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](#_Toc83023615)

[2 システム構成 7](#_Toc83023616)

[2.1 システム構成図 7](#_Toc83023617)

[2.2 サービス構成 8](#_Toc83023618)

[2.2.1 サービス一覧 8](#_Toc83023619)

[2.2.2 サブスクリプション 9](#_Toc83023620)

[2.2.3 デプロイモデル 10](#_Toc83023621)

[2.2.4 リソースグループ 10](#_Toc83023622)

[2.2.5 リージョン 11](#_Toc83023623)

[2.3 サーバー構成 12](#_Toc83023624)

[2.3.1 APサーバー(Azure Functions、Logic Apps) 12](#_Toc83023625)

[2.3.2 DBサーバー(Azure SQL Database) 16](#_Toc83023626)

[2.3.3 ストレージ(Azure Storage) 21](#_Toc83023627)

[2.3.4 データ統合サーバー(Data Factory) 25](#_Toc83023628)

[2.4 ソフトウェア構成 26](#_Toc83023629)

[2.5 ネットワーク構成 26](#_Toc83023630)

[2.5.1 VNet(仮想ネットワーク) 26](#_Toc83023631)

[2.5.2 サブネット 28](#_Toc83023632)

[2.5.3 ネットワークセキュリティグループ(NSG) 29](#_Toc83023633)

[2.5.4 ルートテーブル 32](#_Toc83023634)

[2.5.5 名前解決 34](#_Toc83023635)

[3 可用性 35](#_Toc83023636)

[3.1 耐障害性 35](#_Toc83023637)

[3.2 災害対策 35](#_Toc83023638)

[4 拡張性 36](#_Toc83023639)

[4.1 拡張性設計 36](#_Toc83023640)

[5 保守性 38](#_Toc83023641)

[5.1 バックアップ・リストア 38](#_Toc83023642)

[5.1.1 バックアップ 38](#_Toc83023643)

[5.1.2 リストア 38](#_Toc83023644)

[5.2 リソース監視 39](#_Toc83023645)

[5.2.1 リソース監視方式 39](#_Toc83023646)

[5.2.2 メトリック保存期間 39](#_Toc83023647)

[5.2.3 リソース監視状況確認方法 39](#_Toc83023648)

[5.2.4 リソース監視項目 39](#_Toc83023649)

[5.2.5 しきい値監視 54](#_Toc83023650)

[5.3 ログ管理 55](#_Toc83023651)

[5.3.1 ログ保存期間 55](#_Toc83023652)

[5.3.2 ログ保存先 55](#_Toc83023653)

[5.3.3 ログ保存方法 56](#_Toc83023654)

[5.3.4 ログ一覧 56](#_Toc83023655)

[5.3.5 ログ監視 59](#_Toc83023656)

[5.4 時刻同期 59](#_Toc83023657)

[5.5 ソフトウェアのアップデート 59](#_Toc83023658)

[5.6 アラート通知先 59](#_Toc83023659)

[6 セキュリティ 60](#_Toc83023660)

[6.1 暗号化方針 60](#_Toc83023661)

[6.1.1 APサーバー(Azure Functions、Logic Apps) 60](#_Toc83023662)

[6.1.2 DBサーバー(Azure SQL Database) 60](#_Toc83023663)

[6.1.3 ストレージ(Azure Storage) 60](#_Toc83023664)

[6.1.4 ストレージ(Azure Storage) 60](#_Toc83023665)

[6.2 Webアクセス 61](#_Toc83023666)

[6.2.1 API Management 61](#_Toc83023667)

[6.2.1 Front Door 63](#_Toc83023668)

[6.2.2 Azure Web Application Firewall 68](#_Toc83023669)

# はじめに

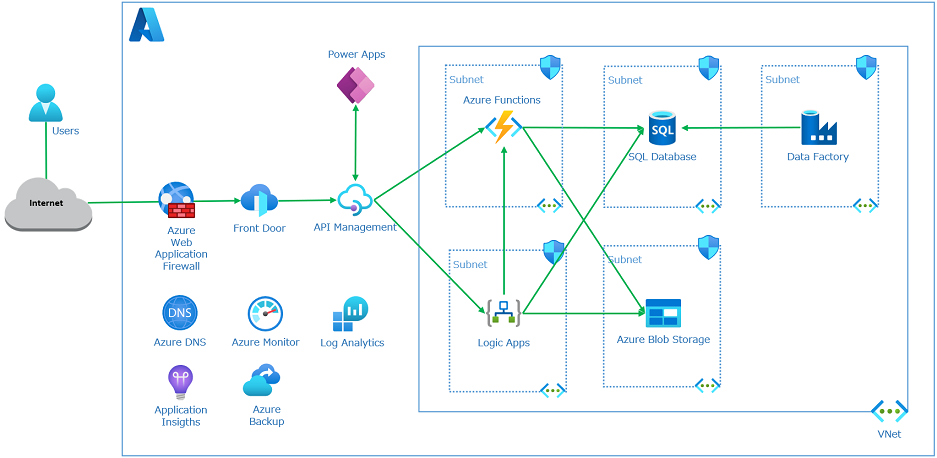
本書はLMS準備システム インフラ環境(以下、本システム)の構成、機能の実現方法、及び運用方式について記載する。

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。 |
| Application Insigths |  | 実行中のアプリケーションを監視することができる。 パフォーマンスの異常を自動的に検出し、組み込まれている強力な分析ツールを使用して、問題を診断し、ユーザーがアプリを使用して実行している操作を把握できる。 |
| Azure Backup |  | バックアップ ストレージのニーズに基づいてスケーラブルな、コスト効率の高い、セキュリティで保護された、ワンクリックで利用できるバックアップ ソリューション。 |
| 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 DNS |  | Azure DNS は、DNS ドメインのホスティング サービスであり、Microsoft Azure インフラストラクチャを使用した名前解決を提供する。 Azure でドメインをホストすることで、その他の Azure サービスと同じ資格情報、API、ツール、課金情報を使用して DNS レコードを管理できる。 |
| 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。 |
| Data Factory |  | フル マネージドのサーバーレス データ統合サービス。組み込みのコネクタを使用して、データ ソースを視覚的に統合できる。直感的な環境でコードなしで ETL および ELT プロセスを簡単に構築することも、独自のコードを書くこともできる。 |
| 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、Logic Apps)

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

#### Azure Functions

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

SQL DatabaseやBlob Storageにプライベートネットワークで接続するためにVNet統合を使用する。

VNet統合を使用する場合はApp Serviceプラン、もしくはFunctions Premiumを選択する必要があるが、本システムではApp Seviceプランを採用し、パフォーマンスに問題が生じた場合にFunctions Premiumの採用を検討する。

App Serviceプランはシングルインスタンスデプロイのため、クライアントがセッションの有効期間を通して同じインスタンスにルーティングされるARRアフィニティは使用しない。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 本番環境 | 検証環境 | 備考 |
| 関数アプリ名 | prod-ymhlms-functionapp | stg-ymhlms-functionapp | 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 | コード | 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 | Node.js | Node.js | 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 | 14LTS | 14LTS | 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。 |
| ストレージアカウント | prodymhlmsstorageaccount | stgymhlmsstorageaccount | 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。 |
| オペレーティングシステム | Windows | Windows | 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 | App Serviceプラン | App Serviceプラン | 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 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。 |
| プラン名 | prod-ymhlms-asp | stg-ymhlms-asp | プラン名を指定。 |
| SKUとサイズ | Standard S1  コア数：1  RAM：1.75GB  ストレージ：50GB | Standard S1  コア数：1  RAM：1.75GB  ストレージ：50GB | 実行環境のスペックを指定。 |
| ネットワーク インジェクションを有効にする |  |  | App Service 関数アプリは、インターネットに公開された、または Azure 仮想ネットワークに分離された受信アドレスを使用してプロビジョニングできる。App Service 関数アプリは、送信トラフィックを使用してプロビジョニングすることもでき |
| Application Insights | はい | はい | 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。 |
| VNet統合 | 以下サブネットに接続する。  App Service用サブネット | 以下サブネットに接続する。  App Service用サブネット |  |

