PDF のダウンロード エクスペリエンスについてお聞かせください。

Azure AI サービスのドキュメント

AI を活用して、市場に投入可能で社会的責任を果たす最先端のアプリケーションを組織向けに構築する

概要
Azure AI サービスとは

概要
Azure AI Studio とは?

チュートリアル
Azure AI Studio のコパイロットのチュートリアル

概念
AI の責任ある使用

Azure OpenAI

さまざまな自然言語タスクを実行します。

Speech

音声テキスト変換、テキスト読み上げ、翻訳、話者認識

Language

業界をリードする自然言語理解機能を備えたアプリを構築します。

Translator

AI を利用した翻訳テクノロジを使用して、100 を超える使用中の言語、危険な状態の言語、消滅の危機に瀕している言語を翻訳します。

Vision

Custom Vision

画像と動画のコンテンツを分析します。

画像認識をビジネス用にカスタマイズします。

Face

画像内の人や感情を検出および識別します。

コンテンツの安全性

望ましくないコンテンツを検出する AI サービス

Bot Service

ボットを作成し、それらをチャネル間で接続します。

Document Intelligence

ドキュメントをインテリジェントなデータ ドリブン ソリューションに変換します。

Azure AI Search

AI を利用したクラウド検索をモバイルおよび Web アプリで使用できるようにします。

Video Indexer

ご利用のビデオからアクションにつながる分析情報を抽出します。

Immersive Reader

ユーザーがテキストを読み、理解するのを支援します。

他のリソース

デモ & カスタマイズ スタジオ

Azure AI Studio

Azure OpenAI

Speech

その他の AI リソースを調べる

Azure Machine Learning

セマンティック カーネル

AI Builder

言語

Vision

Custom Vision

Document Intelligence

Content Safety

Custom Translator

Azure Machine Learning

Azure AI Language を使用した Power Virtual Agents

Windows AI

GitHub Copilot

トレーニングと認定

AI 学習とコミュニティ ハブ

責任ある AI の原則とプラクティスを特定する

AI のラーニング パスとモジュール

AI エンジニアのキャリア パス

非推奨の Azure AI サービス

Content Moderator

Language Understanding (LUIS)

QnA Maker

Metrics Advisor

Anomaly Detector

Personalizer

Azure AI サービスとは

[アーティクル] • 2024/03/21

Azure AI サービスは、開発者と組織が、すぐに使用できる事前構築済みのカスタマイズ可能な API とモデルを使用して、インテリジェントで最先端の市場対応の責任あるアプリケーションを迅速に作成するのに役立ちます。 アプリケーションの例には、会話、検索、監視、翻訳、音声、ビジョン、意思決定のための自然言語処理が含まれます。

> **ヒント**
>
> Azure AI Studio で、Azure OpenAI、Content Safety、Speech、Vision などの Azure AI サービスをお試しください。 詳細については、「**Azure AI Studio とは**」をご覧ください。

ほとんどの Azure AI サービスは、REST API とクライアント ライブラリ SDK を通じて、一般的な開発言語で利用できます。 詳細については、各サービスのドキュメントを参照してください。

利用可能な Azure AI サービス

Azure AI サービスをアプリケーションの強化とワークフローの最適化に役立てる方法について説明します。

テーブルを展開する

サービス	説明
Anomaly Detector (廃止)	潜在的な問題を早期に特定します。
Azure AI Search	AI を利用したクラウド検索をモバイルおよび Web アプリで実現できます。
Azure OpenAI	さまざまな自然言語タスクを実行します。
Bot Service	ボットを作成し、それらをチャネル間で接続します。
Content Moderator (廃止)	不快感を与える可能性がある、または望ましくないコンテンツを検出する。
Content Safety	望ましくないコンテンツを検出する AI サービス

サービス	説明
Custom Vision	ビジネス用に画像認識をカスタマイズします。
Document Intelligence	ドキュメントをインテリジェントなデータ ドリブン ソリューションに変換します。
Face	画像内の人や感情を検出および識別します。
Immersive Reader	ユーザーがテキストを読み、理解するのを支援します。
Language	業界をリードする自然言語理解機能を備えたアプリを構築します。
Language understanding (廃止)	アプリで自然な言語を理解します。
Metrics Advisor (廃止)	望ましくないコンテンツを検出する AI サービス
Personalizer (廃止)	ユーザーごとに豊富でパーソナライズされたエクスペリエンスを作成します。
QnA maker (廃止)	情報を、よりナビゲートしやすい質問と回答に変換する。
Speech	音声テキスト変換、テキスト読み上げ、翻訳、話者認識。
Translator	AI を利用した翻訳テクノロジを使用して、100 以上の使用中の言語、危険にさらされている言語、消滅の危機に瀕している言語や方言を翻訳します。
Video Indexer	ご利用のビデオからアクションにつながる分析情報を抽出します。
Vision	画像と動画のコンテンツを分析します。

価格レベルと請求

価格レベル (および請求される金額) は、認証情報を使用して送信するトランザクションの数に基づきます。 各価格レベルにより、以下が指定されます。

- 1 秒あたりに許可されるトランザクションの最大数 (TPS)。
- 価格レベル内で有効にされるサービス機能。
- 事前に定義された数のトランザクションのコスト。 この数を超えると、サービスの「価格の詳細」で指定されている追加料金が発生します。

注意

Azure AI サービスの多くには無料レベルがあり、これを使用してサービスを試すことができます。 無料レベルを使用するには、リソースの SKU として `F0` を使用します。

開発オプション

モデルをカスタマイズおよび構成するために使用するツールは、Azure AI サービス を呼び出すために使用するツールとは異なります。 ほとんどの Azure AI サービス は、何もカスタマイズすることなく、そのままの状態で、データを送信し、分析情報を受信することができます。 次に例を示します。

- Azure AI Vision サービスに画像を送信して、単語や語句を検出したり、フレーム内の人の数を数えたりすることができます
- Speech サービスにオーディオ ファイルを送信して、文字起こしを行い、同時に音声をテキストに変換することができます

Azure にはさまざまな種類のユーザー向けに設計された幅広いツールが用意されており、その多くは Azure AI サービスで使用できます。 デザイナー駆動型ツールは最も使いやすく、簡単に設定して自動化できますが、カスタマイズに関しては制限がある場合があります。 REST API とクライアント ライブラリを使用すると、ユーザーが制御できる範囲や柔軟性は向上しますが、ソリューションを構築するにはより多くの労力、時間、専門知識が必要になります。 REST API とクライアント ライブラリを使用する場合は、C#、Java、Python、JavaScript、その他の一般的なプログラミング言語など、最新のプログラミング言語を使用すると作業が快適になると思われます。

Azure AI サービス を使用できるさまざまな方法を見ていきます。

クライアント ライブラリと REST API

Azure AI サービス のクライアント ライブラリと REST API を使用すると、サービスに直接アクセスできます。 これらのツールを使用すると、Azure AI サービス とそのベース ライン モデルにプログラムでアクセスでき、多くの場合、モデルとソリューションをプログラムでカスタマイズできます。

- **対象ユーザー**: 開発者とデータ科学者
- **利点**: 任意の言語と環境からのサービスの呼び出しに関して、最大限の柔軟性が提供されます。
- **UI**: なし - コードのみ
- **サブスクリプション**: Azureアカウント + Azure AI サービスリソース

使用可能なクライアント ライブラリと REST API の詳細を確認したい場合は、Azure AI サービスの概要に関するページを使用してサービスを選択し、いずれかのクイックスタートの使用を開始してください。

継続的インテグレーションと継続的配置

Azure DevOps と GitHub Actions を使用して、デプロイを管理できます。 次のセクションでは、Speech および Language Understanding (LUIS) サービス用のカスタム モデルをトレーニングしてデプロイするための CI/CD 統合の 2 つの例を示します。

- **対象ユーザー**: 開発者、データ科学者、データ エンジニア
- **利点**:プログラムによってアプリケーションやモデルを継続的に調整、更新、デプロイできます。 データを使用して音声、視覚、言語、決定のモデルを定期的に改善および更新する場合、大きな利点があります。
- **UI ツール**: なし - コードのみ
- **サブスクリプション**: Azure アカウント + Azure AI サービス リソース + GitHub アカウント

DevOps と GitHub Actions を使用した継続的インテグレーションと継続的デリバリー

Language Understanding と音声サービスには、Azure DevOps と GitHub Actions を利用した継続的インテグレーション ソリューションと継続的配置ソリューションが用意されています。 これらのツールは、カスタム モデルのトレーニング、テスト、リリース管理を自動化するために使用されます。

- Custom Speech の CI/CD
- LUIS 用の CI/CD

オンプレミスのコンテナー

Azure AI サービス の多くは、オンプレミスでのアクセスと使用のためにコンテナーにデプロイできます。 これらのコンテナーを使用すると、コンプライアンス、セキュリティ、またはその他の運用上の理由でデータの近くで Azure AI サービスを使用することが柔軟に可能になります。 Azure AI コンテナーの完全な一覧については、「Azure AI サービス用のオンプレミス コンテナー」 を参照してください。

モデルのトレーニング

一部のサービスでは、自分のデータを取り込んでからモデルをトレーニングすることができます。 トレーニング済みのカスタム モデルにより、サービスのデータとアルゴリ

ズムに自分のデータを加えてモデルを拡張できます。 出力はニーズに合ったものとなります。 自分のデータを取り込むときに、サービスに固有の方法でデータにタグを付ける必要がある場合があります。 たとえば、花を識別するようにモデルをトレーニングする場合は、花の画像のカタログを、各画像における花の位置と共に提供してモデルをトレーニングできます。

エコシステム内の Azure AI サービス

Azure と Azure AI サービスを使用すると、広大なエコシステムを利用できます。以下はその例です。

- Logic Apps や Power Automate のような自動化および統合ツール。
- Azure Functions や App Service のようなデプロイ オプション。
- セキュリティで保護されたアクセス用の Azure AI サービス Docker コンテナー。
- ビッグ データ シナリオ用の Apache Spark、Azure Databricks、Azure Synapse Analytics、Azure Kubernetes Service などのツール。

詳細については、「Azure AI サービスのエコシステム」を参照してください。

リージョン別の提供状況

Azure AI サービスの API は、Microsoft マネージド データ センターの拡大しているネットワーク上でホストされます。 Azure リージョン一覧 で API ごとのリージョン別の提供状況がわかります。

まだサポートされていないリージョンを探しているのですか。 UserVoice フォーラム に機能要求を記入してご連絡ください。

言語のサポート

Azure AI サービスでは、さまざまなカルチャ言語がサービス レベルでサポートされています。 各 API で利用可能な言語は、サポート対象の言語一覧に関するページで検索できます。

セキュリティ

Azure AI サービスには、Microsoft Entra 資格情報を使った認証、有効なリソース キー、Azure 仮想ネットワークを含む多層型のセキュリティ モデルが用意されています。

認定資格とコンプライアンス

Azure AI サービスは、Cloud Security Alliance STAR Certification、FedRAMP Moderate、HIPAA BAA などの認証を受けています。

プライバシーやデータ管理については、トラスト センター を参照してください。

ヘルプとサポート

Azure AI サービスでは、インテリジェント アプリケーション作成のサポートについて、複数のオプションを提供しています。 Azure AI サービスには、独自の質問にも対応してもらえる、開発者の頼れるコミュニティがあります。 提供されているすべてのサポート オプションの一覧については、Azure AI サービスのサポート オプションとヘルプ オプションに関する記事を参照してください。

次のステップ

- Azure Quantum の使用を開始する 方法について学習する
- Azure AI Studio で Azure AI サービスなどを試しませんか?
- Azure AI サービスのコストを計画および管理する

Azure AI サービスの自然言語のサポート

[アーティクル] • 2024/03/25

Azure AI サービスでは、ユーザーを見て、聞いて、明確に説明し、理解するアプリケーションを構築できます。 Microsoft の言語サポート機能を使用すると、ユーザーは自然な方法でアプリケーションと通信し、グローバル展開を強化できます。 表のリンクを使用して、サービス別の言語のサポートと可用性を確認してください。

言語がサポートされているサービス

次の表に、サポートされているサービスごとの言語サポートのリファレンス記事へのリンクを示します。

テーブルを展開する

Azure AI Language サポート	説明
Content Moderator (廃止)	不快感を与える可能性がある、または望ましくないコンテンツを検出する。
Document Intelligence	ドキュメントをインテリジェントなデータ ドリブン ソリューションに変換します。
Immersive Reader	ユーザーがテキストを読み、理解するのを支援します。
Language サービス	業界をリードする自然言語理解機能を備えたアプリを構築します。
Language Understanding (LUIS) (廃止)	アプリで自然な言語を理解します。
QnA Maker (廃止)	情報を、よりナビゲートしやすい質問と回答に変換する。
Speech Service	音声合成、テキスト読み上げ、翻訳、話者認識アプリケーションを構成します。
Translator	100 を超える使用中の言語、危険にさらされている言語、消滅の危機に瀕している言語や方言を翻訳します。
Video Indexer	ご利用のビデオからアクションにつながる分析情報を抽出します。

Azure AI Language サポート	説明
Vision	画像と動画のコンテンツを分析します。

言語に依存しないサービス

次の Azure AI サービスは言語に依存せず、人間の言語に基づく制限はありません。

テーブルを展開する

Azure AI サービス	説明
Anomaly Detector	潜在的な問題を早期に特定します。
Custom Vision	画像認識をビジネス用にカスタマイズします。
Face	画像内の人や感情を検出および識別します。
Personalizer	ユーザーに豊富でパーソナライズされたエクスペリエンスを作成します。

関連項目

- Azure AI サービスとは
- アカウントの作成

クイックスタート: Azure AI サービスのマルチサービス リソースを作成する

[アーティクル] • 2023/09/08

このクイックスタートを使用して、Azure AI サービスのマルチサービス リソースを作成および管理します。 マルチサービス リソースを使用すると、1 つのキーとエンドポイントを使用して複数の Azure AI サービスにアクセスできます。 また、ご利用の複数のサービスの課金が統合されます。

Azure AI サービスには 2 つの異なるリソース (マルチサービス リソースとシングルサービス リソース) を通じてアクセスできます。

- マルチサービス リソース:
  - 1 つのキーとエンドポイントを使用して複数の Azure AI サービスにアクセスします。
  - ご利用の複数のサービスの課金を統合します。
- 単一サービス リソース:
  - 作成されたサービスごとに一意のキーとエンドポイントを使用して、単一の Azure AI サービスにアクセスします。
  - ほとんどの Azure AI サービスには、試用のための無料レベルが用意されています。

Azure AI サービスは、ご利用の Azure サブスクリプションに作成した Azure リソースによって表されます。 リソースの作成後、生成されたキーとエンドポイントを使用して、アプリケーションを認証できます。

マルチサービス リソースでサポートされているサービス

マルチサービス リソースを使用すると、1 つのキーとエンドポイントを使用して、以下の Azure AI サービスにアクセスできます。 リソースの使用を開始する方法については、以下のリンクからクイックスタート記事やサンプルなどを参照してください。

サービス	説明
Content Moderator (廃止)	不快感を与える可能性がある、または望ましくないコンテンツを検出する
Custom Vision	ビジネスに合わせて画像認識をカスタマイズする

サービス	説明
Document Intelligence	わずかな時間とコストでドキュメントを使用可能なデータに変換します
Face	画像内の人や感情を検出および識別する
Language	業界をリードする自然言語理解機能を備えたアプリを構築する
Speech	音声テキスト変換、テキスト読み上げ、翻訳、話者認識
Translator	100 以上の言語と方言を翻訳する
Vision	画像と動画のコンテンツを分析する

前提条件

- 有効な Azure サブスクリプション - 無料アカウントを作成する。
- 責任ある AI のご契約条件に同意してリソースを作成するためには、Azure アカウントに `Cognitive Services Contributor` ロールが割り当てられている必要があります。 このロールをアカウントに割り当てるには、ロールの割り当てに関するドキュメントの手順に従うか、管理者にお問い合わせください。

