、そのホストから Front Door経由でトラフィックをルーティングする。必要に応じてカスタムドメインをオンボードすることもできる。 | | |
|  | フロントエンドホスト | | |  |  |  |
|  |  | ホスト名 | | prod-ymhlms-afd  .azurefd.net | stg-ymhlms-afd  .azurefd.net | ルーティングされる必要があるユーザー要求の受信ホスト名 |
|  |  | セッションアフィニティ | | 無効 | 無効 | ユーザーセッションから同一のアプリケーションバックエンドへの直接の後続トラフィックを有効にして、Front Doorで生成されたCookieを使用して処理できるようにする。 |
|  |  | WEB アプリケーション ファイアウォール | | 無効 | 無効 | WAF ポリシーを1つ以上のFront Door フロントエンドに適用して、Webアプリケーションの一元的な保護を提供できる。 |
|  | カスタムドメイン | | | フロントドアにカスタムドメインを追加する。DNSプロバイダーでカスタムドメインから Front Door azurefd.net フロントエンド ホストへのDNSマッピングを作成する必要がある。 | | |
|  |  | カスタムホスト名 | | 本番環境ドメイン名 | 検証環境ドメイン名 | Front Door 構成に追加するカスタム ドメイン名 |
|  |  | セッションアフィニティ | | 無効 | 無効 | ユーザーセッションから同一のアプリケーションバックエンドへの直接の後続トラフィックを有効にして、Front Doorで生成されたCookieを使用して処理できるようにする。 |
|  |  | WEB アプリケーション ファイアウォール | | 有効 | 有効 | WAF ポリシーを1つ以上のFront Door フロントエンドに適用して、Webアプリケーションの一元的な保護を提供できる。 |
|  |  |  | ポリシー | prodymhlmswafpolicy | stgymhlmswafpolicy | 適用するWAFポリシーを指定 |
| バックエンドプール | | | | バックエンドプールは、フロントドアロードでクライアント要求を分散する同等のバックエンドのセット。 | | |
|  | 名前 | | | prod-ymhlms-fd-apim-backend | stg-ymhlms-fd-apim-backend | ルーティングされる必要があるユーザー要求の受信ホスト名 |
|  | バックエンド | | | バックエンドは、Front Door がクライアント要求をルーティングする宛先となるアプリケーションサーバーである。送信するトラフィックの割合を定義するためにバックエンドに重みを割り当てたり、アーキテクチャのアクティブ/スタンバイの分類を定義するためにバックエンドの優先順位を設定することが可能。 | | |
|  | バックエンドホスト名 | | API Managementホスト名 | API Managementホスト名 | バックエンドのホスト名または IP アドレス |
|  | 優先度 | | 1 | 1 | すべてのトラフィックでプライマリサービスバックエンドを使用する場合は、さまざまなバックエンドに優先度を割り当てることができ、プライマリバックエンドまたはバックアップバックエンドが使用できない場合は、バックアップを提供することができる。 |
|  | 重み | | 50 | 50 | 均等にまたは加重の係数に応じて、バックエンドのセット全体にトラフィックを分散する場合、さまざまなバックエンドに加重を割り当てることができる。 |
|  | 正常性ブローブ | | | Front Doorは、構成された各バックエンドに定期的な HTTP/HTTPS プローブ要求を送信して各バックエンドの近接性と正常性を判断し、エンド ユーザーの要求を負荷分散する。 | | |
|  |  | 状態 | | 有効 | 有効 | 正常性ブローブの有効/無効を指定 |
|  |  | プロトコル | | HTTPS | HTTPS | 正常性プローブのバックエンドとの通信プロトコル |
|  |  | ブローブメソッド | | HEAD | HEAD | 正常性プローブによるバックエンドプールインスタンスのクエリに使用される HTTPメソッド。応答本文を確認する必要がない場合は、HEADを使用する。 |
|  |  | 間隔(秒) | | 30 | 30 | 正常性プローブの頻度 |
|  | 負荷分散 | | | バックエンドが正常か異常かを示すために使用する必要のあるサンプルセットを定義するには負荷分散の設定を構成する。値がゼロ(0)の待機時間感度は、使用可能な最速のバックエンドに常に送信することを意味する。それ以外の場合、フロントドアでは、構成済みの待機時間感度内で、最速のバックエンドと次に速いバックエンドの間でトラフィックをラウンドロビンする。 | | |
|  |  | サンプルサイズ | | 4 | 4 | バックエンドの可用性を評価するためのサンプルセット |
|  |  | 成功したサンプルが必要です | | 2 | 2 | バックエンドの正常性を宣言するためのサンプルセット |
|  |  | 待機時間感度(ミリ秒) | | 0 | 0 | 最小遅延時間でのバックエンドを識別するための待機時間感度 |
| ルーティング規則 | | | | バックエンドプールは、フロントドアロードでクライアント要求を分散する同等のバックエンドのセット。 | | |