#### Logic Apps

以下にLogic Appsの定義を示す。

SQL DatabaseやBlob Storageにプライベートネットワークで接続するために仮想ネットワークに接続する。

仮想ネットワークに接続する場合「統合サービス環境で消費タイプのロジックアプリを作成する」、または「Standardタイプを指定する」必要がある。統合サービス環境はグローバルなマルチテナントLogic Appsサービスから分離された専用のストレージや他のリソースを使用する環境であり、高度なパフォーマンスが要求されるシステムの場合に使用する。

本システムでは、Standardタイプを使用し、パフォーマンスに問題が生じた場合に統合サービス環境の使用を検討する。

Standardタイプはシングルインスタンスデプロイのため、クライアントがセッションの有効期間を通して同じインスタンスにルーティングされるARRアフィニティは使用しない。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 本番環境 | 検証環境 | 備考 |
| タイプ | Standard | Standard | リソースに使用するロジック アプリのリソースの種類と課金モデルを指定する。  消費:  グローバルなマルチテナント Azure Logic Apps で実行され、従量課金モデルを使用する。  Standard:  シングルテナントAzure Logic Apps で実行され、標準課金モデルを使用する。 |
| ロジックアプリ名 | prod-ymhlms-logicapp | stg-ymhlms-logicapp | リージョン全体で一意の名前を2文字以上で指定する。  有効な文字は以下の通りである。  文字、数字、ハイフン (-)、アンダースコア (\_)、かっこ ((、))、ピリオド (.) |
| 公開 | ワークフロー | ワークフロー | タスクをコンテナーで実行する場合はDockerコンテナーを指定する。 |
| ストレージアカウント | prodymhlmsstorageaccount | stgymhlmsstorageaccount | ロジックアプリを作成する場合は、Blob、キュー、テーブル ストレージをサポートする汎用 Azure Storageアカウントを指定する必要がある。 |
| プランの種類 | ワークフロー Standard | ワークフロー Standard | 最小コストのサーバーレスおよびイベントドリブン スケーリングに対しては [従量課金]、イベントベース スケーリングおよびネットワーク分離を備えたエンタープライズレベルのサーバーレスアプリケーションに対しては [Premium]、既存の App Serviceプランからのコンピューティングを再利用するには [App Service プラン] を選択する。 |
| プラン名 | prod-ymhlms-ws | stg-ymhlms-ws | プラン名を指定。 |
| SKUとサイズ | Standard WS1  コア数：1  RAM：3.5GB | Standard WS1  コア数：1  RAM：3.5GB | 実行環境のスペックを指定。 |
| Application Insights | いいえ | いいえ | 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。 |
| VNet統合 | 以下サブネットに接続する。  APサーバー用サブネット | 以下サブネットに接続する。  APサーバー用サブネット |  |

### 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。 |

#### SQL Server

以下にSQL Serverの定義を示す。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | 本番環境 | 検証環境 | 備考 |
| サーバーの詳細 | | 名前と場所の指定を含め、このサーバーに必要な設定を入力する。 | | |
|  | サーバー名 | prod-ymhlms-sqlserver | stg-ymhlms-sqlserver | サーバーの名前を指定する。命名規則は以下の通り。  ・サーバー名には、小文字、数字、および '-' だけを使用できる。  ・先頭と末尾を '-' にすることはできず、63 文字を超えることもできない。 |
| 管理者アカウント | |  |  |  |
|  | サーバー管理者ログイン | admin | admin | 管理者アカウント名 |
|  | パスワード |  |  | 管理者アカウントのパスワード |
| ファイアウォール規則 | | サーバーのネットワーク アクセスを構成する。 | | |
|  | Azure サービスおよびリソースにこのサーバーへのアクセスを許可する | admin | admin | 管理者アカウント名 |
| Azure Defender for SQL | | Azure Defender for SQL を使用してデータを保護する。脆弱性評価と Advanced Threat Protection を含む、サーバー用の統合セキュリティ パッケージ。 | | |
|  | Azure Defender for SQL の有効化 | 有効 | 有効 | データベースの潜在的な脆弱性の検出と軽減、データベースへの脅威を示す可能性がある異常なアクティビティの検出を行うための統合セキュリティ パッケージ。 |

#### SQL Database

以下にAzure SQL Databaseの定義を示す。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | 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 | | prod-ymhlms-database | stg-ymhlms-database |  |
|  | サーバー | | prod-ymhlms-sqlserver | stg-ymhlms-sqlserver |  |
|  | 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(Azure Storage)

本システムではストレージとしてAzure Storage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。 |

#### BLOBストレージ

|  |  |  |
| --- | --- | --- |
| 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。 |

#### Azure Files

|  |  |
| --- | --- |
| 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。 |

### データ統合サーバー(Data Factory)

本システムではデータ統合サーバーとしてData Factoryを使用する。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 本番環境 | 検証環境 | 備考 |
| 名前 | prod-ymhlms-datafactory | stg-ymhlms-datafactory | Microsoft Azure 全体で一意の名前を指定する。 命名規則は以下の通り。  ・名前は3～63文字の長さにする。  ・大文字と小文字を区別されない。  ・英文字または数字で始まり、英文字、数字、ダッシュ (-) 文字のみを含めることができる。  ・すべてのダッシュ (-) 文字は、その直前または直後に文字または数字が使用されている必要がある。  ・連続するダッシュ文字はコンテナー名では使用できない。 |
| バージョン | V2 | V2 | 最新バージョンを指定する。 |
| ネットワーク | 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のどちらを使用してセルフホステッド統合ランタイムを Azure Data Factory に接続するかを選択する。これは、オンプレミスまたはカスタマー マネージド Azure 仮想ネットワークのいずれかで実行されているセルフホステッド統合ランタイムに適用される。 |
| カスタマー マネージド キーを使用して暗号化を有効にする | チェックしない | チェックしない | 既定では、データは Microsoft マネージド キーで暗号化される。暗号化キーをさらに制御するために、BLOB およびファイル データの暗号化に使用するカスタマー マネージド キーを指定できる。 |

## 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  (本システムは単一仮想ネットワーク構成のため、仮想ネットワークをまたいだネットワーク接続ポリシーの管理は不要) | | 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。サブスクリプションと仮想ネットワークをまたいでアプリケーションとネットワークの接続ポリシーを一元的に作成、適用、記録できる。 |

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 | サブネットの委任 | プライベートエンドポイント |
| App Service用サブネット | prod-ymhlms-appservice-subnet | 172.16.0.0/24 | Microsoft.Web/serverFarms |  |
| Workflow Service用サブネット | prod-ymhlms-workflowservice-subnet | 172.16.1.0/24 |  |  |
| SQL Database用サブネット | prod-ymhlms-sqldatabase-subnet | 172.16.2.0/27 |  | SQL Database用  プライベートエンドポイント |
| ストレージアカウント用サブネット | prod-ymhlms-storageaccount-subnet | 172.16.2.32/27 |  | ストレージアカウント用  プライベートエンドポイント |
| データ統合サーバー用サブネット | prod-ymhlms-datafactory-subnet | 172.16.2.64/27 |  |  |

#### 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 | サブネットの委任 | プライベートエンドポイント |
| App Service用サブネット | stg-ymhlms-appservice-subnet | 172.17.0.0/24 | Microsoft.Web/serverFarms |  |
| Workflow Service用サブネット | stg-ymhlms-workflowservice-subnet | 172.17.1.0/24 |  |  |
| SQL Database用サブネット | stg-ymhlms-sqldatabase-subnet | 172.17.2.0/27 |  | SQL Database用  プライベートエンドポイント |
| ストレージアカウント用サブネット | stg-ymhlms-storageaccount-subnet | 172.17.2.32/27 |  | ストレージアカウント用  プライベートエンドポイント |
| データ統合サーバー用サブネット | stg-ymhlms-datafactory-subnet | 172.17.2.64/27 |  |  |