新しいマルチサービス リソースを作成する

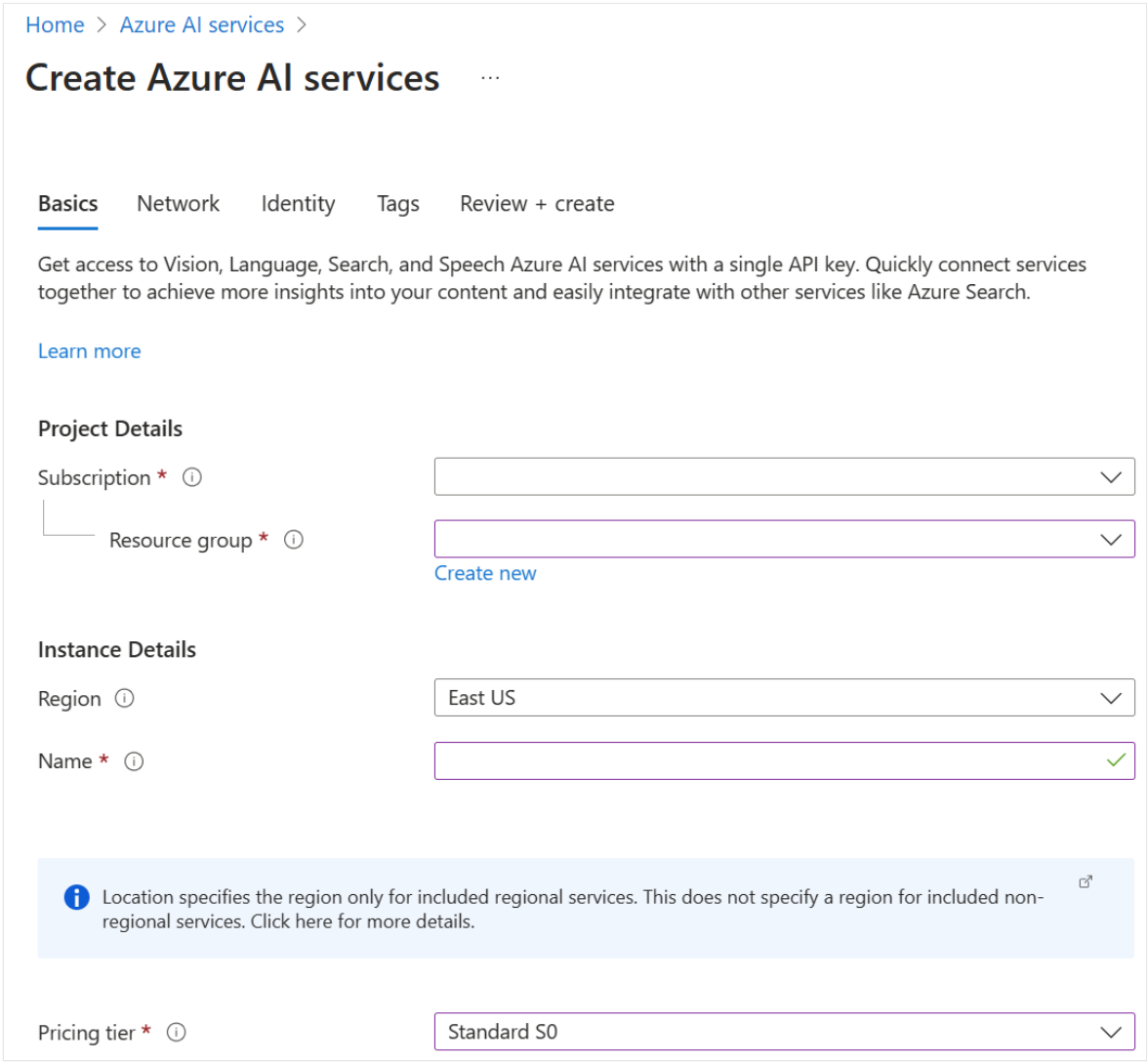
マルチサービス リソースは、ポータルの **[Azure AI サービス]**>**[Azure AI サービス マルチサービス アカウント]** の下に一覧表示されます。 マルチサービス リソースを作成するには、以下の手順を実行します。

1. マルチサービス リソースを作成するには、次のリンクを選択します。 https://portal.azure.com/#create/Microsoft.CognitiveServicesAllInOne

2. **[作成]** ページで、次の情報を指定します。

プロジェクトの詳細	説明
サブスクリプション	使用できる Azure サブスクリプションのいずれかを選択します。
リソース グループ	Azure AI サービス リソースを含める Azure リソース グループ。 新しいグループを作成することも、既存のグループに追加することもできます。

プロジェクトの詳細	説明
リージョン	Azure AI サービス インスタンスの場所。 別の場所を選択すると待機時間が生じる可能性がありますが、リソースのランタイムの可用性には影響しません。
名前	Azure AI サービス リソースのわかりやすい名前。 例: *MyCognitiveServicesResource*。
価格レベル	Azure AI サービス アカウントのコストは、選択しているオプションと使用量によって異なります。 詳細については、「API の価格の詳細」をご覧ください。



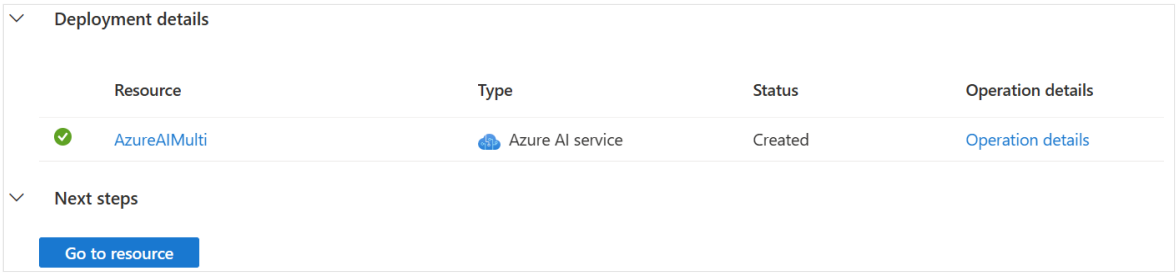
3. 必要に応じてリソースの他の設定を構成し、条件を読み取って同意し (該当する場合)、**[Review + create(確認と作成)]** を選択します。

> **ヒント**
>
> サブスクリプションで Azure AI サービス リソースの作成が許可されていない場合は、**Azure portal**、**PowerShell コマンド**、または **Azure CLI コマンド**を使用して、

その Azure **リソース プロバイダー**の特権を有効にする必要がある場合があります。 サブスクリプションの所有者でない場合は、サブスクリプションの所有者、または管理者のロールを持つユーザーに、登録の完了を要求するか、アカウントに **/register/action** 特権を付与するように要求します。

リソースのキーを取得する

1. リソースが正常にデプロイされたら、**[Next Steps(次のステップ)]** >**[Go to resource(リソースへの移行)]** を選択します。



2. 開かれた [クイックスタート] ウィンドウから、リソースエンドポイントにアクセスしキーを管理できます。

認証用の環境変数を構成する

Azure AI サービス リソースにアクセスするには、アプリケーションを認証する必要があります。 リソース キーの環境変数を設定するには、コンソール ウィンドウを開き、オペレーティング システムと開発環境の指示に従います。 `COGNITIVE_SERVICE_KEY` 環境変数を設定するには、`your-key` をリソースのキーの 1 つに置き換えます。

運用環境では、パスワードで保護されたシークレット コンテナーなどの資格情報を格納してアクセスする安全な方法を使用します。 テストの場合、環境変数への書き込みは標準的な方法ですが、環境変数はローカル コンピューター上のクリア テキストに格納されます。

> **ヒント**
>
> キーは、コードに直接含めないようにし、公開しないでください。 **Azure Key Vault** などのその他の認証オプションについては、Azure AI サービスの**セキュリティ**に関する記事をご覧ください。

Windows

PowerShell には、シークレット ストアや Azure KeyVault などのプラットフォームにセキュリティで保護された文字列を格納するための拡張可能なソリューションであるシークレットの管理が含まれています。

セキュリティで保護された文字列をホストするようにシークレット ストアを設定するには、シークレット ストアの使用の概要に関する記事を参照してください。 その後、次の例を使用して API キーを格納します。

PowerShell

```
Set-Secret -Name COGNITIVE_SERVICE_KEY -value your-key
```

テスト環境の場合は、PowerShell の `$Env:` 構文を使用して現在のセッションのみに環境変数を設定するか、`setx` コマンドを使用してセッション間で変数を保持することができます。 これらの値は、Windows レジストリ キーのクリア テキストに格納されていることに注意してください。

PowerShell

```
$Env:COGNITIVE_SERVICE_KEY = your-key
```

コンソール

```
setx COGNITIVE_SERVICE_KEY your-key
```

`setx` を使用する環境変数を追加した後に、環境変数を読み取る必要がある実行中のコンソールまたは他のプログラムの再起動が必要になる場合があります。 たとえば、Visual Studio をエディターとして使用している場合、サンプルを実行する前に Visual Studio を再起動します。

Azure Cognitive Service for Speech リソース リージョンの環境変数を設定するには、同じ手順に従います。 リソースのリージョンに `COGNITIVE_SERVICE_REGION` を設定します。 たとえば、「 `westus` 」のように入力します。

リソースをクリーンアップする

Azure AI サービス サブスクリプションをクリーンアップして削除したい場合は、リソースまたはリソース グループを削除することができます。 リソース グループを削除すると、そのグループに含まれている他のリソースも削除されます。

1. Azure Portal で左側のメニューを展開してサービスのメニューを開き、 **[リソース グループ]** を選択して、リソース グループの一覧を表示します。
2. 削除するリソースが含まれているリソース グループを見つけます。
3. リソース グループ全体を削除する場合は、リソース グループ名を選択します。 次のページで **[リソース グループの削除]** を選択し、確認します。
4. Azure AI サービス リソースのみを削除する場合は、リソース グループを選択して、その中のすべてのリソースを表示します。 次のページで、削除するリソースを選択し、その行の省略記号メニューを選択して、**[削除]** を選択します。

削除されたリソースを復旧する必要がある場合は、削除された Azure AI サービス リソースの復旧に関するページを参照してください。

次の手順

- リソースが用意できたので、サポートされている Azure AI サービスのいずれかに対する API 要求を認証できます。

Bicep を使用して Azure AI サービス リソースを作成する

[アーティクル] • 2024/04/08

このクイックスタートに従い、Bicep を使用して Azure AI サービス リソースを作成します。

Azure AI サービスは、開発者が直接的な人工知能 (AI) またはデータ サイエンスのスキルや知識がなくてもコグニティブかつインテリジェントなアプリケーションを構築できる、クラウドベースの AI サービスです。 これらは、REST API とクライアント ライブラリ SDK を通じて、一般的な開発言語で利用できます。 開発者は Azure AI サービスを使用して、見たり、聞いたり、話したり、分析したりできるコグニティブ ソリューションを使用したコグニティブ機能をそのアプリケーションに容易に追加することができます。

Bicep は、宣言型の構文を使用して Azure リソースをデプロイするドメイン固有言語 (DSL) です。 簡潔な構文、信頼性の高いタイプ セーフ、およびコードの再利用のサポートが提供されます。 Bicep により、Azure のコード ソリューションとしてのインフラストラクチャに最適な作成エクスペリエンスが実現します。

考慮事項

Bicep を使用して Azure AI サービス リソースを作成すると、マルチサービス リソースを作成できます。 これを使用すると、次のことができます。

- 1 つのキーとエンドポイントを使用して複数の Azure AI サービスにアクセスします。
- ご利用の複数のサービスの課金を統合します。
- Azure AI Vision で空間分析を、または Azure AI Language で Text Analytics for Health を使用する計画がある場合は、ご契約条件を確認して承認できるように、Azure portal で最初の Vision リソースまたは Language リソースを作成する必要があります。 これは、それぞれ Azure AI Language 、Azure AI Vision のリンクから行うことができます。 その後、同じ Azure サブスクリプションの下で任意のデプロイ ツール (SDK、CLI、または ARM テンプレートなど) を使用して、後続のリソースを作成できます。

前提条件

- Azure サブスクリプションをお持ちでない場合は、無料でアカウントを作成 してください。

Bicep ファイルを確認する

このクイックスタートで使用される Bicep ファイルは、Azure クイックスタート テンプレート からのものです。

> **注意**
>
> - 異なるリソース `kind` (以下の一覧) を使う場合、利用する**価格** レベルに合わせて `sku` パラメーターを変更する必要がある場合があります。 たとえば、 `TextAnalytics` の種類は `S0` ではなく `S` を使います。
> - 多くの Azure AI サービスには、サービスを試すために使用できる無料の `F0` 価格レベルがあります。

`sku` パラメーターを、必要な価格 インスタンスに変更してください。 `sku` は、使っているリソース `kind` によって異なります。 たとえば、 `TextAnalytics` のように指定します。

Bicep

```
@description('That name is the name of our application. It has to be
unique.Type a name followed by your resource group name. (<name>-
<resourceGroupName>)')
param cognitiveServiceName string =
'CognitiveService-${uniqueString(resourceGroup().id)}'

@description('Location for all resources.')
param location string = resourceGroup().location

@allowed([
  'S0'
])
param sku string = 'S0'

resource cognitiveService 'Microsoft.CognitiveServices/accounts@2021-10-01'
= {
  name: cognitiveServiceName
  location: location
  sku: {
    name: sku
  }
  kind: 'CognitiveServices'
  properties: {
    apiProperties: {
```

```
      statisticsEnabled: false
    }
  }
}
```

Bicep ファイルには、1 つの Azure リソースが定義されています。 Microsoft.CognitiveServices/accounts はそれが Azure AI サービス リソースであることを指定します。 Bicep ファイルの `kind` フィールドは、リソースの種類を定義します。

次の表に、Azure AI サービスの製品と価格に関する情報を示します。

マルチサービス

テーブルを展開する

サービス	種類
複数のサービス。 詳細については、価格 に関するページを参照してください。	`CognitiveServices`

視覚

テーブルを展開する

サービス	種類
Vision	`ComputerVision`
Custom Vision - Prediction	`CustomVision.Prediction`
Custom Vision - Training	`CustomVision.Training`
Face	`Face`
Document Intelligence	`FormRecognizer`

音声

テーブルを展開する

サービス	種類
Speech	`SpeechServices`

Language

テーブルを展開する

サービス	種類
Language Understanding (LUIS)	`LUIS`
QnA Maker	`QnAMaker`
Language	`TextAnalytics`
Text Translation	`TextTranslation`

決定

テーブルを展開する

サービス	種類
Anomaly Detector	`AnomalyDetector`
Content Moderator	`ContentModerator`
Personalizer	`Personalizer`

Azure OpenAI

テーブルを展開する

サービス	種類
Azure OpenAI	`OpenAI`

価格レベルと請求

価格レベル (および請求される金額) は、認証情報を使用して送信するトランザクションの数に基づきます。 各価格レベルにより、以下が指定されます。

- 1 秒あたりに許可されるトランザクションの最大数 (TPS)。
- 価格レベル内で有効にされるサービス機能。
- 事前に定義された数のトランザクションのコスト。 この数を超えると、サービスの「価格の詳細」で指定されている追加料金が発生します。

> ⓘ **注意**
>
> Azure AI サービスの多くには無料レベルがあり、これを使用してサービスを試すことができます。 無料レベルを使用するには、リソースの価格レベルとして `F0` を使用します。

Bicep ファイルをデプロイする

1. Bicep ファイルを **main.bicep** としてローカル コンピューターに保存します。
2. Azure CLI または Azure PowerShell のどちらかを使用して Bicep ファイルをデプロイします。

   CLI

   Azure CLI

   ```
   az group create --name exampleRG --location eastus
   az deployment group create --resource-group exampleRG --template-file main.bicep
   ```

   デプロイが完了すると、デプロイが成功したことを示すメッセージが表示されます。

デプロイされているリソースを確認する

Azure portal、Azure CLI、または Azure PowerShell を使用して、リソースグループ内のデプロイ済みリソースをリスト表示します。

CLI

Azure CLI

```
az resource list --resource-group exampleRG
```

リソースをクリーンアップする

不要になったら、Azure portal、Azure CLI、または Azure PowerShell を使用して、リソース グループとそのリソースを削除します。

CLI

Azure CLI

```
az group delete --name exampleRG
```

関連項目

- Azure AI サービスを安全に使用する方法については、「**Azure AI サービスに対する要求の認証**」を参照してください。
- Azure AI サービスの一覧については、「**Azure AI サービスとは?**」を参照してください。
- Azure AI サービスがサポートする自然言語の一覧を確認するには、「**自然言語のサポート**」を参照してください。
- Azure AI サービスをオンプレミスで使用する方法を確認するには、「**Azure AI サービスのコンテナーとしての使用**」を参照してください。
- Azure AI サービスの使用コストを見積もるには、「**Azure AI サービスのコストの計画および管理**」を参照してください。

クイックスタート: ARM テンプレートを使用して Azure AI サービス リソースを作成する

[アーティクル] • 2024/03/18

このクイックスタートでは、Azure Resource Manager テンプレート (ARM テンプレート) を使用して Azure AI サービス内にリソースを作成する方法を示します。