|  | 名前 | | | prod-ymhlms-afd-route | stg-ymhlms-afd-route | ルーティングされる必要があるユーザー要求の受信ホスト名 |
|  | 受入れ済みのプロトコル | | | HTTPとHTTPS | HTTPとHTTPS | ルーティング規則で許可される受信プロトコルを指定 |
|  | フロントエンドまたはドメイン | | | prod-ymhlms-afd.azurefd.net | stg-ymhlms-afd.azurefd.net | フロントエンドまたはドメインを指定 |
|  | 一致するパターン | | | / | / | このルートで受け入れられるすべてのURLパスパターンを設定する。たとえば、/users/\*に設定するとURL 「www.contoso.com/users/\*」のすべての要求を受け入れることができる。 |
|  | ルートの種類 | | | 進む | 進む | フロントドアのルートが一致すると、このルーティング規則に関連付けられているルールエンジンの構成が実行された後、下で定義されている一般的なルートの構成が実行される。 |
|  | バックエンドプール | | | prod-ymhlms-afd-apim-backend | stg-ymhlms-afd-apim-backend | ルート対象のバックエンドプールを指定 |
|  | 転送プロトコル | | | HTTPSのみ | HTTPSのみ | 要求をバックエンドに転送するため、または着信要求からのプロトコルと一致させるために使用するプロトコル |
|  | URLの書き換え | | | 無効 | 無効 | バックエンドに転送するための URL 書き換え要求を作成するときに使用するパス |
|  | キャッシュ | | | 無効 | 無効 | キャッシュを有効にすると、Front Door によって静的なコンテンツがキャッシュされる。 |
| ルールエンジンの構成 | | | | エッジでの HTTP 要求の処理方法をカスタマイズし、Web アプリケーションの動作をより細かく制御する。 | | |
|  | ルールエンジン名 | | | prodYmhlmsAfdRulengine | stgYmhlmsAfdRulengine | ルールエンジンの名称を指定。  文字で始まり、数字と文字のみ使用可。 |
|  | ルール | | | prodYmhlmsAfdHTTPRequestHeaderRule | stgYmhlmsAfdHTTPRequestHeaderRule | ルールの名称を指定。  文字で始まり、数字と文字のみ使用可。 |
|  |  | アクションの追加 | |  |  |  |
|  |  |  | アクション | 要求ヘッダー | 要求ヘッダー | 要求ヘッダー / 応答ヘッダー / ルーティングの構成をオーバーライドする  から選択。 |
|  |  |  | 演算子 | 追加 | 追加 | 追加 /　上書き /　削除 から選択。 |
|  |  |  | ヘッダー名 | Authorization | Authorization | API Managementでヘッダーを確認し、ヘッダー値が含まれる要求のみアクセス可とする。 |
|  |  |  | ヘッダー値 | ZDe~PmzcZE00BsQV\eC}K5NPD:uqFV\_6 | [gK7=0s6:.}RoNfwo=4FW+v5D#\F$7.K |

Azure Front Door は、Microsoftグローバルエッジネットワークを使用して、セキュリティで保護された高速でスケーラビリティの高Webアプリケーションを配信するためのスケーラブルなグローバルエントリ ポイントであり、DDoS保護や、アプリケーション層のセキュリティとキャッシュを内蔵している。Front Doorは以下の機能を提供する。

|  |  |
| --- | --- |
| 機能概要 | 内容 |
| 分割TCP ベースの エニーキャスト プロトコル を使用したアプリケーションのパフォーマンスの高速化 | 分割 TCP は、長いラウンドトリップ時間が発生する接続を小さく分割することによって待機時間と TCP の問題を軽減する手法。また、エニーキャストプロトコルを使用することにより、ユーザー要求は最も少ないネットワーク ホップで最も近い環境に到達する。 |
| インテリジェントな 正常性プローブ によるバックエンド リソースの監視 | それぞれの Front Door 環境では、特定の Front Door 環境の各バックエンドの正常性と近接性を確認するために、構成されている各バックエンドに合成 HTTP/HTTPS 要求を定期的に送信する。 Front Door は、プローブからのこれらの応答を使用して、クライアント要求のルーティング先として 最適なバックエンドリソースを決定する。 |
| 要求の URL パス ベース のルーティング | 接続の確立と TLS ハンドシェイクが行われ、要求が Front Door 環境に届いたときに、Front Door で最初に行われることの 1 つとして、その要求と一致する特定のルーティング規則が決定され、構成内で定義されているアクションが実行される。 |
| 効率的なアプリケーション インフラストラクチャを実現する、複数の Web サイトのホスティング | URLパスベースをルーティングすることにより、複数のWebサイトをホスティングすることができる。 |