### 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 | App Service用NSG | | | | | |
| NSG名 | prod-ymhlms-appservice-nsg | | | | | |
| 割当先サブネット | App Service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 |
| 100 | 80 | TCP | ApiManagement | VirtualNetwork | Allow |
| 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 | Workflow Service用NSG | | | | | |
| NSG名 | prod-ymhlms-workflowservice-nsg | | | | | |
| 割当先サブネット | Workflow Service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 |
| 100 | 80 | TCP | ApiManagement | VirtualNetwork | Allow |
| 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 |
| - | - | - | - | - | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | データ統合サーバー用NSG | | | | | |
| NSG名 | prod-ymhlms-datafactory-nsg | | | | | |
| 割当先サブネット | データ統合サーバー用サブネット | | | | | |
| 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 | APサーバー用NSG | | | | | |
| NSG名 | stg-ymhlms-appservice-nsg | | | | | |
| 割当先サブネット | App Service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 |
| 100 | 80 | TCP | ApiManagement | VirtualNetwork | Allow |
| 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 | Workflow Service用NSG | | | | | |
| NSG名 | stg-ymhlms-workflowservice-nsg | | | | | |
| 割当先サブネット | Workflow Service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 |
| 100 | 80 | TCP | ApiManagement | VirtualNetwork | Allow |
| 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 |
| - | - | - | - | - | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NSG | データ統合サーバー用NSG | | | | | |
| NSG名 | stg-ymhlms-datafactory-nsg | | | | | |
| 割当先サブネット | データ統合サーバー用サブネット | | | | | |
| 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 |

#### 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プライベートエンドポイントのIPv4アドレス)/32 | (SQL Databaseプライベートエンドポイントの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 | | 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プライベートエンドポイントのIPv4アドレス)/32 | (ストレージアカウントプライベートエンドポイントの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Microsoftが管理・提供するAzureクラウドプラットフォーム上で実行される。

本システムは東日本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。

Azureクラウドプラットフォームは回復性のあるプラットフォームを提供し、ユーザーのすべてのワークロードに対する組織の信頼性の目標を達成する。ユーザーはミッションクリティカルなアプリケーションを自信を持って設計および運用することができる。Azureは透明性を重視しており、サービスの問題が発生しても常に情報を把握し、迅速に対応することができる。

Azureは様々な高可用性、ディザスターリカバリー、バックアップの機能を提供する。ユーザーは用途に応じて最適なコンピューティング、ストレージ、地理的(ローカル、ゾーン、リージョン)の冗長性オプションを選択することができる。

Azure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 |
| 99.99% | API Management / Azure Blob Storage / Azure Web Application Firewall / Front Door / SQL Database |
| 99.95% | Azure Functions |
| 99.9% | Azure Monitor / Data Factory / Logic Apps / PowerApps |

## 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。

#### APサーバー(本番環境、検証環境共通)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サーバー | 対象リソース | 拡張方式 | 自動拡張/手動拡張 | 変更時サーバー停止 |
| APサーバー | CPU | インスタンスの追加 | 自動拡張 | 不要 |
|  | メモリ |  |  |  |

#### DBサーバー(本番環境)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サーバー | 対象リソース | 拡張方式 | 自動拡張/手動拡張 | 変更時サーバー停止 |
| DBサーバー | CPU | サーバーレベル、コンピューティングサイズの変更 | 手動拡張 | 平均で 4 秒未満、最大で30秒未満の停止が発生 |
|  | メモリ |  |
|  | I/Oスループット |  |
|  | ストレージ容量 | ストレージ容量の手動追加 |  | 不要 |

#### DBサーバー(検証環境)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サーバー | 対象リソース | 拡張方式 | 自動拡張/手動拡張 | 変更時サーバー停止 |
| DBサーバー | CPU | 最小仮想コア数 と 最大仮想コア数を指定する。指定範囲内で処理状況に応じて自動で拡張する。メモリと IO の上限は、指定された仮想コアの範囲に比例する。 | 自動拡張 | 最大仮想コア数（最大CPU、最大メモリ）の変更時に、平均で 4 秒未満、最大で30秒未満の停止が発生。  最小仮想コア数の変更時には停止は発生しない。 |
|  | メモリ |  |
|  | I/Oスループット |  |
|  | ストレージ容量 | ストレージ容量の手動追加 | 手動拡張 | 不要 |

#### ストレージ(本番環境、検証環境共通)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| サーバー | 対象リソース | 拡張方式 | 自動拡張/手動拡張 | 変更時サーバー停止 |
| BLOBストレージ | I/Oスループット | 自動拡張 | 自動拡張 | 不要 |
| ストレージ容量 |  |  |  |
| Azure Files | I/Oスループット |  |  |  |
|  | ストレージ容量 | なし。最大5TiB | - | - |

# 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 | バックアップ方式 | バックアップ保存先 | 暗号化 |
| SQL Database(短期保有) | 35日  (最大35日) | 差分バックアップ | BLOBストレージ | 6.1暗号化方針を参照 |
| SQL Database(長期保有) | -  (最大10年) | - |  |  |
| ストレージ | 35日  (最大360日) | 完全バックアップ | バックアップコンテナー |  |

### リストア

|  |  |  |  |
| --- | --- | --- | --- |
| 対象 | リストア方式 | 復旧時点 | 復旧時間 |
| SQL Database(短期保有) | Azure Portalより、復元処理を実行する。 | 保存期間内の任意の時点 | 12時間未満 |
| ストレージ | バックアップが古いほど完了までの時間が長くなる。  データの復元にかかる時間は、復元期間中に行われた書き込み操作と削除操作の数に基づく。 たとえば、100 万オブジェクトを持つアカウントで毎日 3,000 オブジェクトが追加され、毎日 1,000 オブジェクトが削除される場合、過去 30 日間のポイントまで復元するのに約 2 時間必要になる。 |

## 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Azure Monitorサービスによりリソースを監視する。

### メトリック保存期間

メトリックの保存期間は標準で93日間である。

93日を超えてメトリックを保存する場合はLog Analyticsワークスペースやストレージアカウントに格納する必要がある。

|  |  |
| --- | --- |
| メトリック保存期間 | 確認後記載 |

### 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Azure Portal各サービスのメトリックページで確認する。

### リソース監視項目

本システムのリソース監視項目をサービス別に記載する。

#### API Management

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| CAPACITY | Capacity | ApiManagement サービスの使用率メトリック。 注: Premium 以外の SKU の場合、"Max" 集計では、値は 0 と表示される。 |
| EVENTHUB EVENTS | Dropped EventHub Events | キューのサイズ制限に達したためスキップされたイベントの数 |
| Failed EventHub Events | 失敗した EventHub イベントの数 |
|  | Rejected EventHub Events | 拒否された EventHub イベントの数 (誤った構成または未承認) |
|  | Size of EventHub Events | EventHub イベントの合計サイズ (バイト単位) |
|  | Successful EventHub Events | 成功した EventHub イベントの数 |
|  | Throttled EventHub Events | 調整された EventHub イベントの数 |
|  | Timed Out EventHub Events | タイムアウトした EventHub イベントの数 |
| GATEWAY REQUESTS | Duration of Backend Requests | バックエンド要求の期間 (ミリ秒) |
| Overall Duration of Gateway Requests | ゲートウェイ要求の全体の期間 (ミリ秒単位) |
|  | Requests | 複数のディメンションを持つゲートウェイ要求メトリック |