Azure AI サービスは、AI サービスのクラウドベースのポートフォリオです。 Azure AI サービスは、開発者が直接的な AI またはデータ サイエンスのスキルや知識がなくても、コグニティブかつインテリジェントなアプリケーションを構築するのに役立ちます。

Azure AI サービスは、REST API とクライアント ライブラリ SDK を通じて、一般的な開発言語で利用できます。 開発者は Azure AI サービスを使用して、見たり、聞いたり、話したり、分析したりできるコグニティブ ソリューションを使用したコグニティブ機能をそのアプリケーションに容易に追加することができます。

Azure AI サービス リソースを作成すると、次の操作を行うことができます。

- 1 つのキーとエンドポイントを使用して Azure 内の複数の AI サービスにアクセスします。
- ご利用の複数のサービスの課金を統合します。

Azure Resource Manager テンプレートは JavaScript Object Notation (JSON) ファイルであり、プロジェクトのインフラストラクチャと構成が定義されています。 このテンプレートでは、宣言型の構文が使用されています。 デプロイしようとしているものを、デプロイを作成する一連のプログラミング コマンドを記述しなくても記述できます。

前提条件

- Azure サブスクリプションをお持ちでない場合は、無料でアカウントを作成 してください。
- ご契約条件を確認して承認するには、最初の Azure AI Face 、Azure AI Language 、または Azure AI Vision のリソースを Azure portal から作成する必要があります。 その後、同じ Azure サブスクリプションの下で任意のデプロイ ツール (SDK、Azure CLI、ARM テンプレートなど) を使用して、リソースを作成できます。

テンプレートを確認する

このクイックスタートで使用するテンプレートは、Azure クイックスタート テンプレート からのものです。

JSON

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "metadata": {
    "_generator": {
      "name": "bicep",
      "version": "0.15.31.15270",
      "templateHash": "17000396405303018145"
    }
  },
  "parameters": {
    "cognitiveServiceName": {
      "type": "string",
      "defaultValue": "[format('CognitiveService-{0}', uniqueString(resourceGroup().id))]",
      "metadata": {
        "description": "That name is the name of our application. It has to be unique.Type a name followed by your resource group name. (<name>-<resourceGroupName>)"
      }
    },
    "location": {
      "type": "string",
      "defaultValue": "[resourceGroup().location]",
      "metadata": {
        "description": "Location for all resources."
      }
    },
    "sku": {
      "type": "string",
      "defaultValue": "S0",
      "allowedValues": [
        "S0"
      ]
    }
  },
  "resources": [
    {
      "type": "Microsoft.CognitiveServices/accounts",
      "apiVersion": "2021-10-01",
      "name": "[parameters('cognitiveServiceName')]",
      "location": "[parameters('location')]",
      "sku": {
        "name": "[parameters('sku')]"
      },
```

```
      "kind": "CognitiveServices",
      "properties": {
        "apiProperties": {
          "statisticsEnabled": false
        }
      }
    }
  ]
}
```

Bicep ファイルには、1 つの Azure リソースが定義されています。 Microsoft.CognitiveServices/accounts はそれが Azure AI サービス リソースであることを指定します。 Bicep ファイルの `kind` フィールドは、リソースの種類を定義します。

次の表に、Azure AI サービスの製品と価格に関する情報を示します。

マルチサービス

テーブルを展開する

サービス	種類
複数のサービス。 詳細については、価格 に関するページを参照してください。	`CognitiveServices`

視覚

テーブルを展開する

サービス	種類
Vision	`ComputerVision`
Custom Vision - Prediction	`CustomVision.Prediction`
Custom Vision - Training	`CustomVision.Training`
Face	`Face`
Document Intelligence	`FormRecognizer`

音声

テーブルを展開する

サービス	種類
Speech	`SpeechServices`

Language

テーブルを展開する

サービス	種類
Language Understanding (LUIS)	`LUIS`
QnA Maker	`QnAMaker`
Language	`TextAnalytics`
Text Translation	`TextTranslation`

決定

テーブルを展開する

サービス	種類
Anomaly Detector	`AnomalyDetector`
Content Moderator	`ContentModerator`
Personalizer	`Personalizer`

Azure OpenAI

テーブルを展開する

サービス	種類
Azure OpenAI	`OpenAI`

価格レベルと請求

価格レベル (および請求される金額) は、認証情報を使用して送信するトランザクションの数に基づきます。 各価格レベルにより、以下が指定されます。

- 1 秒あたりに許可されるトランザクションの最大数 (TPS)。
- 価格レベル内で有効にされるサービス機能。
- 事前に定義された数のトランザクションのコスト。 この数を超えると、サービスの「価格の詳細」で指定されている追加料金が発生します。

> **注意**
>
> Azure AI サービスの多くには無料レベルがあり、これを使用してサービスを試すことができます。 無料レベルを使用するには、リソースの価格レベルとして `F0` を使用します。

テンプレートのデプロイ

Azure Portal

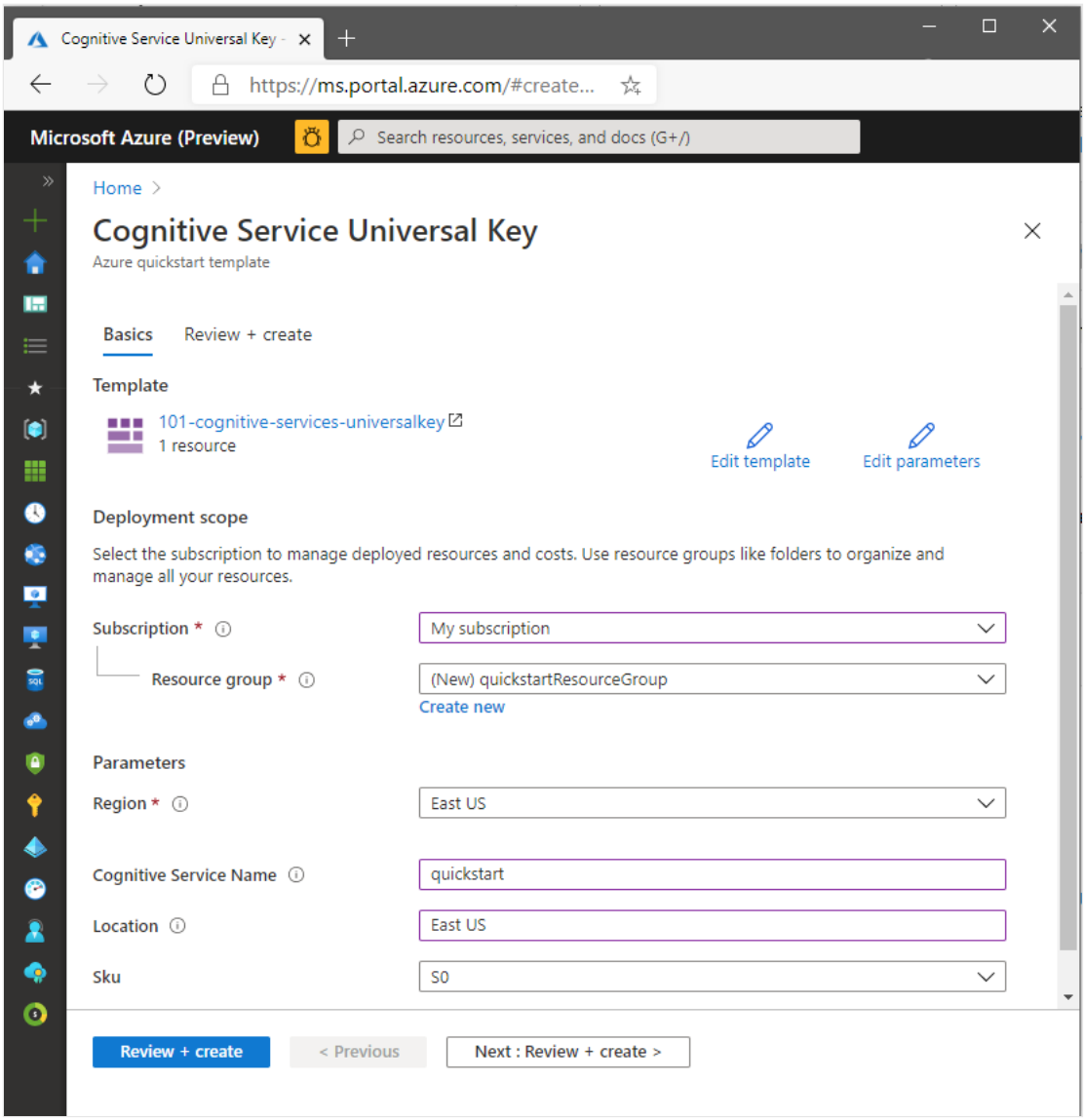
1. **[Azure へのデプロイ]** ボタンを選択します。

   Deploy to Azure

2. 次の値を入力します。

テーブルを展開する

値	説明
サブスクリプション	Azure サブスクリプションを選択します。
リソース グループ	**[新規作成]** を選択し、リソース グループの一意の名前を入力し、**[OK]** を選択します。
リージョン	リージョン (**[米国東部]** など) を選択します。
Cognitive Service 名	Azure AI サービス リソースの一意の名前で値を置き換えます。 次のセクションでデプロイを検証するときに、その名前が必要です。
場所	選択したリージョンに置き換えます。
SKU	リソースの価格レベルを選択します。



3. **[確認と作成]**、**[作成]** の順に選択します。 デプロイが正常に完了すると、**[リソースに移動]** ボタンを使用できます。

ヒント

サブスクリプションで Azure AI サービス リソースの作成が許可されていない場合は、Azure portal、PowerShell コマンド、または Azure CLI コマンドを使用して、その Azure リソース プロバイダーの特権を有効にする必要がある場合があります。 サブスクリプションの所有者でない場合は、サブスクリプションの所有者、または管理者ロールを持つユーザーに、登録の完了を要求してください。 または、アカウントに */register/action* 特権を付与するように要求します。

デプロイされているリソースを確認する

ポータル

デプロイが完了すると、**[リソースに移動]** ボタンを選択して新しいリソースを表示できるようになります。 リソース グループは、次の方法でも見つけることができます。

1. 左側のウィンドウから **[リソース グループ]** を選択する。
2. リソース グループ名を選択する。

リソースをクリーンアップする

Azure AI サービス サブスクリプションをクリーンアップして削除したい場合は、リソースまたはリソース グループを削除することができます。 リソース グループを削除すると、そのグループに含まれている他のリソースも削除されます。

Azure Portal

1. 左側のウィンドウで、**[リソース グループ]** を選択して、リソース グループの一覧を表示します。
2. 削除するリソースが含まれているリソース グループを見つけます。
3. リソース グループを右クリックし、**[リソース グループの削除]** を選択して確認します。

関連するコンテンツ

- Azure AI サービスを安全に使用する方法の詳細については、「Azure AI サービスに対する要求の認証」を参照してください。
- Azure AI サービスの一覧については、「Azure AI サービスとは」を参照してください。
- Azure AI サービスがサポートする自然言語の一覧については、「Azure AI サービスでの自然言語のサポート」を参照してください。
- Azure AI サービスをオンプレミスで使用する方法を確認するには、「Azure AI コンテナーとは」を参照してください。
- Azure AI サービスの使用コストを見積もるには、「Azure AI Studio のコストの計画および管理」を参照してください。

クイック スタート: Terraform を使用して Azure AI サービス リソースを作成する

[アーティクル] • 2024/04/07

ⓘ **AI-assisted content.** Content was created by a human author with the help of AI. A human author reviewed and revised the content as needed. Learn more

この記事では、Terraform を使用して Azure AI サービス アカウントを作成する方法について説明します。

Azure AI サービスは、開発者が直接的な人工知能 (AI) またはデータ サイエンスのスキルや知識がなくてもコグニティブかつインテリジェントなアプリケーションを構築できる、クラウドベースの AI サービスです。 これらは、REST API とクライアント ライブラリ SDK を通じて、一般的な開発言語で利用できます。 開発者は Azure AI サービスを使用して、見たり、聞いたり、話したり、分析したりできるコグニティブ ソリューションを使用したコグニティブ機能をそのアプリケーションに容易に追加することができます。

Terraform を使用すると、クラウド インフラストラクチャの定義、プレビュー、およびデプロイを行うことができます。 Terraform を使用する際は、HCL 構文を使って構成ファイルを作成します。 HCL 構文では、Azure などのクラウド プロバイダーと、クラウド インフラストラクチャを構成する要素を指定できます。 構成ファイルを作成したら、"実行プラン" を作成します。これにより、インフラストラクチャの変更をデプロイ前にプレビューすることができます。 変更を確認したら、実行プランを適用してインフラストラクチャをデプロイします。

この記事では、次のことについて説明します。

- ✓ random_pet を使用して Azure リソース グループ名のランダムなペット名を作成する
- ✓ azurerm_resource_group を使用して Azure リソース グループを作成する
- ✓ random_string を使用してランダムな文字列を作成する
- ✓ azurerm_cognitive_account を使用して Azure AI サービス アカウントを作成する

前提条件

- Terraform のインストールと構成

Terraform コードを実装する

ⓘ 注意

この記事のサンプル コードは、Azure Terraform GitHub リポジトリ にあります。 Terraform の現在および以前のバージョンのテスト結果 を含むログ ファイルを表示できます。

Terraform を使用して Azure リソースを管理する方法を示すその他の記事とサンプル コードを参照してください

1. サンプル Terraform コードをテストして実行するディレクトリを作成し、それを現在のディレクトリにします。

2. `main.tf` という名前のファイルを作成し、次のコードを挿入します。

```
Terraform
```

```
resource "random_pet" "rg_name" {
  prefix = var.resource_group_name_prefix
}

resource "azurerm_resource_group" "rg" {
  name     = random_pet.rg_name.id
  location = var.resource_group_location
}

resource "random_string" "azurerm_cognitive_account_name" {
  length  = 13
  lower   = true
  numeric = false
  special = false
  upper   = false
}

resource "azurerm_cognitive_account" "cognitive_service" {
  name                =
"CognitiveService-${random_string.azurerm_cognitive_account_name.result
}"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  sku_name            = var.sku
  kind                = "CognitiveServices"
}
```

3. `outputs.tf` という名前のファイルを作成し、次のコードを挿入します。

```
Terraform
```

```
output "resource_group_name" {
  value = azurerm_resource_group.rg.name
}

output "azurerm_cognitive_account_name" {
  value = azurerm_cognitive_account.cognitive_service.name
}
```

4. `providers.tf` という名前のファイルを作成し、次のコードを挿入します。

Terraform

```
terraform {
  required_version = ">=1.0"
  required_providers {
    azurerm = {
      source  = "hashicorp/azurerm"
      version = "~>3.0"
    }
    random = {
      source  = "hashicorp/random"
      version = "~>3.0"
    }
  }
}
provider "azurerm" {
  features {}
}
```

5. `variables.tf` という名前のファイルを作成し、次のコードを挿入します。

Terraform

```
variable "resource_group_location" {
  type        = string
  description = "Location for all resources."
  default     = "eastus"
}

variable "resource_group_name_prefix" {
  type        = string
  description = "Prefix of the resource group name that's combined with
a random ID so name is unique in your Azure subscription."
  default     = "rg"
}

variable "sku" {
  type        = string
  description = "The sku name of the Azure Analysis Services server to
create. Choose from: B1, B2, D1, S0, S1, S2, S3, S4, S8, S9. Some skus
are region specific. See https://docs.microsoft.com/en-
```

```
us/azure/analysis-services/analysis-services-overview#availability-by-
region"
  default     = "S0"
}
```

Terraform を初期化する

terraform init を実行して、Terraform のデプロイを初期化します。 このコマンドによって、Azure リソースを管理するために必要な Azure プロバイダーがダウンロードされます。

コンソール

```
terraform init -upgrade
```

重要なポイント:

- `-upgrade` パラメーターは、必要なプロバイダー プラグインを、構成のバージョン制約に準拠する最新バージョンにアップグレードします。

Terraform 実行プランを作成する

terraform plan を実行して、実行プランを作成します。

コンソール

```
terraform plan -out main.tfplan
```

重要なポイント:

- `terraform plan` コマンドは、実行プランを作成しますが、実行はしません。 代わりに、構成ファイルに指定された構成を作成するために必要なアクションを決定します。 このパターンを使用すると、実際のリソースに変更を加える前に、実行プランが自分の想定と一致しているかどうかを確認できます。
- 省略可能な `-out` パラメーターを使用すると、プランの出力ファイルを指定できます。 `-out` パラメーターを使用すると、レビューしたプランが適用内容とまったく同じであることが確実になります。

Terraform 実行プランを適用する

terraform apply を実行して、クラウド インフラストラクチャに実行プランを適用します。

コンソール