| Cookie ベースの セッション アフィニティ | 既定では、セッション アフィニティを使用しない場合、Front Door は同じクライアントからの要求を別のバックエンドに転送する。 一部のステートフルなアプリケーションや、同じユーザーからの要求が続く特定のシナリオでは、最初の要求を処理したのと同じバックエンドが優先される。 Cookie ベースのセッション アフィニティ機能は、同じバックエンド上にユーザー セッションを保持する。 マネージド Cookie を使用すると、Azure Front Door は、ユーザー セッションからの後続のトラフィックを、処理のために同じバックエンドに送ることができる。 |
| SSL オフロード と証明書管理 | カスタム ドメイン (例: https://www.contoso.com) で HTTPS プロトコルを使用すると、インターネット経由での送信時、機密データが TLS/SSL 暗号化でセキュリティ保護されて配信される。 Web ブラウザーが HTTPS 経由で Web サイトに接続しているときに、Web サイトのセキュリティ証明書を検証し、正当な証明機関によって発行されていることを確認する。 このプロセスによりセキュリティを確保し、Web アプリケーションを攻撃から保護する。  証明書の取得または更新の追加コストやHTTPS トラフィックの追加コストは不要。証明書は自動的にプロビジョニングされ、有効期限になる前に更新される。これにより、証明書の期限切れによりサービスが中断されるリスクがなくなる。 |
| 独自の カスタム ドメイン の定義 | Front Door を作成すると、azurefd.net のサブドメインである既定のフロントエンド ホストが、バックエンドから Front Door コンテンツを配信するための URL に、既定で含まれるようになる (例: https://contoso-frontend.azurefd.net/activeusers.htm)。 便宜を図るため、Azure Front Door には、カスタム ドメインを既定のホストと関連付けることができる。 |
| Web Application Firewall (WAF) が統合されたアプリケーション セキュリティ | Web アプリケーション ファイアウォール (WAF) 機能を利用し、SQL インジェクションやクロスサイト スクリプティングなどのWebアプリケーションを対象とした攻撃や一般的な悪用、脆弱性から Web アプリケーションを一元的に保護することができる。 |
| URL リダイレクト による、HTTPS への HTTP トラフィックのリダイレクト | Azure Front Door を使用すると、プロトコル、ホスト名、パス、クエリ文字列の各レベルでトラフィックをリダイレクトできる。 リダイレクトはパス ベースであるため、これらの機能を個々のマイクロサービスに対して構成できる。 これにより、リソースの使用を最適化することで、アプリケーションの構成を簡約化し、グローバルなパス ベースのリダイレクトを含む、新しいリダイレクト シナリオをサポートすることができる。 |
| URL 書き換え によるカスタム転送パス | Azure Front Door を使用すると、バックエンドに転送する要求を作成するときに使用するオプションの カスタム転送パス を構成することで、URL 書き換えを行うことができる。 |
| エンド ツー エンドの IPv6 接続と HTTP/2 プロトコル のネイティブ サポート | HTTP/2 は HTTP/1.1 のメジャー リビジョンであり、応答時間を短縮することにより、Web パフォーマンスを向上させることができる。 HTTP/2 は、使い慣れた HTTP メソッド、状態コード、およびセマンティクスを維持することによって、ユーザー エクスペリエンスを向上させる。 HTTP/2 は HTTP および HTTPS と連携して動作するように設計されているが、多くのクライアント Web ブラウザーは、HTTP/2 over TLS (トランスポート層セキュリティ) のみをサポートしている。また、IPv6接続をサポートする。 |
| キャッシュ | Front Door は最新の Content Delivery Network (CDN) であり、動的サイト アクセラレーションおよび負荷分散に加えて、他の CDN と同様にキャッシュの動作もサポートされている。 |

### Azure Web Application Firewall

Azure Web Application Firewallを使用し、悪意のある攻撃や一般的な Web 脆弱性 (SQL インジェクション、クロスサイト スクリプティングなど) から Web アプリを保護する。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Azureマネージドルールセットを適用する。

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記録(検出)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。

Azure Web Application Firewallの定義を以下に示す。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | 本番環境 | 検証環境 | 備考 |
| プロジェクトの詳細 | | |  |  |  |
|  | 次に対するポリシー | | グローバルWAF(フロントドア) | グローバルWAF(フロントドア) | WAF ポリシーを使用して保護するリソースの種類を指定 |