#### Application Insigths(ログベースメトリック)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| カスタム | HeartbeatState | ハートビートの状態。 |
| サーバー | Dependency calls | 依存関係呼び出しの数。 |
| Dependency duration | 依存関係呼び出しの期間。 |
|  | Server requests | Web アプリケーションによって受信された受信サーバー要求の数。 |
|  | Serve response time | サーバーが受信要求を処理するのにかかった時間。 |
| パフォーマンスカウンター | ASP.NET requests execution time | HTTP 要求実行時間。 |
|  | ASP.NET request rate | HTTP 要求率。 |
|  | ASP.NET request in application queue | アプリケーション キュー内の HTTP 要求。 |
|  | Available memory | 使用可能なメモリ。 |
|  | Exception rate | 例外レート。 |
|  | Process CPU | 監視対象のアプリをホストしているプロセスによって消費されるプロセッサの容量の合計を示す。 |
|  | Process CPU(all cores) | このメトリックは、監視対象のアプリをホストしているプロセスによって消費されるすべてのプロセッサの容量の合計を示します。 |
|  | Process IO rate | プロセス IO 量。 |
|  | Process private bytes | 監視対象プロセスによってデータに割り当てられた非共有メモリの量。 |
|  | Processor time | 監視対象のサーバー インスタンスで実行されている すべての プロセスによる CPU 使用量。 |
| ブラウザー | Browser page load time | ユーザーが要求を出してから DOM、スタイル シート、スクリプト、およびイメージが読み込まれるまでの時間。 |
|  | Client processing time | ドキュメントの最終バイトを受信してから、DOM が読み込まれるまでの時間。 非同期要求がまだ処理されている可能性がある。 |
|  | Page load network connect time | ユーザー要求からネットワーク接続までの時間。 DNS の参照とトランスポートの接続が含まれる。 |
|  | Receiving response time | 最初のバイトから最後のバイトまで、または切断までの時間。 |
|  | Send sequest time | ネットワーク接続から、最初のバイトを受信するまでの時間。 |
| 使い方 | Data point count | データポイントの数。 |
|  | Data point volume | データポイントの容量。 |
|  | Events | イベントの数。 |
|  | Page view load time | PageView イベントの読み込みにかかった時間。 |
|  | Page views | TrackPageView () Application Insights API でログに記録された PageView イベントの数。 |
|  | Sessions | 個別のセッション ID の数。 |
|  | Traces | TrackTrace () Application Insights API 呼び出しを使用してログに記録されたトレース ステートメントの数。 |
|  | Users | アプリケーションにアクセスした個別のユーザーの数。 テレメトリ サンプリングとフィルター処理を使用すると、このメトリックの精度が大幅に低下する可能性がある。 |
|  | Users,authenticated | アプリケーションに認証された個別のユーザーの数。 |
| 可用性 | Availability | 問題が検出されなかった Web テストの実行の割合を示す。 可能な最小値は 0 で、これはすべての Web テストの実行が失敗したことを示す。 値 100 は、すべての Web テストの実行が検証条件に合格したことを意味する。 |
|  | Availability test results count | Azure Monitor によって実行される Web テストの数。 |
|  | Test duration | Web テストの実行にかかった時間を示す。 複数ステップの Web テストの場合、メトリックには、すべてのステップの合計実行時間が反映される。 |
| 失敗 | Browser exceptions | ブラウザーで実行されているアプリケーション コードからスローされた例外の数。 メトリックには、trackException() Application Insights API 呼び出しで追跡される例外のみが含まれる。 |
|  | Dependency failures | 失敗した依存関係呼び出しの数。 |
|  | Exceptions | Application Insights に例外を記録するたびに、SDK のtrackexception () メソッドが呼び出される。 例外メトリックは、ログに記録された例外の数を示す。 |
|  | Failed requests | 失敗 としてマークされた追跡されたサーバー要求の数。 既定では、Application Insights SDK は HTTP 応答コード 5xx または 4xx を返した各サーバー要求を、失敗した要求として自動的にマークする。 このロジックをカスタマイズするには、カスタムのテレメトリ初期化子の要求テレメトリ項目の success プロパティを変更する。 |
|  | Server exceptions | サーバーの例外の数を示す。 |

#### Application Insigths(標準メトリック)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| サーバー | Dependency calls | 外部リソースに対するアプリケーションからの呼び出しの数。 |
|  | Depedency duration | 外部リソースに対するアプリケーションからの呼び出しの期間。 |
|  | Server request rate | 1 秒あたりのサーバー要求数による率。 |
|  | Server requests | 完了した HTTP 要求の数。 |
|  | Server response time | HTTP 要求を受信してから、応答の送信を終了するまでの時間。 |
| パフォーマンスカウンター | Available memory | プロセスへの割り当てまたはシステムの使用にすぐに利用可能な物理メモリ。 |
|  | Exception rate | .NET 例外、および .NET 例外に変換されたアンマネージ例外を含む、Windows に報告された処理済み例外と未処理の例外の数。 |
|  | HTTP request execution time | 最新の要求の実行時間。 |
|  | HTTP request rate | ASP.NET からの 1 秒あたりのアプリケーションへのすべての要求のレート。 |
|  | HTTP requests in application queue | アプリケーション要求キューの長さ。 |
|  | Process CPU | すべてのプロセス スレッドで命令を実行するためにプロセッサを使用した経過時間の割合。 これは 0 から 100 の間で変化することがある。 このメトリックは、w3wp プロセスのみのパフォーマンスを示す。 |
|  | Process IO rate | ファイル、ネットワーク、およびデバイスに対する読み書きで 1 秒あたりに処理される合計バイト数。 |
|  | Process private bytes | 監視対象のアプリケーション プロセスに対して専用に割り当てられるメモリ。 |
|  | Processor time | プロセッサによって非アイドル スレッドで費やされる時間の割合。 |
| ブラウザー | Browser page load time | ユーザーが要求を出してから DOM、スタイル シート、スクリプト、およびイメージが読み込まれるまでの時間。 |
|  | Client processing time | ドキュメントの最終バイトを受信してから、DOM が読み込まれるまでの時間。 非同期要求がまだ処理されている可能性がある。 |
|  | Page load network connect time | ユーザー要求からネットワーク接続までの時間。 DNS の参照とトランスポートの接続が含まれる。 |
|  | Receiving response time | 最初のバイトから最後のバイトまで、または切断までの時間。 |
|  | Send request time | ネットワーク接続から、最初のバイトを受信するまでの時間。 |
| 使い方 | Page view load time | ページ ビューの読み込み時間。 |
|  | Page views | ページ ビューの数。 |
|  | Traces | トレース ドキュメント数。 |
| 可用性 | Availability | 正常に完了した可用性テストの割合。 |
|  | Availability test duration | 可用性テスト継続時間。 |
|  | Availability tests | 可用性テストの数。 |
| 失敗 | Browser exceptions | ブラウザーでスローされた、キャッチされない例外の数。 |
|  | Dependency call failures | 外部リソースに対するアプリケーションからの失敗した依存関係呼び出しの数。 |
|  | Exceptions | キャッチされていないすべての例外の合計数。 |
|  | Failed requests | 失敗としてマークされた HTTP 要求の数。 ほとんどの場合、応答コードが 400 以上で、かつ 401 に等しくない要求。 |
|  | Server exceptions | サーバー アプリケーションでスローされ、キャッチされていない例外の数。 |

#### ストレージアカウント(アカウント)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| CAPACITY | Used capacity | アカウントの使用済み容量 |
| TRANSACTION | Availability | ストレージ サービスまたは指定された API 操作の可用性の割合。 可用性は、TotalBillableRequests の値を取得し、それを該当する要求の数 (予期しないエラーが発生した要求を含む) で割ることによって、計算される。 予期しないエラーすべてが、ストレージ サービスまたは指定された API 操作の可用性の低下をもたらす。 |
|  | Egress | エグレス データの量。 この数値には、Azure Storage から外部クライアントへのエグレスおよび Azure 内でのエグレスが含まれる。 したがって、この値には、課金対象のエグレスが反映されない。 |
|  | Ingress | イングレス データの量 (バイト単位)。 この値には、外部クライアントから Azure Storage へのイングレスおよび Azure 内でのイングレスが含まれる。 |
|  | Success E2E Latency | ストレージ サービスまたは指定された API 操作に対して行われた成功した要求の平均エンド ツー エンド待機時間 (ミリ秒単位)。 この値には、要求の読み取り、応答の送信、および応答の受信確認を受け取るために Azure Storage 内で必要な処理時間が含まれる。 |
|  | Success Server Latency | 成功した要求の処理に Azure Storage が使った待機時間 (ミリ秒単位)。 この値には、SuccessE2ELatency で指定されているネットワーク待機時間は含まれない。 |
|  | Transactions | ストレージ サービスまたは指定された API 操作に対して行われた要求の数。 この数には、成功した要求と失敗した要求およびエラーが発生した要求が含まれる。 別の種類の応答の数には ResponseType ディメンションを使う。 |