```
terraform apply main.tfplan
```

重要なポイント:

- `terraform apply` コマンドの例は、以前に `terraform plan -out main.tfplan` が実行されたことを前提としています。
- `-out` パラメーターに別のファイル名を指定した場合は、`terraform apply` の呼び出しで同じファイル名を使用します。
- `-out` パラメーターを使用しなかった場合は、パラメーターを指定せずに `terraform apply` を呼び出します。

結果を確認する

Azure CLI

1. Azure AI サービス アカウントが作成された Azure リソース名を取得します。

   コンソール

   ```
   resource_group_name=$(terraform output -raw resource_group_name)
   ```

2. Azure AI サービス アカウント名を取得します。

   コンソール

   ```
   azurerm_cognitive_account_name=$(terraform output -raw
   azurerm_cognitive_account_name)
   ```

3. az cognitiveservices account show を実行して、この記事で作成した Azure AI サービス アカウントを表示します。

   Azure CLI

   ```
   az cognitiveservices account show --name
   $azurerm_cognitive_account_name \
   ```

```
                                        --resource-group
$resource_group_name
```

リソースをクリーンアップする

Terraform を使用して作成したリソースが不要になった場合は、次の手順を実行します。

1. terraform plan を実行して、`destroy` フラグを指定します。

   コンソール

   ```
   terraform plan -destroy -out main.destroy.tfplan
   ```

   重要なポイント:

   - `terraform plan` コマンドは、実行プランを作成しますが、実行はしません。代わりに、構成ファイルに指定された構成を作成するために必要なアクションを決定します。 このパターンを使用すると、実際のリソースに変更を加える前に、実行プランが自分の想定と一致しているかどうかを確認できます。
   - 省略可能な `-out` パラメーターを使用すると、プランの出力ファイルを指定できます。 `-out` パラメーターを使用すると、レビューしたプランが適用内容とまったく同じであることが確実になります。

2. terraform apply を実行して、実行プランを適用します。

   コンソール

   ```
   terraform apply main.destroy.tfplan
   ```

Azure での Terraform のトラブルシューティング

Azure で Terraform を使用する場合の一般的な問題のトラブルシューティング

次のステップ

- Azure AI リソースについて詳しく知る

Azure AI サービスと AI エコシステム

[アーティクル] • 2023/11/16

Azure AI サービスには、一般的な問題を解決する機能が備わっています。たとえば、テキストで感情 (センチメント) を分析したり、画像を分析して物や顔を認識したりすることができます。 これらのサービスを使用するために、機械学習やデータ サイエンスに関する特別な知識は必要ありません。

Azure Machine Learning

Azure AI サービスと Azure Machine Learning にはいずれも、実現方法はそれぞれのオファリングで異なりますが、どちらも人工知能 (AI) を業務の強化に応用するという最終目標があります。

一般に、対象ユーザーは異なります。

- Azure AI サービスは機械学習の経験がない開発者を対象としています。
- Azure Machine Learning はデータ サイエンティスト向けに特化されています。

ビッグ データの Azure AI サービス

ビッグ データ向けの Azure AI サービスを使用すると、継続的に改善されるインテリジェントなモデルを Apache Spark™ と SQL の計算に直接埋め込むことができます。 これらのツールにより、開発者は低レベルの細かいネットワーク設定から解放され、スマートな分散アプリケーションの作成に集中できます。 ビッグ データ向けの Azure AI サービスでは、次のプラットフォームとコネクタがサポートされています: Azure Databricks、Azure Synapse、Azure Kubernetes Service、およびデータ コネクタ。

- **対象ユーザー**: データ科学者、データ エンジニア
- **利点**: ビッグ データ向けの Azure AI サービスを使用すると、ユーザーは Apache Spark™ を使用して Azure AI サービス経由で数テラバイトのデータを処理できます。 データストアを使用して大規模なインテリジェント アプリケーションを簡単に作成できます。
- **UI**: なし - コードのみ
- **サブスクリプション**: Azureアカウント + Azure AI サービスリソース

Azure AI サービスのビッグ データの詳細については、「Azure Synapse Analytics の Azure AI サービス」 を参照してください。

Azure Functions と Azure Service Web ジョブ

Azure Functions と Azure App Service Web ジョブはどちらも、開発者向けに設計されたコード第一の統合サービスを提供するものであり、Azure App Service 上に構築されています。 これらの製品により、コードを記述するためのサーバーレス インフラストラクチャが提供されます。 そのコード内では、クライアント ライブラリと REST API を使用して、サービスを呼び出すことができます。

- **対象ユーザー**: 開発者とデータ科学者
- **利点**:イベントによってトリガーされるコードを実行できるサーバーレス コンピューティング サービス。
- **UI**: はい
- **サブスクリプション**: Azure アカウント + Azure AI サービス リソース + Azure Functions サブスクリプション

Azure Logic Apps

Azure Logic Apps では、Power Automate と同じワークフロー デザイナーとコネクタが共有されますが、Visual Studio や DevOps との統合などのより高度な制御が提供されます。 Power Automate を使用すると、API 関連のプロキシまたはラッパーを提供するサービス固有のコネクタを通して Azure AI サービスリソースと簡単に統合できます。 これらは、Power Automate で使用できるものと同じコネクタです。

- **対象ユーザー**: 開発者、インテグレーター、IT プロフェッショナル、DevOps
- **利点**:コーディングの少ないソリューションで高度なオプションと統合を提供するデザイナー第一 (宣言型) の開発モデル。
- **UI**: はい
- **サブスクリプション**: Azure アカウント + Azure AI サービス リソース + Logic Apps デプロイ

Power Automate

Power Automate は、コードを記述せずにアプリとサービスの間の自動化されたワークフローを作成するために役立つ、Power Platform 内のサービスです。 Power Automate ソリューションで Azure AI サービス リソースと簡単にやりとりできるように、いくつかのコネクタが用意されています。 Power Automate は Logic Apps の上に構築されています。

- **対象ユーザー**: ビジネス ユーザー (アナリスト)、SharePoint 管理者
- **利点**:デスクトップからマウス クリック、キーストローク、コピーと貼り付けの手順を記録するだけで、反復的な手動タスクを自動化できます。
- **UI ツール**: はい - UI のみ

- **サブスクリプション**: Azure アカウント + Azure AI サービス リソース + Power Automate サブスクリプション + Office 365 サブスクリプション

AI Builder

Microsoft Power Platform の機能である AI Builder を使用すると、プロセスを自動化して結果を予測することにより、ビジネスのパフォーマンスを向上させることができます。 AI Builder は、ポイント アンド クリック エクスペリエンスを通して、ソリューションに AI の機能を組み込みます。 言語サービス、Computer Vision などの多くの Azure AI サービス がここに直接統合されており、独自のAzure AI サービスを作成する必要はありません。

- **対象ユーザー**: ビジネス ユーザー (アナリスト)、SharePoint 管理者
- **利点**:ポイント アンド クリック エクスペリエンスにより AI の機能を組み込むターンキー ソリューション。 コーディングやデータ サイエンスのスキルは必要ありません。
- **UI ツール**: はい - UI のみ
- **サブスクリプション**: AI Builder

次のステップ

- Azure AI Studio で生成型 AI アプリケーションを構築する方法について確認します。
- Azure AI の FAQ の記事で、よくあるご質問とその回答を確認します。
- Azure portal で、または Azure CLI を使用して、Azure AI サービス リソースを作成します。
- サービスの更新情報 で最新情報を入手する。

Azure AI サービスのカスタム サブドメイン名

[アーティクル] • 2024/01/20

2019 年 7 月以降、Azure AI サービスでは、Azure portal、Azure Cloud Shell、または Azure CLI を使用して作成された各リソースに対して、カスタム サブドメイン名を使用します。 特定の Azure リージョンのすべてのお客様に共通だった、リージョン エンドポイントとは異なり、カスタム サブドメイン名はリソースに対して一意です。 認証で Microsoft Entra ID などの機能を有効にするには、カスタム サブドメイン名が必要です。

これは既存のリソースにどのように影響しますか?

2019 年 7 月 1 日より前に作成された Azure AI サービス リソースには、関連するサービスのリージョン エンドポイントが使用されています。 これらのエンドポイントは、既存および新しいリソースで動作します。

既存のリソースを移行してカスタム サブドメイン名を使用し、Microsoft Entra ID などの機能を有効にできるようにするには、次の手順に従います:

1. Azure portal にサインインし、カスタム サブドメイン名を追加する Azure AI サービス リソースを見つけます。
2. **[概要]** ブレードで、 **[カスタム ドメイン名を生成します]** を見つけて選択します。
3. パネルが開き、リソースの一意のカスタム サブドメインを作成する手順が示されます。

> ⚠ **警告**
>
> カスタム サブドメインの名前は、作成後に変更することは**できません**。

既存のリソースを更新する必要はありますか?

不正解です。 リージョン エンドポイントは、新しい、および既存の Azure AI サービスで引き続き機能します。カスタム サブドメイン名は省略できます。 カスタム サブドメイン名が追加されている場合でも、リージョン エンドポイントはリソースで引き続き機能します。

SDK でリソースのリージョンが要求された場合はどうすればよいですか?

> ⚠ **警告**
>
> Speech Service では、**プライベート エンドポイントのみ**でカスタム サブドメインが使用されます。 それ以外の場合は、Speech Service および関連付けられている SDK で**リージョン エンドポイント**を使用してください。

リージョン エンドポイントとカスタム サブドメイン名は両方サポートされており、どちらを使用しても変わりはありません。 ただし、完全なエンドポイントが必要です。

リージョン情報は、Azure portal のご利用のリソースの **[概要]** ブレードで確認できます。 リージョン エンドポイントの完全な一覧については、Is リージョン エンドポイントの一覧はありますか? に関するページをご覧ください。

カスタム サブドメイン名はリージョン単位ですか?

はい。 カスタム サブドメイン名を使用しても、Azure AI サービス リソースのリージョンについては何も変わりません。

カスタム サブドメイン名にはどのような要件がありますか?

カスタム サブドメイン名はリソースに対して一意です。 名前に含めることができるのは、英数字と `-` 文字のみです。長さは 2 文字から 64 文字である必要があり、末尾を `-` にすることはできません。

カスタム ドメイン名を変更できますか?

いいえ。 カスタム サブドメイン名は、作成されてリソースに関連付けられた後は、変更することはできません。

カスタム ドメイン名を再利用できますか?

各カスタム サブドメイン名は一意であるため、Azure AI サービス リソースに割り当てたカスタム サブドメイン名を再利用するには、既存のリソースを削除する必要があります。 リソースが削除された後、カスタム サブドメイン名を再利用できます。

リージョン エンドポイントの一覧はありますか?