|  | フロントドアSKU | | Front Door | Front Door | フロントドアSKUの選択によって、利用できる機能と、WAFポリシーに関連付けることができるフロントドアプロファイルが決まる。 |
| インスタンスの詳細 | | |  |  |  |
|  | ポリシー名 | | prodYmhlmsWafpolicy | stgYmhlmsWafpolicy | WAF ポリシーの一意の名前 |
|  | ポリシーの状態 | | 有効 | 有効 | WAFポリシーの有効/無効を指定。無効の場合、WAFポリシーはどのWeb サイトにも適用されない。 |
|  | ポリシーモード | | 防止 | 検出 | 検出モードでは、すべての脅威アラートを監視し、ログファイルに記録する。ログファイルに記録する場合、Front Door 診断が有効で、WAF ポリシー アクションが「ログ」に設定されている必要がある。防止モードでは要求がルールに一致する場合、該当するWAFアクションを実行する。 |
| 規定のルールセット | | | DefaultRuleSet\_1.0 | DefaultRuleSet\_1.0 | 事前構成済みのルールセットは既定で有効。このルールセットは、Webアプリケーションを上位10件のOpen Web Application Security Project (OWASP) カテゴリで定義されている一般的な脅威から保護する。 |
|  | FIXルールグループ | | 可能性のあるセッション固定攻撃向けルール | | |
|  |  | アクション | ブロック | ログ | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 有効 | 有効 | 状態の有効/無効を指定 |
|  | JAVAルールグループ | | JAVA攻撃向けルール | | |
|  |  | アクション | ブロック | ブロック | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 無効 | 無効 | 状態の有効/無効を指定  本システムではJAVAを使わないため無効とする。 |
|  | LFIルールグループ | | ローカル ファイル インクルージョン向けルール | | |
|  |  | アクション | ブロック | ログ | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 有効 | 有効 | 状態の有効/無効を指定 |
|  | PHPルールグループ | | PHPインジェクション攻撃向けルール | | |
|  |  | アクション | ブロック | ブロック | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 無効 | 無効 | 状態の有効/無効を指定  本システムではPHPを使わないため無効とする。 |
|  | PROTOCOL-ATTACKルールグループ | | プロトコル攻撃向けルール | | |
|  |  | アクション | ブロック | ログ | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 有効 | 有効 | 状態の有効/無効を指定 |
|  | RCEルールグループ | | リモート コマンド実行向けルール | | |
|  |  | アクション | ブロック | ログ | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 有効 | 有効 | 状態の有効/無効を指定 |
|  | SQLIルールグループ | | SQLインジェクション向けルール | | |
|  |  | アクション | ブロック | ログ | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 有効 | 有効 | 状態の有効/無効を指定 |
|  | XSSルールグループ | | クロスサイトスクリプティング向けルール | | |
|  |  | アクション | ブロック | ログ | 許可 / ブロック / ログ / リダイレクト から選択 |
|  |  | 状態 | 有効 | 有効 | 状態の有効/無効を指定 |
| ポリシー設定 | | | Web Application Firewall (WAF) ポリシーを使用すると、カスタムおよび管理されたルールのセットによって Web アプリケーションへのアクセスを制御できる。 | | |
|  | 要求本文の検査を有効にする | | 無効 | 無効 | 要求本文の検査が無効になっている場合、WAFでは、HTTPメッセージ本文の内容が評価されない。このような場合、WAFではヘッダー、Cookie、URIに対してWAFのルールの適用が続行される。要求本文の検査が無効になっている場合は、要求本文の最大サイズのフィールドを適用できず、設定することができない。 |
|  | リダイレクト URL | | - | - | WAFポリシーに含まれているいずれかのルールに対してリダイレクトアクションが選択されている場合に要求をリダイレクトするリダイレクトURLを指定。 |
|  | ブロックの応答状態コード | | 403 | 403 | 要求がブロックされたときに WAF が送信する応答状態コード |
|  | ブロックの応答本文 | | - | - | WAFルールによって要求がブロックされたときに、カスタム応答メッセージを追加する。 |