#### ストレージアカウント(BLOB)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| CAPACITY | Blob Capacity | ストレージ アカウントの Blob service によって使われているストレージの量 (バイト単位)。 |
|  | Blob Container Count | ストレージ アカウントの Blob service 内のコンテナーの数。 |
|  | Blob Count | ストレージ アカウントの Blob service 内の BLOB の数。 |
|  | Index Capacity | ADLS Gen2 (階層構造) インデックスで使用されるストレージの容量 (バイト単位)。 |
| TRANSACTION | Availability | ストレージ サービスまたは指定された API 操作の可用性の割合。 可用性は、TotalBillableRequests の値を取得し、それを該当する要求の数 (予期しないエラーが発生した要求を含む) で割ることによって、計算される。 予期しないエラーすべてが、ストレージ サービスまたは指定された API 操作の可用性の低下をもたらす。 |
|  | Egress | エグレス データの量 (バイト単位)。 この値には、外部クライアントから Azure Storage へのエグレスおよび Azure 内でのエグレスが含まれる。 したがって、この値には、課金対象のエグレスが反映されない。 |
|  | Ingress | イングレス データの量 (バイト単位)。 この値には、外部クライアントから Azure Storage へのイングレスおよび Azure 内でのイングレスが含まれる。 |
|  | Success E2E Latency | ストレージ サービスまたは指定された API 操作に対して行われた成功した要求のエンド ツー エンド待機時間 (ミリ秒単位)。 この値には、要求の読み取り、応答の送信、および応答の受信確認を受け取るために Azure Storage 内で必要な処理時間が含まれる。 |
|  | Success Server Latency | 成功した要求の処理に Azure Storage が使った待機時間 (ミリ秒単位)。 この値には、SuccessE2ELatency で指定されているネットワーク待機時間は含まれない。 |
|  | Transactions | ストレージ サービスまたは指定された API 操作に対して行われた要求の数。 この数には、成功した要求と失敗した要求およびエラーが発生した要求が含まれる。 別の種類の応答の数には ResponseType ディメンションを使う。 |

#### ストレージアカウント(ファイル)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| CAPACITY | File Capacity | ストレージ アカウントの File サービスによって使用されているストレージの量 (バイト単位)。 |
|  | File Count | ストレージ アカウントの File サービス内のファイルの数。 |
|  | File Share Capacity Quota | Azure Files サービスで使用できる記憶域の容量の上限 (バイト単位)。 |
|  | File Share Count | ストレージ アカウントの File サービス内のファイル共有の数。 |
|  | File Share Snapshot Count | ストレージ アカウントの Files サービス内の共有に存在するスナップショットの数。 |
|  | File Share Snapshot Size | ストレージ アカウントの Files サービスのスナップショットによって使用されている記憶域の容量 (バイト単位)。 |
| TRANSACTION | Availability | ストレージ サービスまたは指定された API 操作の可用性の割合。 可用性は、TotalBillableRequests の値を取得し、それを該当する要求の数 (予期しないエラーが発生した要求を含む) で割ることによって、計算される。 予期しないエラーすべてが、ストレージ サービスまたは指定された API 操作の可用性の低下をもたらす。 |
|  | Egress | エグレス データの量 (バイト単位)。 この値には、外部クライアントから Azure Storage へのエグレスおよび Azure 内でのエグレスが含まれる。 したがって、この値には、課金対象のエグレスが反映されない。 |
|  | Ingress | イングレス データの量 (バイト単位)。 この値には、外部クライアントから Azure Storage へのイングレスおよび Azure 内でのイングレスが含まれる。 |
|  | Success E2E Latency | ストレージ サービスまたは指定された API 操作に対して行われた成功した要求のエンド ツー エンド待機時間 (ミリ秒単位)。 この値には、要求の読み取り、応答の送信、および応答の受信確認を受け取るために Azure Storage 内で必要な処理時間が含まれる。 |
|  | Success Server Latency | 成功した要求の処理に Azure Storage が使った待機時間 (ミリ秒単位)。 この値には、SuccessE2ELatency で指定されているネットワーク待機時間は含まれない。 |
|  | Transactions | ストレージ サービスまたは指定された API 操作に対して行われた要求の数。 この数には、成功した要求と失敗した要求およびエラーが発生した要求が含まれる。 別の種類の応答の数には ResponseType ディメンションを使う。 |

#### Azure DNS(DNSゾーン)

|  |  |
| --- | --- |
| メトリック | 内容 |
| Query Volume | DNS ゾーンで処理されたクエリの数 |
| Record Set Capacity Utilization | DNS ゾーンで使用されるレコード セットの容量の割合 |
| Record Set Count | DNS ゾーンのレコード セットの数 |

#### Azure Functions(App Serviceプラン)

|  |  |
| --- | --- |
| メトリック | 内容 |
| CPU Percentage | プランの全インスタンスで使用された平均 CPU。 |
| Data In | プランの全インスタンスで使用された平均受信帯域幅。 |
| Data Out | プランの全インスタンスで使用された平均送信帯域幅。 |
| Disk Queue Length | ストレージのキューに登録された読み取り要求と書き込み要求の平均数。 ディスク キューが長いときは、過剰なディスク I/O のためにアプリの速度が低下している可能性があることを示している。 |
| Established Socket Count for Outbound Requests | プランのすべてのインスタンスで送信接続に使用される ESTABLISHED 状態のソケットの平均数。 |
| Http Queue Length | 処理される前にキューで待つ必要があった HTTP 要求の平均数。 HTTP キューが長いこと、または HTTP キューの長さが増加していることは、プランに大きな負荷がかかっている。 |
| Memory Percentage | プランの全インスタンスで使用された平均メモリ。 |
| Socket Count for Inbound Requests | プランのすべてのインスタンスで受信 HTTP 要求に使用されるソケットの平均数。 |
| Socket Count for Loopback Connections | プランのすべてのインスタンスでループバック接続に使用されるソケットの平均数。 |
| Socket Count of Outbound Requests | TCP の状態にかかわらず、プランのすべてのインスタンスで送信接続に使用されるソケットの平均数。 送信接続が多すぎると、接続エラーが発生する場合がある。 |
| TCP Close Wait | プランのすべてのインスタンスで CLOSE\_WAIT 状態のソケットの平均数。 |
| TCP Closing | プランのすべてのインスタンスで CLOSING 状態のソケットの平均数。 |
| TCP Established | プランのすべてのインスタンスで ESTABLISHED 状態のソケットの平均数。 |
| TCP Fin Wait 1 | プランのすべてのインスタンスで FIN\_WAIT\_1 状態のソケットの平均数。 |
| TCP Fin Wait 2 | プランのすべてのインスタンスで FIN\_WAIT\_2 状態のソケットの平均数。 |
| TCP Last Ack | プランのすべてのインスタンスで LAST\_ACK 状態のソケットの平均数。 |
| TCP Syn Received | プランのすべてのインスタンスで SYN\_RCVD 状態のソケットの平均数。 |
| TCP Syn Sent | プランのすべてのインスタンスで SYN\_SENT 状態のソケットの平均数。 |
| TCP Time Wait | プランのすべてのインスタンスで TIME\_WAIT 状態のソケットの平均数。 |
| Time Wait Socket Count for Outbound Requests | プランのすべてのインスタンスで送信接続に使用される TIME\_WAIT 状態のソケットの平均数。 TIME\_WAIT 状態の送信ソケット数が多い場合、または増加している場合は、接続エラーが発生することがある。 |