はい。 これは、Azure AI サービス リソースで使用できるリージョン エンドポイントの一覧です。

> **注意**
>
> Translator サービスと Bing Search API にはグローバル エンドポイントが使用されます。

テーブルを展開する

エンドポイントの種類	リージョン	エンドポイント
パブリック	グローバル (Translator と Bing)	`https://api.cognitive.microsoft.com`
	オーストラリア東部	`https://australiaeast.api.cognitive.microsoft.com`
	ブラジル南部	`https://brazilsouth.api.cognitive.microsoft.com`
	カナダ中部	`https://canadacentral.api.cognitive.microsoft.com`
	米国中部	`https://centralus.api.cognitive.microsoft.com`
	東アジア	`https://eastasia.api.cognitive.microsoft.com`
	米国東部	`https://eastus.api.cognitive.microsoft.com`
	米国東部 2	`https://eastus2.api.cognitive.microsoft.com`
	フランス中部	`https://francecentral.api.cognitive.microsoft.com`
	インド中部	`https://centralindia.api.cognitive.microsoft.com`
	東日本	`https://japaneast.api.cognitive.microsoft.com`
	韓国中部	`https://koreacentral.api.cognitive.microsoft.com`
	米国中北部	`https://northcentralus.api.cognitive.microsoft.com`

エンドポイントの種類	リージョン	エンドポイント
	北ヨーロッパ	`https://northeurope.api.cognitive.microsoft.com`
	南アフリカ北部	`https://southafricanorth.api.cognitive.microsoft.com`
	米国中南部	`https://southcentralus.api.cognitive.microsoft.com`
	東南アジア	`https://southeastasia.api.cognitive.microsoft.com`
	英国南部	`https://uksouth.api.cognitive.microsoft.com`
	米国中西部	`https://westcentralus.api.cognitive.microsoft.com`
	西ヨーロッパ	`https://westeurope.api.cognitive.microsoft.com`
	米国西部	`https://westus.api.cognitive.microsoft.com`
	米国西部 2	`https://westus2.api.cognitive.microsoft.com`
US Gov	US Gov バージニア州	`https://virginia.api.cognitive.microsoft.us`
中国	中国東部 2	`https://chinaeast2.api.cognitive.azure.cn`
	中国北部	`https://chinanorth.api.cognitive.azure.cn`

関連項目

- Azure AI サービスとは
- 認証

Azure AI Studio のコストを計画および管理する

[アーティクル] • 2024/02/05

この記事では、Azure AI Studio のコストを計画および管理する方法について説明します。 コストを見積もるサービスに対してリソースを追加する前に、まず、Azure AI Studio のコストの計画に役立つ Azure 料金計算ツールを使用します。 次に、Azure リソースを追加するときに、推定コストを確認します。

Azure AI Studio で Azure AI サービスを使用します。 Azure AI サービスのコストは、Azure の請求に記載された月額料金の一部にすぎません。 課金は、サードパーティのサービスを含め、ご使用の Azure サブスクリプションで使用されている Azure のすべてのサービスとリソースに対して行われます。

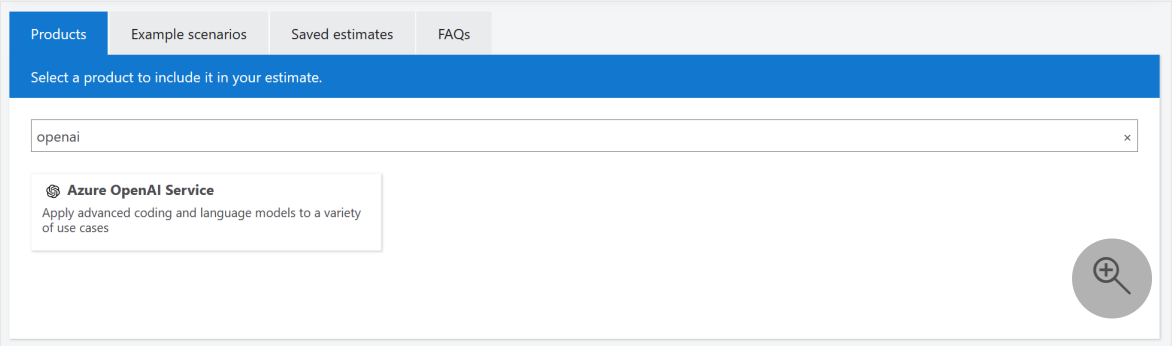
前提条件

Microsoft Cost Management のコスト分析では、ほとんどの種類の Azure アカウントがサポートされますが、すべてではありません。 サポートされているアカウントの種類の完全な一覧については、「Understand Cost Management data (Cost Management データの概要)」を参照してください。 コスト データを表示するには、少なくとも Azure アカウントの読み取りアクセス許可が必要です。 Azure Cost Management データに対するアクセス権の割り当てについては、データへのアクセス許可の割り当てに関するページを参照してください。

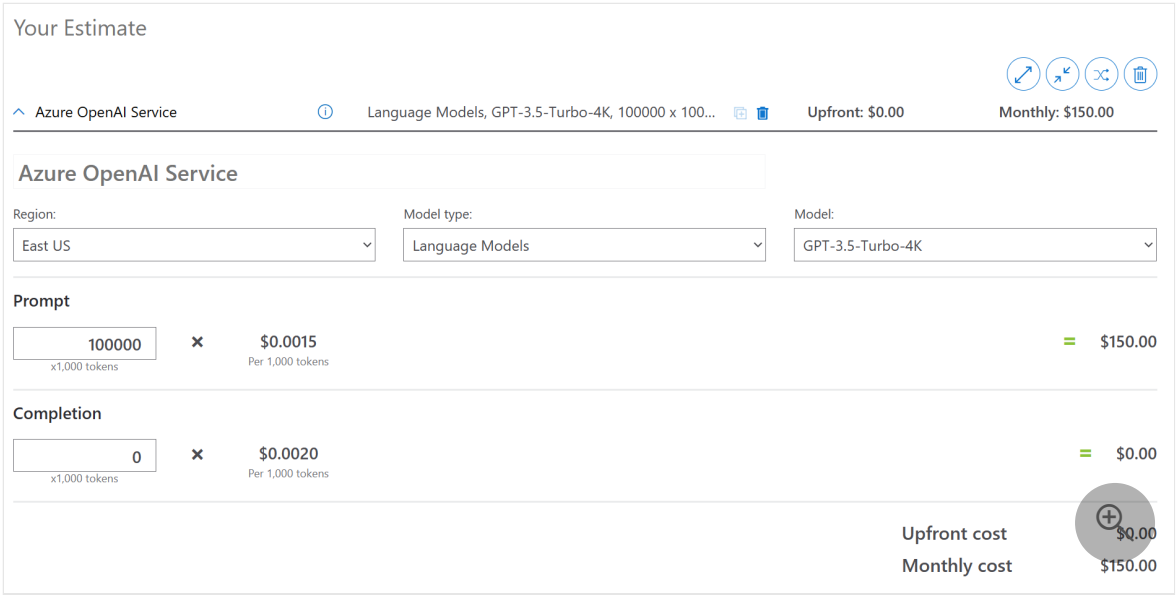
Azure AI サービスを使用する前にコストを見積もる

Azure AI サービスを追加する前に、Azure 料金計算ツール を使用してコストを見積もります。

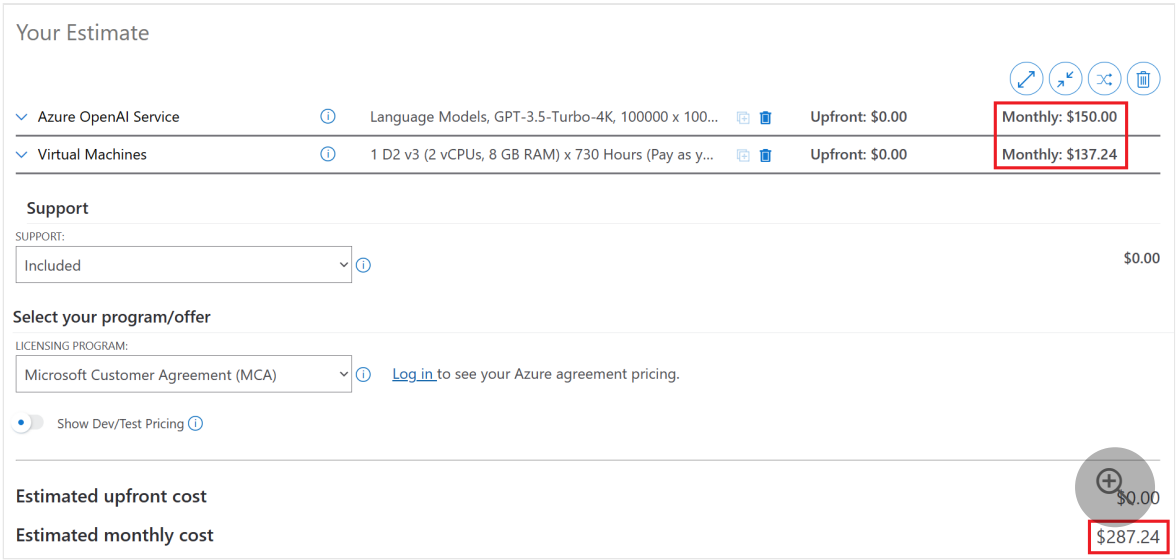
1. Azure 料金計算ツールで Azure OpenAI などの製品を選択します。



2. 使用する予定のユニット数を入力します。 たとえば、プロンプトと入力補完のトークンの数を入力します。



3. 複数の製品を選択して、複数の製品のコストを見積もることができます。 たとえば、Virtual Machines を選択して、コンピューティング リソースの潜在的なコストを追加します。



プロジェクトに新しいリソースを追加したら、この計算ツールに戻り、同じリソースをここに追加して、コストの見積もりを更新します。

Azure AI と Azure AI Studio で通常発生するコスト

Azure AI ハブ リソースのリソースを作成すると、他の Azure サービスのリソースも作成されます。 以下のとおりです:

テーブルを展開する

サービスの価格ページ	ユース ケースの例を含む説明
Azure AI サービス	Azure OpenAI、音声、Content Safety、Vision、Document Intelligence、Language などのサービスを使用するために支払います。 コストは、サービスごと、および各サービス内の一部の機能によって異なります。 Azure AI サービスのプロビジョニングの詳細については、「Azure AI ハブ リソース」を参照してください。
Azure AI Search	ユース ケース例の 1 つが、ベクトル検索インデックスへのデータの保存です。
Azure Machine Learning	Azure AI Studio を介して Visual Studio Code (Web またはデスクトップ) とプロンプト フローを実行するには、コンピューティング インスタンスが必要です。 コンピューティング インスタンスを作成する場合、仮想マシン (VM) はそのまま維持されるため、作業に使用できます。 アイドリングからのシャットダウンを有効にして、VM が指定された期間アイドル状態のときにコストを節約します。 または、コンピューティング インスタンスが自動的に開始および停止されるようにスケジュールを設定して、使用する予定がないときのコストを節約します。
Azure 仮想マシン	Azure Virtual Machines では、Linux、Windows Server、SQL Server、Oracle、IBM、SAP などをサポートするさまざまなコンピューティング ソリューションに対する仮想化に、柔軟に対応することができます。
Azure Container Registry Basic アカウント	プライベート Docker コンテナー イメージのストレージを提供し、Azure でのコンテナー ワークロードの迅速でスケーラブルな取得と、ネットワークに近いデプロイを可能にします。
Azure Blob Storage	Azure AI プロジェクト ファイルを保存するために使用できます。
Key Vault	シークレットを格納するためのキー コンテナー。
Azure Private Link	Azure Private Link を使用すると、仮想ネットワーク内のプライベート エンドポイント経由で Azure PaaS サービス (Azure Storage、SQL Database など) にアクセスできます。

リソースの削除前にコストが発生する可能性がある

Azure portal 内で、または Azure CLI を使用して Azure AI ハブ リソースを削除するまでは、以下のサブ リソースは一般的なコストとして、ワークスペース内でアクティブに

作業していない場合でも蓄積されます。 後に Azure AI ハブ リソースに戻ることを計画している場合、以下のリソースによってコストが蓄積され続ける可能性があります。

- Azure AI Search (データ用)
- 仮想マシン
- Load Balancer
- Virtual Network
- 帯域幅

VM はそれぞれ、実行している時間ごとに課金されます。 コストは VM の仕様によって異なります。 実行中であっても、データセットに対してアクティブに動作していない VM については、ロード バランサー経由で課金されます。 コンピューティング インスタンスごとに、1 日あたり 1 つのロード バランサーが課金されます。 コンピューティング クラスターの 50 ノードごとに、1 つの Standard ロード バランサーが課金されます。 ロード バランサーあたりの課金額は 1 日あたり約 0.33 ドルです。 停止しているコンピューティング インスタンスとコンピューティング クラスターに対してロード バランサーのコストが発生するのを回避するには、コンピューティング リソースを削除します。

コンピューティング インスタンスでは、停止状態でも P10 ディスク コストが発生します。 これは、そこに保存されたすべてのユーザー コンテンツが、Azure VM と同様に停止状態にまたがって保持されるためです。 コストをより適切に制御するために、OS ディスクのサイズ/タイプを構成できるように取り組んでいます。 仮想ネットワークについては、サブスクリプションごと、およびリージョンごとに 1 つの仮想ネットワークが課金されます。 仮想ネットワークは、複数のリージョンまたはサブスクリプションにまたがることはできません。 仮想ネットワークの設定内でプライベート エンドポイントを設定した場合にも、料金が発生することがあります。 帯域幅は使用量に基づいて課金されます。転送データが多いほど、料金は高くなります。

リソースの削除後にコストが発生する可能性がある

Azure portal 内で、または Azure CLI を使用して Azure AI ハブ リソースを削除した後も、以下のリソースは存在し続けます。 これらを削除するまで、これらのコストは発生し続けます。

- Azure Container Registry
- Azure Blob Storage
- Key Vault
- Application Insights (これを Azure AI ハブ リソースに対して有効にした場合)

コストを監視する

Azure AI ハブ リソースで Azure AI Studio を使用すると、コストが発生します。 Azure リソース使用のユニット コストは、期間 (秒、分、時間、日数) やユニット使用量 (バイト、メガバイトなど) によって異なります。 発生したコストはコスト分析で確認できます。

コスト分析を使用すると、さまざまな期間の Azure AI ハブ リソースのコストをグラフや表で確認できます。 たとえば、日単位、現在の月、以前の月、年単位などがあります。 予算や予想コストを基準としてコストを表示することもできます。 時間経過を示す、より長い期間のビューに切り替えると、支出の傾向を特定するのに役立ちます。 超過出費が発生した可能性のある時期を確認できます。 予算を作成したら、それを超えた場所も簡単に確認できます。

Azure AI Studio プロジェクトのコストを監視する

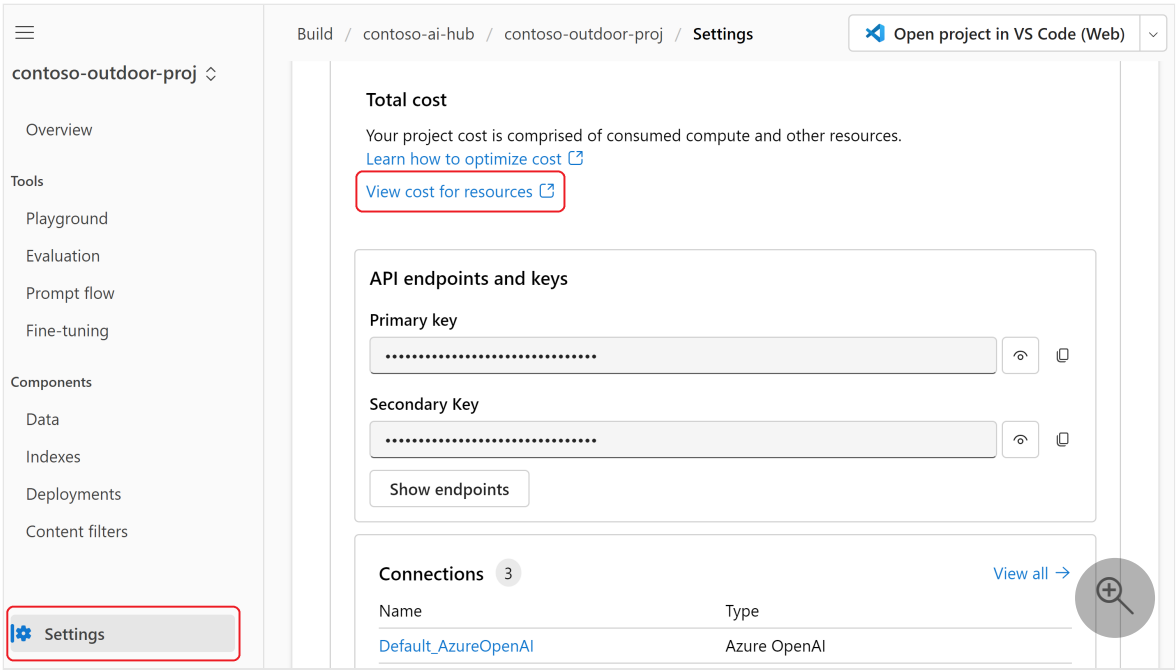
コスト分析は Azure portal から取得できます。 また、Azure AI Studio からコスト分析にアクセスすることもできます。

> **重要**
>
> Azure AI プロジェクトのコストは、アプリケーションまたはソリューションの全体的なコストの一部にすぎません。 アプリケーションまたはソリューションで使われるすべての Azure リソースのコストを監視する必要があります。 詳細については、「**Azure AI ハブ リソース**」を参照してください。

このセクションの例では、すべての Azure AI Studio リソースが同じリソース グループに属していることを前提としています。 ただし、異なるリソース グループにリソースを含めることもできます。 たとえば、Azure AI Search リソースは、Azure AI Studio プロジェクトとは異なるリソース グループに属する可能性があります。

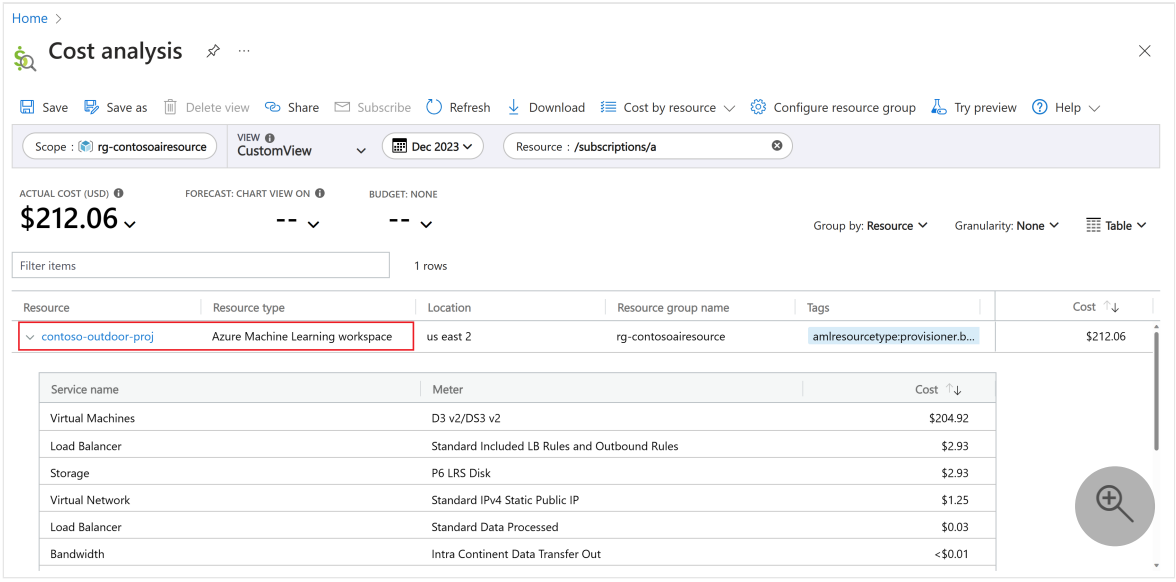
Azure AI Studio プロジェクトのコストを監視する方法の例を次に示します。 これらのコストはあくまでも例として使っています。 コストは、使っているサービスや使用量によって変わります。

1. Azure AI Studio にサインインします。
2. プロジェクトを選び、左側のナビゲーション メニューから **[AI プロジェクトの設定]** を選びます。