#### Azure Functions(Function App)

|  |  |
| --- | --- |
| メトリック | 内容 |
| Average memory working set | アプリで使用された平均メモリ量 (メガバイト (MiB))。 |
| Connections | サンドボックス内に存在するバインドされたソケットの数 (w3wp.exe とその子プロセス)。 バインドされたソケットは、bind()/connect() API の呼び出しによって作成され、対象のソケットが CloseHandle()/closesocket() で閉じられるまで残る。 |
| Current Assemblies | このアプリケーション内のすべての AppDomain で読み込まれたアセンブリの現在の数。 |
| Data In | アプリで消費された受信帯域幅の量 (MiB)。 |
| Data Out | アプリで消費された送信帯域幅の量 (MiB)。 |
| File System Usage | アプリによって使用されたファイル システム クォータの割合。 |
| Function Execution Count | 関数の実行回数。 |
| Function Execution Units | 関数の実行単位。 |
| Gen 0 Garbage Collections | アプリ プロセスが開始されてからジェネレーション 0 オブジェクトがガベージ コレクションされた回数。 上位のジェネレーションの GC には、下位のジェネレーションの GC がすべて含まれる。 |
| Gen 1 Garbage Collections | アプリ プロセスが開始されてからジェネレーション 1 オブジェクトがガベージ コレクションされた回数。 上位のジェネレーションの GC には、下位のジェネレーションの GC がすべて含まれる。 |
| Gen 2 Garbage Collections | アプリ プロセスが開始されてからジェネレーション 2 オブジェクトがガベージ コレクションされた回数。 |
| Handle Count | アプリ プロセスによって現在開かれているハンドルの合計数。 |
| Health check status | 正常性チェックの状態。 |
| Http 101 | HTTP 状態コード 101 が結果として返された要求の数。 |
| Http 2xx | 200 以上 300 未満の HTTP 状態コードが結果として返された要求の数。 |
| Http 3xx | 300 以上 400 未満の HTTP 状態コードが結果として返された要求の数。 |
| Http 401 | HTTP 401 状態コードが結果として返された要求の数。 |
| Http 403 | HTTP 403 状態コードが結果として返された要求の数。 |
| Http 404 | HTTP 404 状態コードが結果として返された要求の数。 |
| Http 406 | HTTP 406 状態コードが結果として返された要求の数。 |
| Http 4xx | 400 以上 500 未満の HTTP 状態コードが結果として返された要求の数。 |
| Http Server Errors | アプリが要求に応答するのに要した時間 (秒単位)。 |
| IO Other Bytes Per Second | アプリ プロセスがデータを含まない I/O 操作 (制御操作など) にバイトを発行している速度。 |
| IO Other Operations Per Second | アプリ プロセスが読み取りまたは書き込み操作ではない I/O 操作を発行している速度。 |
| IO Read Bytes Per Second | アプリ プロセスが I/O 操作からバイトを読み取っている速度。 |
| IO Read Operations Per Second | アプリ プロセスが読み取り I/O 操作を発行している速度。 |
| IO Write Bytes Per Second | アプリ プロセスが I/O 操作にバイトを書き込んでいる速度。 |
| IO Write Operations Per Second | アプリ プロセスが書き込み I/O 操作を発行している速度。 |
| Memory working set | アプリで使用されている現在のメモリ量 (MiB)。 |
| Private Bytes | プライベート バイトは、アプリ プロセスによって割り当てられた、他のプロセスとは共有できないメモリの現在のサイズ (バイト単位) 。 |
| Requests | 結果として返された HTTP 状態コードを問わない、要求の合計数。 |
| Requests In Application Queue | アプリケーション要求キュー内の要求の数。 |
| Response Time | アプリが要求に応答するのに要した平均時間 (秒単位)。 |
| Thread Count | アプリ プロセス内で現在アクティブなスレッドの数。 |
| Total App Domains | 現在このアプリケーションに読み込まれている AppDomain の数。 |
| Total App Domains Unloaded | アプリケーションの開始以降にアンロードされた AppDomain の合計数。 |

#### データ統合サーバー(Data Factory)

|  |  |
| --- | --- |
| メトリック | 内容 |
| Cancelled activity runs metrics | キャンセルしたアクティビティの実行回数。 |
| Cancelled pipeline runs metrics | キャンセルしたパイプライン実行回数。 |
| Canncelled SSIS integration runtime start metrics | キャンセルされた SSIS 統合ランタイム開始回数。 |
| Cancelled SSIS package execution metrics | キャンセルされた SSIS パッケージ実行回数。 |
| Cancelled trigger runs metrics | キャンセルしたトリガー実行の回数。 |
| Elapsed Time Pipeline Runs Metrics | パイプライン実行経過時間。 |
| Failed activity runs metrics | 失敗したアクティビティ実行回数。 |
| Failed pipeline runs metrics | 失敗したパイプライン実行回数。 |
| Failed SSIS integration runtime start metrics | 失敗した SSIS 統合ランタイム開始回数。 |
| Failed SSIS package execution metrics | 失敗した SSIS パッケージ実行回数。 |
| Failed trigger runs metrics | 失敗したトリガー実行の回数。 |
| Integration runtime available memory | 統合実行時に使用可能なメモリ。 |
| Integration runtime available node count | 統合ランタイムの使用可能なノード数。 |
| Integration runtime CPU utilization | 統合実行時の CPU 使用率。 |
| Integration runtime queue duration | 統合ランタイム キューの期間。 |
| Integration runtime queue length | 統合ランタイム キューの長さ。 |
| Maximum allowed entities count | 許可されているエンティティの最大数。 |
| Maximum allowed factory size (GB unit) | 許可されている最大の工場出荷時サイズ (GB 単位)。 |
| Stuck SSIS integration runtime stop metrics | 停止した SSIS 統合ランタイム停止回数。 |
| Succeeded activity runs metrics | 成功したアクティビティ実行回数。 |
| Succeeded pipeline runs metrics | 成功したパイプライン実行回数。 |
| Succeeded SSIS integration runtime start metrics | 成功した SSIS 統合ランタイム開始回数。 |
| Succeeded SSIS integration runtime stop metrics | 成功した SSIS 統合ランタイム停止回数。 |
| Succeeded SSIS package execution metrics | 成功した SSIS パッケージ実行回数。 |
| Succeeded trigger runs metrics | 成功したトリガー実行の回数。 |
| Total entities count | エンティティの合計数。 |
| Total factory size (GB unit) | 合計の工場出荷時サイズ (GB 単位)。 |

#### Front Door

|  |  |
| --- | --- |
| メトリック | 内容 |
| Backend Health Percentage | HTTP/S プロキシからバックエンドへの成功した正常性プローブの割合。 |
| Backend Request Count | バックエンドに HTTP/S プロキシから送信された要求の数。 |
| Backend Request Latency | HTTP/S プロキシによってバックエンドに要求が送信されてから、HTTP/S プロキシでバックエンドから最後の応答バイトが受信されるまでの算出時間。 |
| Billable Response Size | HTTP/S プロキシからクライアントへの応答として送信された、課金対象のバイト数 (要求あたり最小 2 KB)。 |
| Request Count | HTTP/S プロキシによって処理されるクライアント要求の数。 |
| Request Size | HTTP/S プロキシにクライアントからの要求として送信されたバイトの数。 |
| Response Size | クライアントに HTTP/S プロキシからの応答として送信されたバイトの数。 |
| Total Latency | HTTP/S プロキシによってクライアント要求が受信されてから、HTTP/S プロキシからの最後の応答バイトがクライアントで確認されるまでの算出時間。 |
| Web Application Firewall Request Count | Web アプリケーション ファイアウォールによって処理されるクライアント要求の数。 |

#### Logic Apps

|  |  |
| --- | --- |
| メトリック | 内容 |
| Action Latency | 完了したワークフロー アクションの待機時間。 |
| Action Success Latency | 成功したワークフロー アクションの待機時間。 |
| Action Throttled Events | ワークフロー アクション スロットル イベントの数。 |
| Actions Completed | 完了したワークフロー アクションの数。 |
| Actions Failed | 失敗したワークフロー アクションの数。 |
| Actions Skipped | スキップされたワークフロー アクションの数。 |
| Actions Started | 開始したワークフロー アクションの数。 |
| Actions Succeeded | 成功したワークフロー アクションの数。 |
| Billable Action Executions | 課金されるワークフロー アクションの実行数。 |
| Billable Trigger Executions | 課金されるワークフロー トリガーの実行数。 |
| Billing Usage for Native Operation Executions | 請求対象となるネイティブ操作の実行回数。 |
| Billing Usage for Standard Connector Executions | 請求対象となる Standard コネクタの実行回数。 |
| Billing Usage for Storage Consumption Executions | 請求対象となるストレージ使用の実行回数。 |
| Run Failure Percentage | 失敗したワークフロー実行の割合。 |
| Run Latency | 完了したワークフロー実行の待機時間。 |
| Run Stard Throttled Events | ワークフロー実行開始スロットル イベントの数。 |
| Run Success Latency | 成功したワークフロー実行の待機時間。 |
| Run Throttled Events | ワークフロー アクションまたはトリガー スロットル イベントの数。 |
| Runs Cancelled | キャンセルされたワークフロー実行の数。 |
| Runs Completed | 完了したワークフロー実行の数。 |
| Runs Failed | 失敗したワークフロー実行の数。 |
| Runs Started | 開始したワークフロー実行の数。 |
| Runs Succeeded | 成功したワークフロー実行の数。 |
| Total Billable Executions | 課金されるワークフローの実行数。 |
| Trigger Fire Latency | 起動されたワークフロー トリガーの待機時間。 |
| Trigger Latency | 完了したワークフロー トリガーの待機時間。 |
| Trigger Success Latency | 成功したワークフロー トリガーの待機時間。 |
| Trigger Throttled Events | ワークフロー トリガー スロットル イベントの数。 |
| Triggers Completed | 完了したワークフロー トリガーの数。 |
| Triggers Failed | 失敗したワークフロー トリガーの数。 |
| Triggers Fired | 起動されたワークフロー トリガーの数。 |
| Triggers Skipped | スキップされたワークフロー トリガーの数。 |
| Triggers Startd | 開始したワークフロー トリガーの数。 |
| Triggers Succeeded | 成功したワークフロー トリガーの数。 |

#### DBサーバー(本番環境SQL Database)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| BASIC | Blocked by Firewall | ファイアウォールによってブロックされたセッションの数。 |
|  | CPU limit | CPU 制限。 |
|  | CPU percentage | CPU の割合。 |
|  | CPU used | 使用された CPUの数。 |
|  | Data IO percentage | データ IO の割合。 |
|  | Data space allocated | 割り当て済みのデータ ストレージ。 |
|  | Data space used | 使用済みのデータ領域。 |
|  | Data space used percent | 使用済みのデータ領域の割合。 |
|  | Deadlocks | デッドロックの発生回数。 |
|  | Differential backup storage size | 累積的な差分バックアップ ストレージ サイズ。 |
|  | Failed Connections | 失敗した接続の数。 |
|  | Full backup storage size | 累積的な完全バックアップ ストレージ サイズ。 |
|  | In-Memory OLTP storage percent | インメモリ OLTP ストレージの割合。 |
|  | Log backup storage size | 累積的なログ バックアップ ストレージ サイズ。 |
|  | Log IO percentage | ログ IO の割合。 |
|  | Sessions percentage | セッションの割合。 |
|  | Successful Connections | 成功した接続の数。 |
|  | Workers percentage | ワーカーの割合。 |
| INSTANCEANDAPPADDVANCED | SQL Server process core percent | SQL DB プロセスに対する CPU 使用率 (%)。 |
|  | SQL Server process memory percent | SQL DB プロセスに対するメモリ使用率 (%)。 |
|  | Tempdb Data File Size Kilobytes | tempdb データ ファイルで使用されている領域 (キロバイト単位)。 |
|  | Tempdb Log File Size Kilobytes | tempdb トランザクション ログ ファイルで使用されている領域 (キロバイト単位)。 |
|  | Tempdb Percent Log Used | tempdb トランザクション ログ ファイルで使用されている領域の割合。 |

#### DBサーバー(検証環境SQL Database)

|  |  |  |
| --- | --- | --- |
| 種別 | メトリック | 内容 |
| BASIC | Blocked by Firewall | ファイアウォールによってブロックされたセッションの数。 |
|  | App CPU billed | 課金されるアプリ CPU。 |
|  | App CPU percentage | アプリ CPU の割合。 |
|  | App memory percentage | メモリの割合 (%)。 |
|  | Blocked by Firewall | ファイアウォールによってブロックされたセッションの数。 |
|  | CPU limit | CPU 制限。 |
|  | CPU percentage | CPU の割合。 |
|  | CPU used | 使用された CPUの数。 |
|  | Data IO percentage | データ IO の割合。 |
|  | Data space allocated | 割り当て済みのデータ ストレージ。 |
|  | Data space used | 使用済みのデータ領域。 |
|  | Data space used percent | 使用済みのデータ領域の割合。 |
|  | Deadlocks | デッドロックの発生回数。 |
|  | Differential backup storage size | 累積的な差分バックアップ ストレージ サイズ。 |
|  | Failed Connections | 失敗した接続の数。 |
|  | Full backup storage size | 累積的な完全バックアップ ストレージ サイズ。 |
|  | In-Memory OLTP storage percent | インメモリ OLTP ストレージの割合。 |
|  | Log backup storage size | 累積的なログ バックアップ ストレージ サイズ。 |
|  | Log IO percentage | ログ IO の割合。 |
|  | Sessions percentage | セッションの割合。 |
|  | Successful Connections | 成功した接続の数。 |
|  | Workers percentage | ワーカーの割合。 |
| INSTANCEANDAPPADDVANCED | SQL Server process core percent | SQL DB プロセスに対する CPU 使用率 (%)。 |
| SQL Server process memory percent | SQL DB プロセスに対するメモリ使用率 (%)。 |
|  | Tempdb Data File Size Kilobytes | tempdb データ ファイルで使用されている領域 (キロバイト単位)。 |
|  | Tempdb Log File Size Kilobytes | tempdb トランザクション ログ ファイルで使用されている領域 (キロバイト単位)。 |
|  | Tempdb Percent Log Used | tempdb トランザクション ログ ファイルで使用されている領域の割合。 |

#### VNet

|  |  |
| --- | --- |
| メトリック | 内容 |
| Failed Pings to a VM | 宛先 VM の送信された Ping の総数に対する失敗した Ping の数の割合 (%)。 |
| Inbound bytes DDos | DDoS 受信バイト数。 |
| Inbound bytes dropped DDos | DDoS 受信バイト破棄数。 |
| Inbound bytes forwarded DDos | DDoS 受信バイト転送数。 |
| Inbound packets DDos | DDoS 受信パケット数。 |
| Inbound packets dropped DDos | DDoS 受信パケット破棄数。 |
| Inbound packets forwarded DDos | DDoS 受信パケット転送数。 |
| Inbound SYN packets to trigger DDos mitigation | DDoS 軽減をトリガーする受信 SYN パケット数。 |
| Inbound TCP bytes DDos | DDoS 受信 TCP バイト数。 |
| Inbound TCP bytes dropped DDos | DDoS 受信 TCP バイト破棄数。 |
| Inbound TCP bytes forwarded DDos | DDoS 受信 TCP バイト転送数。 |
| Inbound TCP packets DDos | DDoS 受信 TCP パケット数。 |
| Inbound TCP packets dropped DDos | DDoS 受信 TCP パケット破棄数。 |
| Inbound TCP packets forwarded DDos | DDoS 受信 TCP パケット転送数。 |
| Inbound TCP packets to trigger DDos minigation | DDoS 軽減をトリガーする受信 TCP パケット数。 |
| Inbound UDP bytes DDos | DDoS 受信 UDP バイト数。 |
| Inbound UDP bytes dropped DDos | DDoS 受信 UDP バイト破棄数 |
| Inbound UDP bytes forwarded DDos | DDoS 受信 UDP バイト転送数。 |
| Inbound UDP packets DDos | DDoS 受信 UDP パケット数。 |
| Inbound UDP packets dropped DDos | DDoS 受信 UDP パケット破棄数。 |
| Inbound UDP packets forwarded DDos | DDoS 受信 UDP パケット転送数。 |
| Inbound UDP packets to trigger DDos minigation | DDoS 軽減をトリガーする受信 UDP パケット数。 |
| Rount trip time for Pings to a VM | 宛先 VM に送信された Ping のラウンド トリップ時間。 |
| Under DDos attack or not | DDoS 攻撃中かどうか。 |