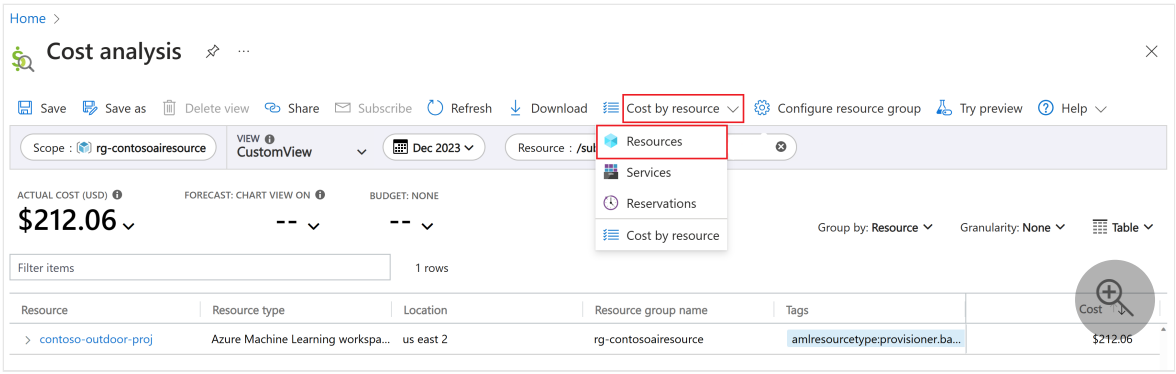


3. **[リソースのコストの表示]** を選択します。 Azure portal が開き、プロジェクトのコスト分析ページが表示されます。

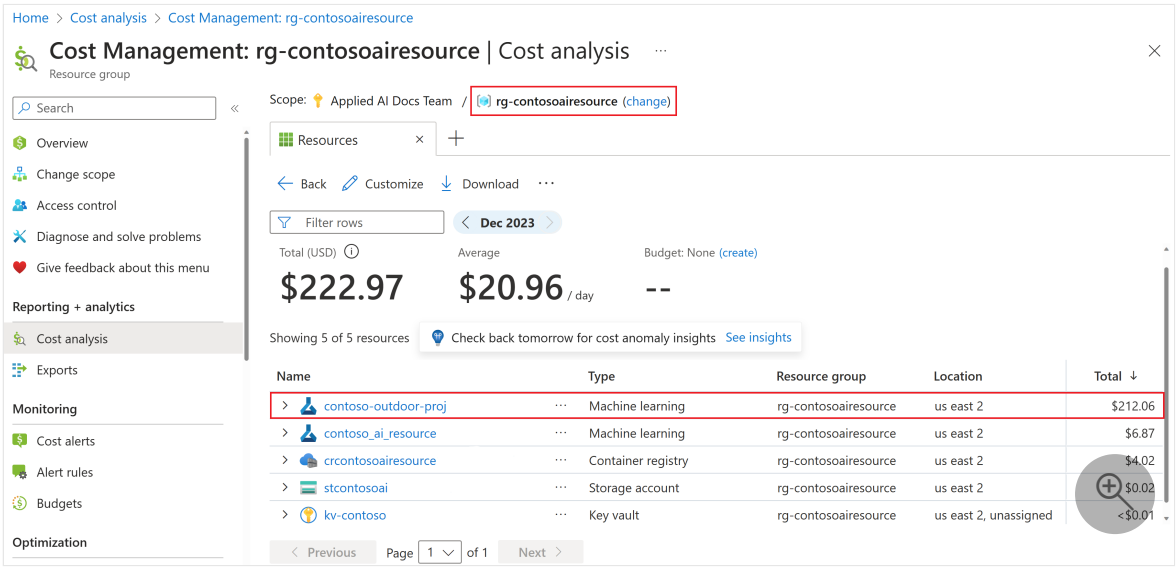
4. **[リソース]** 列を展開すると、Azure AI プロジェクトの基となる各サービスのコストが表示されます。 ただし、このビューには、Azure AI プロジェクトで使用しているすべてのリソースのコストは含まれていません。



5. **[リソースごとのコスト]**>**[リソース]** を選びます。



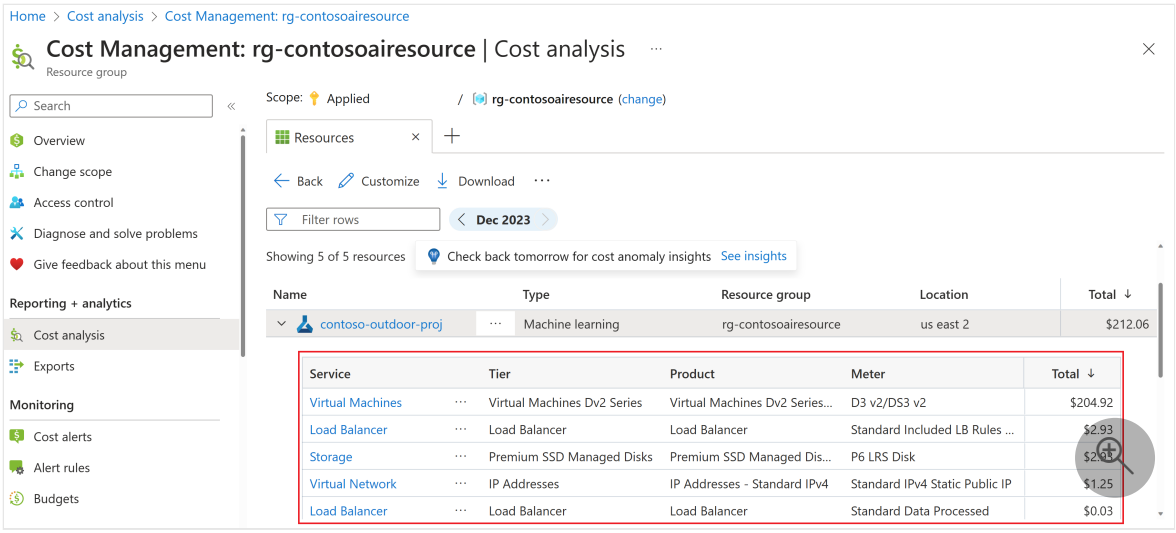
6. 表示される **[コスト分析]** ページで、スコープがリソース グループに設定されていることを確認します。



次の点に注意してください。

- リソース グループ名は **rg-contosoairesource** です。
- このリソース グループ内のすべてのリソースとサービスの合計コストは **$222.97** です。 この例では、これは Azure AI Studio を使って構築しているアプリケーションまたはソリューションの合計コストです。 繰り返しになりますが、これはすべての Azure AI Studio リソースが同じリソース グループに属していることを前提としています。 ただし、異なるリソース グループにリソースを含めることもできます。
- プロジェクト名は **contoso-outdoor-proj** です。
- Azure AI プロジェクトのリソースとサービスに限定したコストは、合計 **$212.06** です。

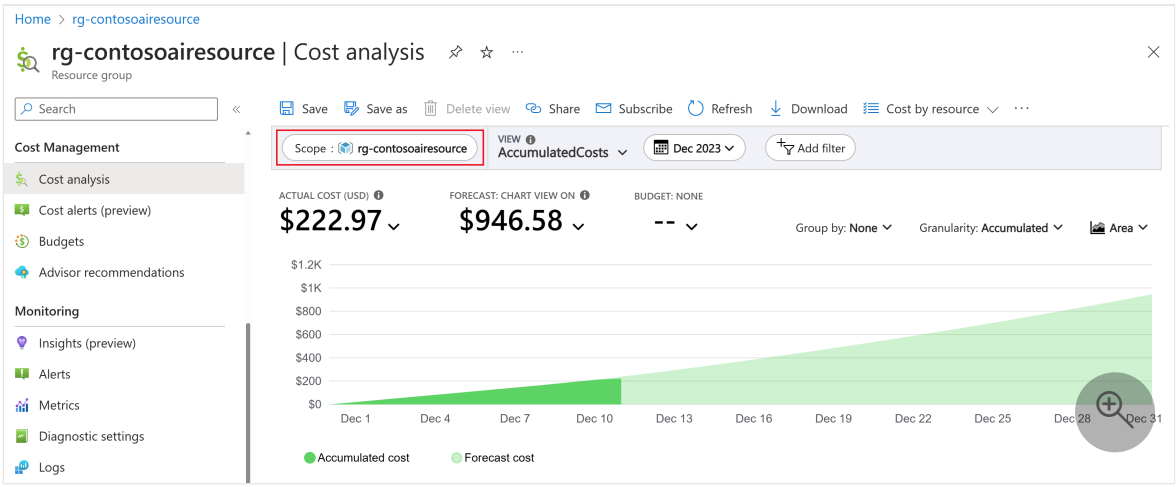
7. **contoso-outdoor-proj** を展開すると、Azure AI プロジェクト リソースの基となるサービスのコストが表示されます。



8. **[contoso_ai_resource]** を展開すると、Azure AI ハブ リソースの根底にあるサービスのコストが表示されます。 フィルターを適用して、リソース グループ内の他のコストに焦点を当てることもできます。

Azure portal からリソース グループのコストを直接表示することもできます。 そのためには次のようにします。

1. Azure ポータル にサインインします。
2. **[リソース グループ]** を選択します。
3. Azure AI Studio リソースが含まれるリソース グループを見つけて選びます。
4. 左側のナビゲーション メニューから **[コスト分析]** を選びます。

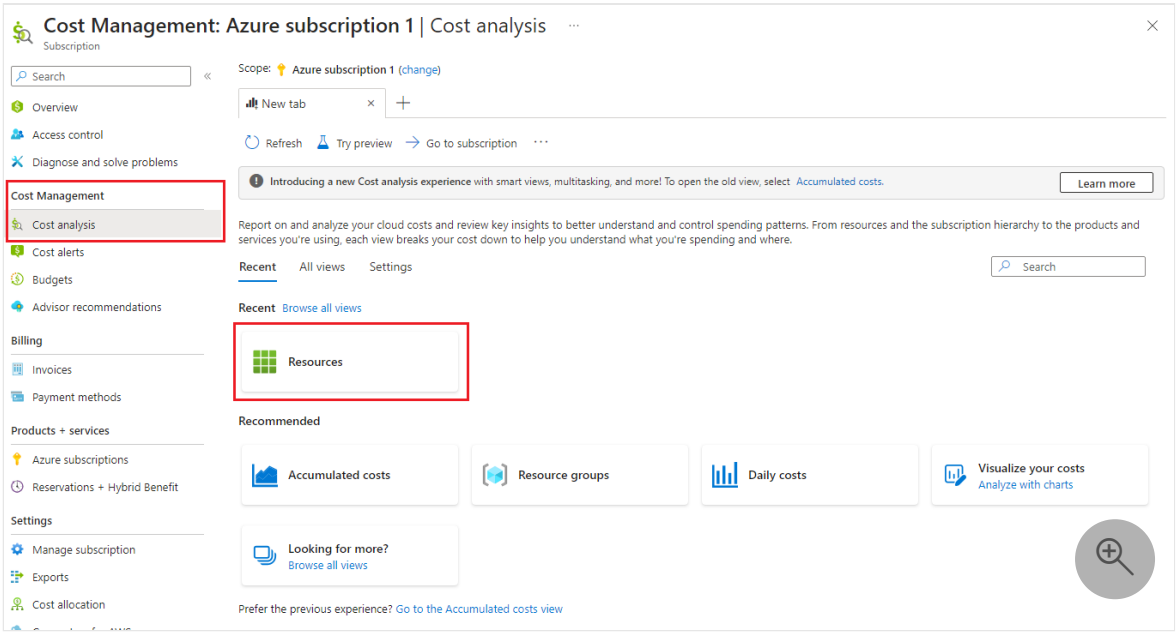


詳細については、Azure の料金計算ツール に関するページをご覧ください。

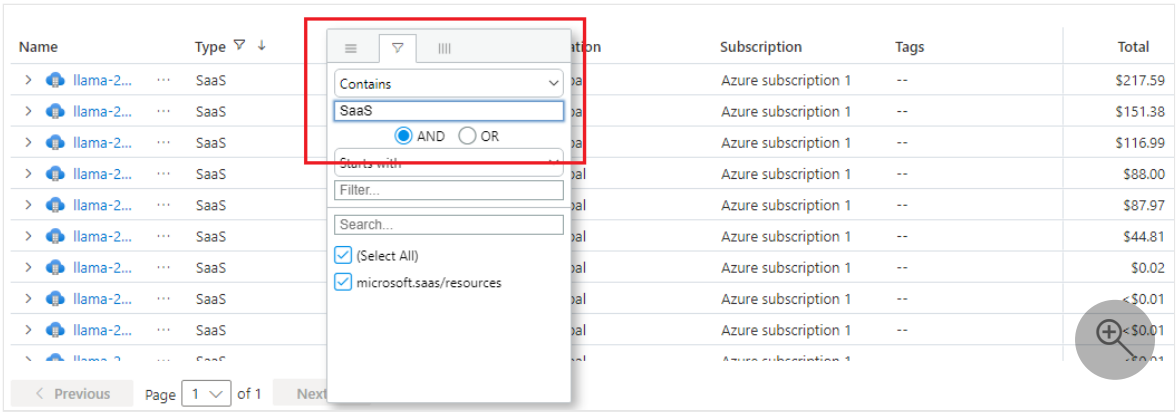
Azure Marketplace を通じて提供されるモデルのコストを監視する

従量課金制を使用してサービスとしてデプロイされたモデルは、Azure Marketplace を通じて提供されます。 モデルの公開元は、オファリングに応じて異なるコストを適用する場合があります。 Azure AI Studio の各プロジェクトには、オファリングを含む独自のサブスクリプションがあり、これによりそのプロジェクトで発生しているコストと消費量を監視できます。 次のように Microsoft Cost Management を使ってコストを監視します。

1. Azure ポータル にサインインします。
2. 左側のナビゲーション領域で、**[Cost Management と Billing]** を選択し、同じメニューで **[Cost Management]** を選択します。
3. 左側のナビゲーション領域で、**[Cost Management]** セクションで、**[コスト分析]** を選択します。
4. **[リソース]** などのビューを選択します。 各リソースに関連付けられているコストが表示されます。



5. **[種類]** 列で、フィルター アイコンを選択して、**[microsoft.saas/resources]** の種類のすべてのリソースをフィルター処理します。 この種類は、Azure Marketplace のオファーから作成されたリソースに対応します。 便宜上、**SaaS** 文字列を含むリソースの種類でフィルター処理できます。

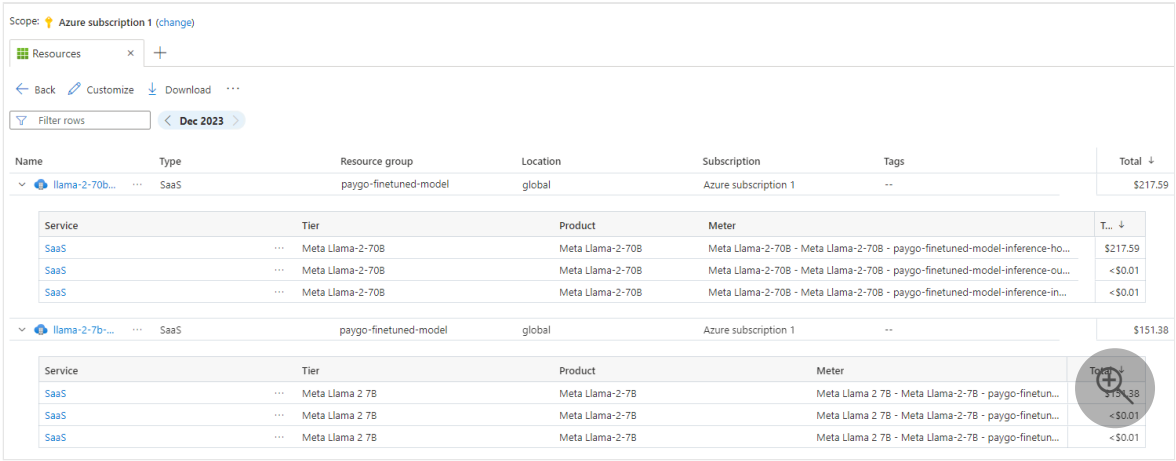


6. プロジェクトごとに各モデル オファーに対して 1 つのリソースが表示されます。 これらのリソースの名前付けは `[Model offer name]-[GUID]` です。

7. 選択してリソースの詳細を展開し、リソースに関連付けられている各コスト メーターにアクセスします。

   - **[レベル]** は、オファリングを表します。
   - **[製品]** は、オファリング内の特定の製品です。

   一部のモデル プロバイダーは、両方に同じ名前を使用する場合があります。



> **ヒント**
>
> プロジェクトがサブスクライブしている各プランごとに、各プロジェクトごとに 1 つのリソースが作成されることに注意してください。

8. 詳細を展開すると、オファリングに関連付けられている各メーターごとにコストが報告されます。 各メーターは、推論や微調整など、さまざまなコストのソースを追跡できます。 次のメーターが表示されます (一部のコストが関連付けられている場合)。

テーブルを展開する

測定	グループ	説明
`paygo-inference-input-tokens`	基本モデル	基本モデルの推論の入力として使用されるトークンに関連付けられているコスト。
`paygo-inference-output-tokens`	基本モデル	基本モデルの推論の出力として生成されるトークンに関連付けられているコスト。
`paygo-finetuned-model-inference-hosting`	微調整されたモデル	微調整されたモデルの推論エンドポイントのホスティングに関連するコスト。 これはモデルをホスティングするコストではなく、エンドポイントがモデルを提供するコストです。
`paygo-finetuned-model-inference-input-tokens`	微調整されたモデル	微調整されたモデルの推論の入力として使用されるトークンに関連付けられたコスト。
`paygo-finetuned-model-inference-output-tokens`	微調整されたモデル	微調整されたモデルの推論の出力として生成されるトークンに関連付けられたコスト。

予算を作成する

予算を作成して、コストを管理し、異常な支出や浪費のリスクについて、関係者に自動的に通知するアラートを作成できます。 アラートは、予算とコストのしきい値と比較した支出に基づきます。 予算とアラートは、Azure サブスクリプションとリソース グループに対して作成されるため、全体的なコスト監視戦略の一環として役立ちます。

監視の粒度をさらに細かく示す必要がある場合は、Azure の特定のリソースまたはサービスに対するフィルターを使用して予算を作成できます。 フィルターを使用すると、追加のコストがかかる新しいリソースが誤って作成されないようにすることができます。 予算を作成するときのフィルター オプションの詳細については、グループとフィルターのオプションに関する記事を参照してください。

コスト データのエクスポート

また、ストレージ アカウントにコスト データをエクスポートすることもできます。 これは、自分や他のユーザーがコストに関する追加のデータ分析を行う必要がある場合に便利です。 たとえば、財務チームは、Excel や Power BI を使用してデータを分析できます。 日単位、週単位、または月単位のスケジュールでコストをエクスポートし、カスタムの日付範囲を設定することができます。 コスト データのエクスポートは、推奨されるコスト データセット取得方法です。

Azure AI サービスの詳細な課金モデルを理解する

Azure AI サービスは、新しいリソースをデプロイすると Azure AI と併せてコストが発生する Azure インフラストラクチャ上で実行されます。 追加のインフラストラクチャでコストが発生する可能性があることを理解しておくことが重要です。 デプロイされたリソースに変更を加える場合は、このコストを管理する必要があります。

Azure AI サービス リソースを作成または使用すると、使用するサービスに基づいて課金される場合があります。 Azure AI サービスに使用できる課金モデルには、次の 2 種類があります。

- 従量課金制: 従量課金制の価格では、課金情報に基づいて、使用した Azure AI サービス内容に従って課金されます。
- コミットメント レベル: コミットメント レベルの価格では、いくつかのサービス機能を固定料金で使用することをコミットします。これにより、ワークロードのニーズに基づいて合計コストが予測可能になります。 選択したプランに従って課金されます。 利用可能なサービス、サインアップする方法、プランを購入する際の考慮事項については、「クイックスタート: コミットメント レベル価格で購入する」を参照してください。

> ⓘ **注意**
>
> コミットメント プランによって指定されたクォータを超えるリソースを使用した場合、コミットメント プランの購入時に Azure portal に規定されている超過分に従い、追加の使用量に対して課金されます。

Azure AI サービスの料金は、Azure 前払い (旧称: 年額コミットメント) のクレジットを使用して支払うことができます。 ただし、Azure 前払いのクレジットを使用して、サードパーティの製品やサービス (Azure Marketplace からのものを含む) の料金を支払うことはできません。

詳細については、Azure の料金計算ツール に関するページをご覧ください。

次のステップ

- Azure Cost Management を使用してクラウドへの投資を最適化する方法について説明します。
- コスト分析を使用してコストを管理する方法について詳細に説明します。
- 予期しないコストを回避する方法について説明します。
- Cost Management のガイド付き学習コースを受講します。

AI サービスの上限を自動スケーリングする

[アーティクル] • 2024/01/20

この記事では、お客様が Azure AI サービス リソースでより高いレート制限を利用する方法に関するガイダンスを提供します。

概要

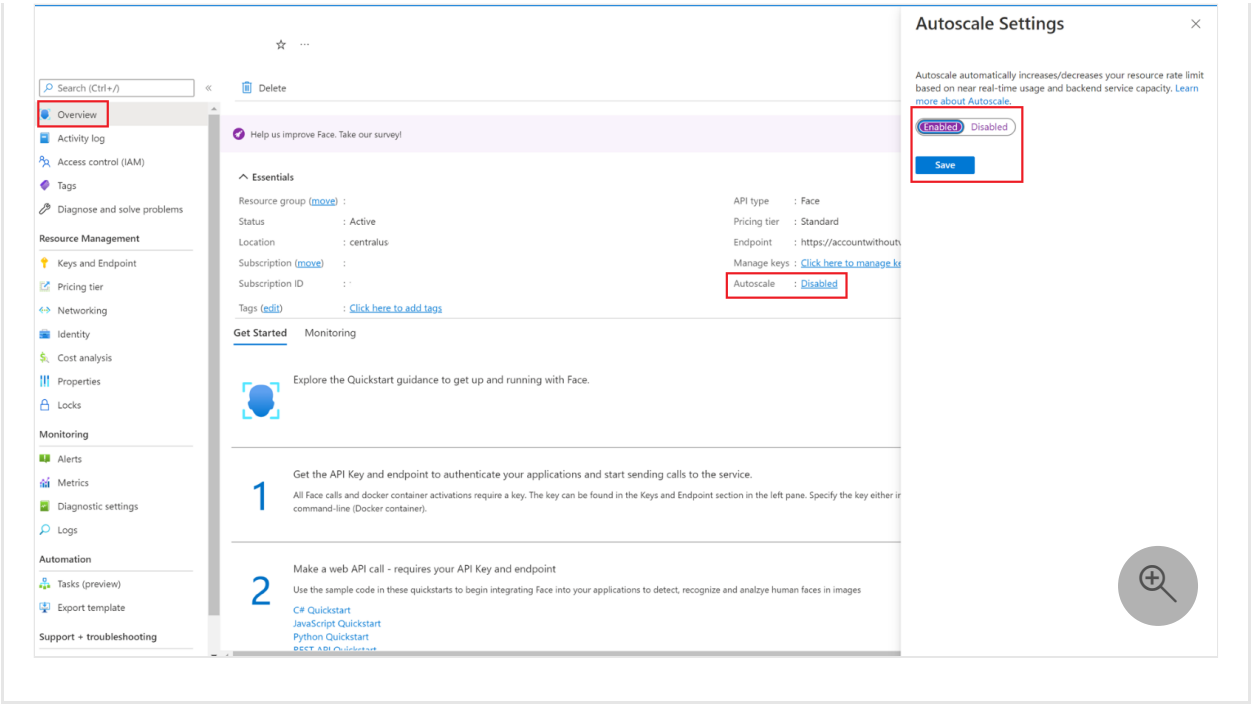
個々の Azure AI サービス リソースには、事前に構成された静的な呼び出しレート (1 秒あたりのトランザクション数) があり、これによって、一定の概算時間内にお客様がバックエンド サービスに対して行うことができる同時呼び出しの数が制限されます。 自動スケーリング機能は、ほぼリアルタイムのリソース使用量メトリックとバックエンド サービス容量メトリックに基づいて、お客様のリソースのレート制限を自動的に増減します。

自動スケーリング機能の概要

すべての新しいリソースで、この機能は既定で無効です。 以下の手順に従って、有効化してください。

Azure Portal

Azure portal でリソースのページに移動し、左側のペインで **[概要]** タブを選択します。 **[要点]** セクションで、**[自動スケール]** の行を探してリンクを選択し、**[自動スケール設定]** ペインを表示して機能を有効にします。



よく寄せられる質問

自動スケーリング機能を有効にすると、リソースは二度と帯域幅調整されなくなるのですか?

いいえ。レート制限超過の `429` エラーは引き続き発生する可能性があります。 アプリケーションでスパイクが発生し、リソースから `429` 応答が報告された場合、自動スケーリングは、現在の容量がレート制限の増加に対応できるかどうかを確認するために、使用可能な容量予測セクションをチェックし、5 分以内に応答します。

使用可能な容量が増加に対して十分な場合は、自動スケーリングによってリソースのレート制限の上限が徐々に引き上げられます。 `429` 帯域幅調整がさらに発生する高いレートでリソースの呼び出しを続けた場合、TPS レートは時間の経過と共に増加し続けます。 このアクションが 1 時間以上続くと、その時点でそのリソースに対して利用可能な最大レート (最大 1000 TPS) に達します。

使用可能な容量が増加に対して十分でない場合、自動スケーリング機能は 5 分間待機し、もう一度チェックします。

既定のレート制限の引き上げが必要な場合、どうすればよいですか?

既定では、Azure AI サービス リソースの既定のレート制限は 10 TPS です。 既定の TPS の引き上げが必要な場合は、Azure portal のリソースのページにある [**新しいサポート**

要求] リンクからチケットを送信してください。 要求に業務上の正当な理由を含めるのを忘れないでください。

この機能によって Azure の支出が増加しますか?

Azure AI サービスの価格は変更されておらず、こちらからご確認いただけます。 Azure AI サービス API の呼び出しが成功した場合にのみ請求が発生します。 ただし、呼び出しレート制限の引き上げに伴って、トランザクションの完了数が増加し、請求額が増加する場合があります。

エラーの可能性とその結果にご注意ください。 クライアント アプリケーションのバグによって 1 秒あたり数百回のサービス呼び出しが発生した場合、請求額が大幅に増加する可能性がありますが、レート制限が固定されていれば費用はかなり抑制されます。 この種のエラーはお客様の責任となります。 自動スケーリング機能をご使用になる前に、固定レート制限のリソースに対して開発テストとクライアント更新テストを実行することを強くお勧めします。

不測の支出が発生しないようにレートを制限したい場合、この機能を無効にできますか?