### 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 | メトリック |
| APサーバー | CPU使用率 | 80%以上が15分 | メールによるアラート通知 | CPU Percentage |
|  | メモリ使用率 | 80%以上が5分 | (アラートの通知先は5.6アラート通知先を参照する。) | Memory Percentage |
| DBサーバー | CPU使用率 | 80%以上が15分 | SQL Server process core percent |
|  | メモリ使用率 | 80%以上が5分 | SQL Server process memory percent |
|  | ストレージ容量 | 80%以上が5分 | Data space used percent |

## ログ管理

本システムのログはApplication Insigths、Log Analyticsにより管理する。

### 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。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 本番環境 | 検証環境 | 備考 |
| ログ保存期間  (Azure Blob Storage以外のサービス) | 確認後記載 | 確認後記載 | 以下より選択する。  30日 / 60 日、90 日、120 日、180 日、270 日、365 日、550 日、730 日 |
| Azure Blob Storageログ保存期間 | 確認後記載 | 確認後記載 | 以下より選択する。  1日 ～ 365日 |

### ログ保存先

本システムではログを以下の送信先に保存する。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 本番環境 | 検証環境 | 備考 |
| ログ保存先 | Log Analytics ワークスペース | Log Analytics ワークスペース | 以下説明を参照。 |
| 名前 | prod-ymhlms-log | stg-ymhlms-log | ログ保存先名を指定。 |
| ターゲットテーブル | リソース固有 | リソース固有 | 診断設定で選択されたカテゴリごとに、個別のテーブルが選択されたワークスペース内に作成される。推奨値。 |

ログは以下の送信先に保存することができる。

|  |  |  |
| --- | --- | --- |
| 送信先 | 用途 | 説明 |
| Log Analytics ワークスペース | 通常保存 | Log Analytics ワークスペースにログやメトリックを送信すると、強力なログ クエリを使用して、Azure Monitor で収集された他の監視データと組み合わせて分析できるほか、アラートや視覚化などの Azure Monitor の他の機能を活用することもできる。 |
| Azure Storage アカウント | 長期保存 | Azure ストレージ アカウントにログとメトリックをアーカイブすると、監査、スタティック分析、またはバックアップに役立つ。 Azure Monitor ログや Log Analytics ワークスペースと比較すると、Azure ストレージはコストが低く、ログを無期限に保持することができる。 |
| Event Hubs | 外部システムとの連携 | Event Hubs にログとメトリックを送信すると、サードパーティ製の SIEM やその他のログ分析ソリューションなどの外部システムにデータをストリーミングできる。 |

### ログ保存方法

一部サービスのログはApplication Insigthsを利用してログを保存する。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 本番環境 | 検証環境 | 備考 |
| Application Insigths名 | prod-ymhlms-appinsigths | stg-ymhlms-appinsigths | リソース グループ内で一意の名前を指定する。命名規約は以下の通り。  ・1 文字以上 255 文字以下  ・使用可能文字は英数字、ピリオド、アンダースコア、ハイフン、かっこのみ。また、末尾をピリオドにすることはできない。 |
| Log Analyticsワークスペース | prod-ymhlms-log | stg-ymhlms-log | Log Analyticsワークスペースを指定。 |
| 対象サービス | ・Azure Functions  ・Log Apps | ・Azure Functions  ・Log Apps | Application Insightsを利用してログを収集するサービス。 |

### ログ一覧

本システムのログ一覧を示す。

#### API Management

|  |  |
| --- | --- |
| ログ | 内容 |
| GatewayLogs | ゲートウェイログ |
| WebSocketConnectionLogs | Webソケット接続ログ |

#### Azure Functions、Logic Apps

Application Insigthsにより取得する。

|  |  |
| --- | --- |
| ログ | 内容 |
| AppAvailabilityResults | アプリケーションインサイト可用性テストの結果。 |
| AppBrowserTimings | アプリケーションインサイトブラウザーのタイミング。 |
| AppEvents | アプリケーションインサイトイベント。 |
| AppMetrics | Application Insights メトリック。 |
| AppDependencies | 依存関係。 |
| AppExceptions | アプリケーションインサイト例外。 |
| AppPageViews | アプリケーションインサイトページ ビュー。 |
| AppPerformanceCounters | アプリケーションインサイト パフォーマンス カウンター。 |
| AppRequests | Application Insights 要求。 |
| AppSystemEvents | システムイベント。 |
| AppTraces | トレースログ。 |

#### データ統合サーバー(Data Factory)

|  |  |
| --- | --- |
| ログ | 内容 |
| ActivityRuns | アクティビティ実行ログ |
| PipelineRuns | パイプライン実行ログ |
| TriggerRuns | トリガー実行ログ |
| SandboxPipelineRuns | サンドボックスパイプライン実行ログ |
| SandboxActivityRuns | サンドボックスアクティビティ実行ログ |
| SSISPackageEventMessages |  |
| SSISPackageExecutableStatistics |  |
| SSISPackageEventMessageContext |  |
| SSISPackageExecutionComponentPhases |  |
| SSISPackageExecutionDataStatistics |  |
| SSISIntegrationRuntimeLogs |  |

#### DBサーバー(SQL Database)

|  |  |
| --- | --- |
| ログ | 内容 |
| SQLInsights |  |
| AutomaticTuning |  |
| QueryStoreRuntimeStatistics |  |
| QueryStoreWaitStatistics |  |
| Errors |  |
| DatabaseWaitStatistics |  |
| Timeouts |  |
| Blocks |  |
| Deadlocks |  |

#### ストレージ(Azure Blob Storage)

|  |  |
| --- | --- |
| ログ | 内容 |
| 読み取り |  |
| 書き込み |  |
| 削除 |  |
| データの削除 |  |

#### Front Door

|  |  |
| --- | --- |
| ログ | 内容 |
| FrontdoorAccessLog |  |
| FrontdoorWebApplicationFirewallLog |  |

#### VNet

|  |  |
| --- | --- |
| ログ | 内容 |
| VMProtectionAlerts |  |

### ログ監視

本システムのログ監視については、運用上問題が発生した場合に実施を検討する。(アプリに確認)

## 時刻同期

本システムが利用する各種サービスの時刻はAzure内部のMicrosoftタイムサーバーに同期される。

MicrosoftタイムサーバーはGPSアンテナを使用して、Microsoft が所有するデバイスから時刻を取得する。

## ソフトウェアのアップデート

本システムのソフトウェアはすべてAzureが自動的に管理を行い、ユーザーによる管理は不要である。

## 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 |
|  | ヤマハ様 |
|  | サンエム保守窓口 |

# セキュリティ

## 暗号化方針

本システムの暗号化方針について記載する。

### APサーバー(Azure Functions、Logic Apps)

|  |  |  |
| --- | --- | --- |
| サービス | 暗号化 | 備考 |
| Azure Functions | 有効 | 自動的に暗号化される。 |
| Logic Apps |  | 自動的に暗号化される。 |

### DBサーバー(Azure SQL Database)

|  |  |
| --- | --- |
| 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(Azure Storage)

|  |  |  |
| --- | --- | --- |
| 暗号化 | 暗号化の種類 | 備考 |
| 有効 | Microsoft マネージド キー | 自動的に暗号化される。 |

### ストレージ(Azure Storage)

|  |  |  |
| --- | --- | --- |
| サービス | 暗号化 | 備考 |
| SQL Database | 有効 | 自動的に暗号化される。 |
| Blob Storage |  | 自動的に暗号化される。 |

## 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 | | None | None | | 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。 | |
| 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> | | | | |
| Power Apps接続 | | | 接続する | | 接続する | | Power Apps接続有無を指定 |

### 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。 |