はい。Azure portal または CLI を使用して自動スケーリング機能を無効にし、既定のレート制限設定に戻すことができます。 より高い既定の TPS がリソースで以前に承認されていた場合、そのレートに戻ります。 変更が有効になるまでに最大 5 分ほどかかることがあります。

どのサービスで自動スケーリング機能がサポートされますか?

自動スケーリング機能は、次のサービスで使用できます。

- Azure AI サービス マルチキー
- Azure AI Vision
- Language (感情分析、キー フレーズ抽出、固有表現認識、Text Analytics for Health でのみ使用可能)
- Anomaly Detector
- Content Moderator
- Custom Vision (Prediction)
- Immersive Reader
- LUIS
- Metrics Advisor
- Personalizer

- QnA Maker
- Document Intelligence

無料のサブスクリプションを使用してこの機能をテストできますか?

いいえ。自動スケーリング機能は Free レベルのサブスクリプションでは使用できません。

次のステップ

- Azure AI サービスのコストを計画および管理する。
- Azure Cost Management でクラウド投資を最適化します。
- 予期しないコストを回避する方法について説明します。
- Cost Management のガイド付き学習コースを受講します。

コミットメント レベル価格で購入する

[アーティクル] • 2024/01/22

Azure AI ではコミットメント レベル価格が提供されており、従量課金制の価格モデルと比べて割引になります。 コミットメント レベル価格では、次の Azure AI サービス機能を固定料金で使用できるようになり、これによってワークロードのニーズに基づく合計コストが予測可能になります。

- 音声テキスト変換 (Standard)
- テキスト読み上げ (ニューラル)
- テキスト翻訳 (標準)
- Language Understanding 標準 (テキスト要求)
- Azure AI 言語
  - 感情分析
  - キー フレーズ抽出
  - 言語検出
  - 名前付きエンティティの認識 (NER)
- Azure AI Vision - OCR
- Document Intelligence - カスタム/請求書

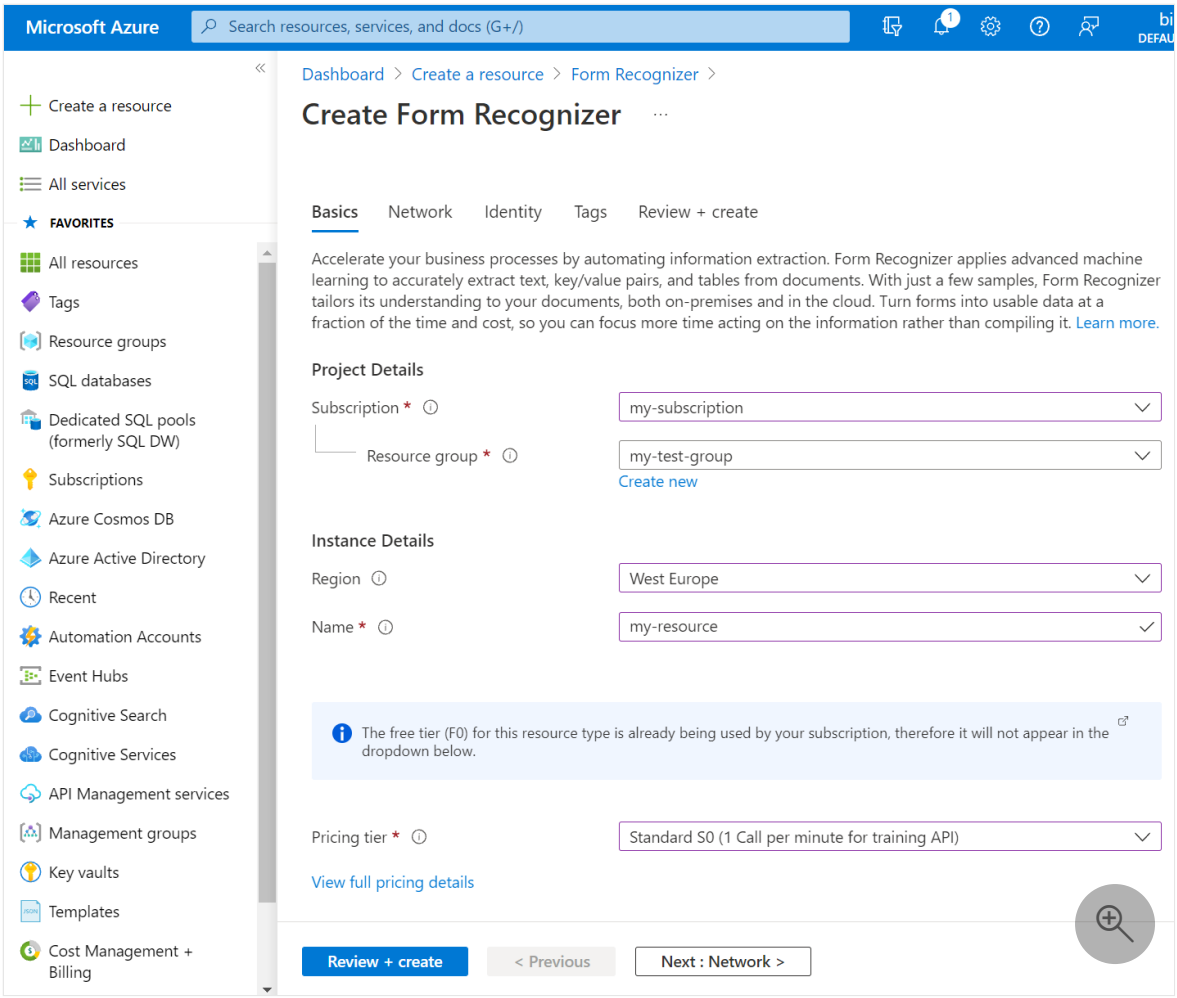
詳しくは、「Azure AI サービスの価格」をご覧ください。

新しいリソースを作成

1. Azure portal にサインインし、一覧にある該当するいずれかの Azure AI サービスに対して **[新しいリソースを作成する]** を選択します。

2. リソースを作成するための該当する情報を入力します。 必ず Standard 価格レベルを選択してください。

> **注意**
>
> 切断されたコンテナーの使用に対してコミットメント レベルを購入する場合は、個別のアクセスを要求し、**[コミットメント レベルの切断済みコンテナー]** 価格レベルを選択する必要があります。 詳細については、「**切断されたコンテナー**」を参照してください。



3. リソースが作成されると、従量課金制からコミットメント プランに価格を変更できるます。

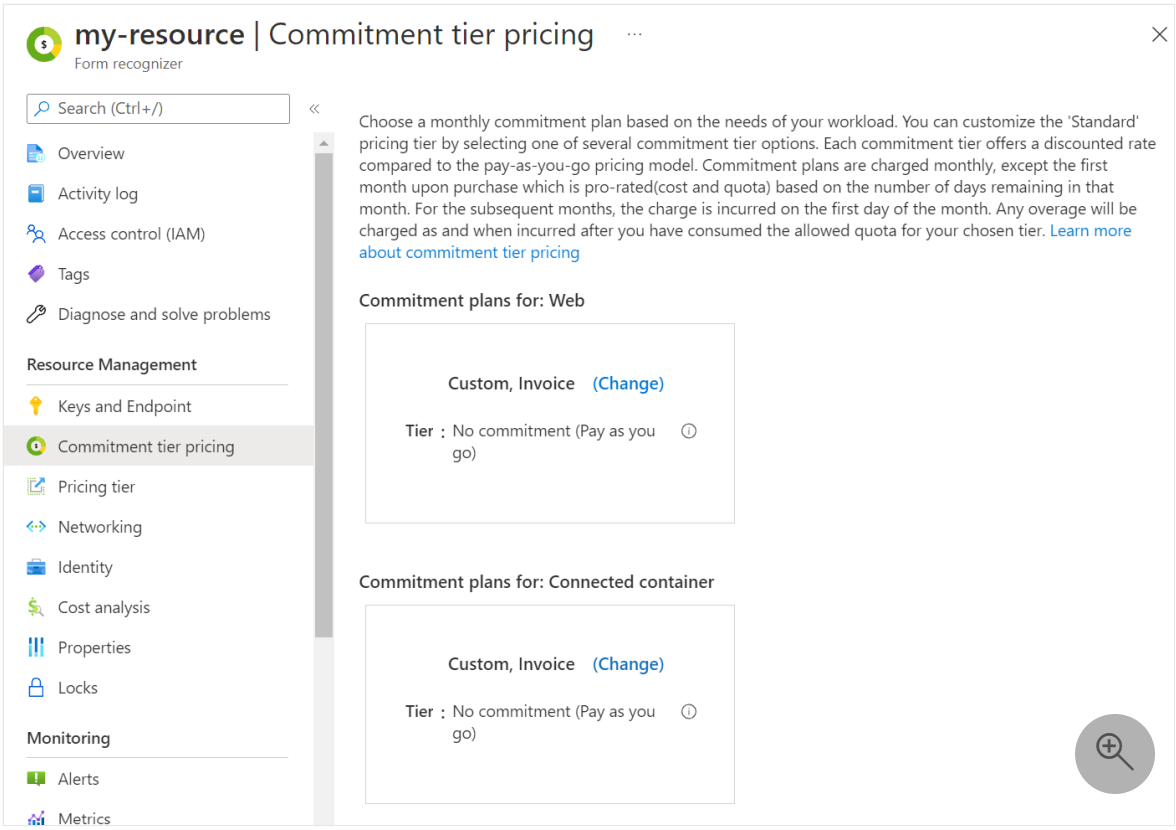
Azure リソースを更新してコミットメント プランを購入する

1. 自分の Azure サブスクリプションを使用して、Azure portal にサインインします。

2. 一覧表示されている該当する機能のいずれかの Azure リソースで、**[コミットメント レベルの価格]** を選択します。

3. **[変更]** を選択して、ホストされている API とコンテナーの使用に関して利用可能なコミットメントを表示します。 次の 1 つ以上のオファリングのコミットメント プランを選択します。

    - **Web**: 処理のために Azure にデータを送信する、Web ベースの API。
    - **接続されたコンテナー**: Azure AI サービスをオンプレミスでデプロイでき、課金と測定のためにインターネット接続を維持できる Docker コンテナー。



4. 表示されるウィンドウで、 **[レベル]** と **[自動更新]** の両方のオプションを選択します。

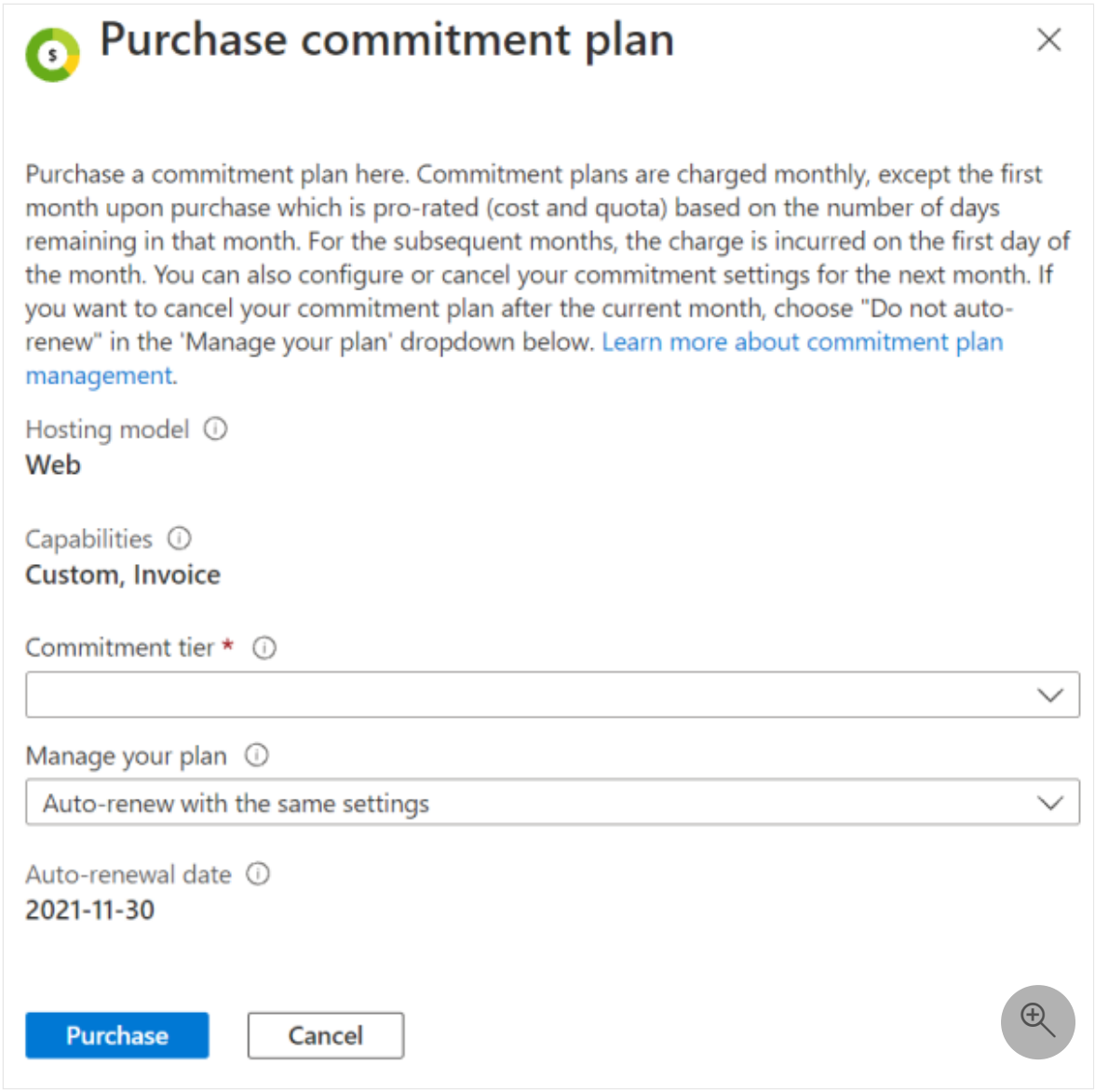
   - **[コミットメント レベル]** - 機能のコミットメントレベル。 コミットメントレベルは **[購入]** を選択した時点ですぐに有効になり、コミットメント金額は日割り計算で課金されます。

   - **[自動更新]** - 次回の請求サイクルから、現在のコミットメント プランを更新、変更、またはキャンセルする方法を選択します。 自動更新を選択した場合、**[自動更新の日付]** は、次回の請求サイクルに対して課金される (ローカル タイムゾーンの) 日付になります。 この日付は、カレンダー月の開始日と一致します。

⊗ 注意事項

[購入] を選択すると、選択したレベルに対して課金されます。 購入すると、コミットメント プランは払い戻しできません。

コミットメント プランは月単位で課金されます。ただし、購入の最初の月は、その月の残りの日数に基づいて日割り計算されます (コストとクォータ)。 翌月以降は、月の最初の日に料金が発生します。



超過分の価格

指定されたクォータを超えるリソースを使用した場合、コミットメント レベルに規定されている超過分に従い、追加の使用量に対して課金されます。

別のコミットメント プランを購入する

コミットメント プランのコミットメント期間は、カレンダー月の 1 か月です。 コミットメント プランは、既定の従量課金制の価格モデルの利用中にいつでも購入できます。 プランを購入すると、月の残りの期間は日割り料金が課金されます。 コミットメント期間中は、現在の月のコミットメント プランを変更できません。 ただし、カレンダー月の翌月について別のコミットメント プランを選択できます。 翌月分の請求は、翌月の最初の日に行われます。

提供されているものよりも大きなコミットメント プランが必要な場合は、`csgate@microsoft.com` にお問い合わせください。

コミットメント プランを終了する

コミットメント プランの購入を継続しない場合、リソースの自動更新を **[自動更新しない]** に設定することができます。 コミットメント プランは、表示されたコミットメントの終了日に期限切れになります。 この日以降、コミットメント プランの料金は課金されません。 引き続き Azure リソースを使用して API を呼び出すことができ、従量課金制の料金で課金されます。 各月の最終日の午前 0 時 (UTC) までコミットメント プランを終了することができ、その場合次の月に対しては課金されません。

切断されたコンテナーのためにコミットメント レベルの料金プランを購入する

切断されたコンテナーのコミットメント プランには、暦年のコミットメント期間があります。 これらは、Web および接続されたコンテナーのコミットメント プランとは異なるプランです。 コミットメント プランを購入すると、すぐに価格の全額が課金されます。 コミットメント期間中にコミットメント プランを変更することはできませんが、年間の残りの日数については、日割り計算の価格で追加のユニットを購入できます。 コミットメントの最終日の午前 0 時 (UTC) までコミットメント プランを終了することができます。

リソースの **[Commitment Tier pricing]** (**コミットメント レベルの価格**) 設定で別のコミットメント プランを選択できます。

切断されたコンテナーの超過分の価格

切断されたコンテナーのコミットメント プランで最初に購入したクォータを超える切断されたコンテナーを使用するには、コミットメント プランを更新することで追加のクォータをいつでも購入できます。

追加のクォータを購入するには、Azure portal でリソースに移動し、切断されたコンテナーのコミットメント プランの "ユニット数" を、スライダーを使って調整します。 これを行うと、追加の月間クォータが追加され、現在の請求期間の残り日数に基づく日割り料金が課金されます。

関連項目

- Azure AI サービスの価格 。

Azure AI サービスの診断ログを有効にする

[アーティクル] • 2024/01/20

このガイドでは、Azure AI サービスの診断ログを有効にするための詳細な手順について説明します。 これらのログでは、問題の識別やデバッグに使用されるリソースの操作に関する豊富で頻繁なデータが提供されます。 続行する前に、少なくとも 1 つの Azure AI サービス (音声サービス など) へのサブスクリプションを持つ Azure アカウントが必要です。

前提条件

診断ログを有効にするには、ログ データを格納する場所が必要になります。 このチュートリアルでは、Azure Storage と Log Analytics を使用します。

- Azure Storage - ポリシー監査、静的解析、またはバックアップの診断ログを保持します。 設定を構成するユーザーが両方のサブスクリプションに対して適切な Azure RBAC アクセスを持っている限り、ストレージ アカウントはログを出力するリソースと同じサブスクリプションに属している必要はありません。
- Log Analytics - Azure リソースによって生成された生ログの分析を可能にする柔軟なログ検索および分析ツール。

> ⓘ **注意**
>
> - その他の構成オプションも使用できます。 詳細については、**Azure リソースからのログ データの収集と使用**に関するページを参照してください。
> - 診断ログの "トレース" は、**カスタムの質問と回答**にのみ使用できます。

診断ログの収集を有効にする

最初に、Azure portal を使用して診断ログを有効にします。

> ⓘ **注意**
>
> PowerShell または Azure CLI を使用してこの機能を有効にするには、**Azure リソースからのログ データの収集と使用**に関するページに示されている手順を使用します。

1. Azure Portal に移動します。 次に、Azure AI サービス リソースを見つけて選択します。 たとえば、音声サービスのサブスクリプションです。
2. 次に、左側のナビゲーション メニューから、 **[監視]** を見つけて **[診断設定]** を選択します。 この画面には、このリソースに対して前に作成したすべての診断設定が含まれています。
3. 前に作成したリソースで使用したいものが存在する場合は、ここでそれを選択できます。 それ以外の場合は、 **[+ Add diagnostic setting] (+ 診断設定の追加)** を選択します。
4. 設定の名前を入力します。 次に、 **[ストレージ アカウントへのアーカイブ]** および **[Log Analytics への送信]** を選択します。
5. 構成するよう求めるメッセージが表示されたら、診断ログを格納するために使用するストレージ アカウントと OMS ワークスペースを選択します。 **注**:ストレージ アカウントまたは OMS ワークスペースがない場合は、プロンプトに従って作成してください。
6. **[Audit]** 、 **[RequestResponse]** 、および **[AllMetrics]** を選択します。 次に、診断ログ データの保持期間を設定します。 保持ポリシーが 0 に設定されていると、そのログ カテゴリのイベントは無期限に格納されます。
7. **[保存]** を選択します。

ログ データがクエリや分析に使用できるようになるまでに最大 2 時間かかることがあります。 そのため、すぐには何も表示されなくても気にしないでください。

Azure Storage の診断データを表示およびエクスポートする

Azure Storage は、大量の非構造化データを格納するために最適化された、強力なオブジェクト ストレージ ソリューションです。 このセクションでは、ストレージ アカウントにクエリを実行して 30 日間の合計トランザクションを取得し、そのデータを Excel にエクスポートする方法について説明します。

1. Azure portal から、最後のセクションで作成した Azure Storage リソースを見つけます。
2. 左側のナビゲーション メニューから、 **[監視]** を見つけて **[メトリック]** を選択します。
3. 使用可能なドロップダウンを使用してクエリを構成します。 この例では、時間範囲を **[過去 30 日間]** に、メトリックを **[トランザクション]** に設定します。
4. クエリが完了すると、過去 30 日間のトランザクションの視覚化が表示されます。 このデータをエクスポートするには、ページの上部にある **[Excel へのエクスポート]** ボタンを使用します。

診断データで実行できる操作の詳細については、Azure Storage に関するページを参照してください。

Log Analytics ログを表示する

リソースに対するログ分析データを調査するには、次の手順に従います。

1. Azure portal で、左側のナビゲーション メニューから **[Log Analytics]** を見つけて選択します。
2. 診断を有効にするときに作成したリソースを見つけて選択します。
3. **[全般]** で、 **[ログ]** を見つけて選択します。 このページから、ログに対してクエリを実行できます。

サンプル クエリ

ログ データを調査するために使用できるいくつかの基本的な Kusto クエリを次に示します。

指定した期間の Azure AI サービスのすべての診断ログを表示するには、次のクエリを実行します。

Kusto

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
```

最新の 10 件のログを表示するには、次のクエリを実行します。

Kusto

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
| take 10
```

リソースで操作をグループ化するには、次のクエリを実行します。

Kusto

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.COGNITIVESERVICES" |
summarize count() by Resource
```

操作を実行するためにかかる平均時間を見つけるには、次のクエリを実行します。

Kusto

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
| summarize avg(DurationMs)
by OperationName
```

OperationName によって分割された一定期間の操作の量と、10 秒ごとにビン分割された数を表示するには、次のクエリを実行します。

Kusto

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
| summarize count()
by bin(TimeGenerated, 10s), OperationName
| render areachart kind=unstacked
```

次のステップ

- ログ記録を有効にする方法、および各種の Azure サービスでサポートされているメトリックやログのカテゴリを理解するには、Microsoft Azure でのメトリックの概要に関するページとAzure 診断ログの概要に関するページを参照してください。
- Event Hubs については次の記事をご覧ください。
  - Azure Event Hubs とは
  - Event Hubs の使用
- 「Azure Monitor ログでのログ検索について」をお読みください。

削除された Azure AI サービス リソースの復旧または消去

[アーティクル] • 2023/11/15

この記事では、既に削除されている Azure AI サービス リソースを復旧または消去する方法について説明します。

リソースを削除すると、48 時間は同じ名前で別のリソースを作成することはでません。 同じ名前のリソースを作成するには、削除したリソースを消去する必要があります。

> ⓘ **注意**
>
> この記事の手順は、マルチサービス リソースと単一サービス リソースの両方に適用されます。 マルチサービス リソースでは、1 つのキーとエンドポイントを使用して複数の Azure AI サービスにアクセスできます。 一方、単一サービス リソースでは、リソースが作成された特定の Azure AI サービスのみにアクセスできます。

削除されたリソースを復旧する

削除されたリソースを復旧するには、次の前提条件を満たす必要があります。

- 復旧するリソースは、過去 48 時間以内に削除されたものである必要があります。
- 復旧するリソースは、まだ消去されていない必要があります。 消去されたリソースを復旧できません。
- 削除されたリソースの復旧を試みる前に、そのアカウントのリソース グループが存在することを確認してください。 リソース グループが削除されている場合は、再作成する必要があります。 リソース グループを復旧することはできません。 詳しくは、リソース グループの管理に関する記事をご覧ください。
- 削除されたリソースによって Azure Key Vault でカスタマー マネージド キーが使用されていて、キー コンテナーも削除されている場合は、Azure AI サービス リソースを復元する前に、そのキー コンテナーを復元する必要があります。 詳細については、Azure Key Vault の復旧の管理に関する記事を参照してください。
- 削除されたリソースによってユーザーが管理するストレージが使用されていて、そのストレージ アカウントも削除されている場合は、Azure AI サービス リソースを復元する前に、そのストレージ アカウントを復元する必要があります。 詳細については、「削除されたストレージ アカウントを復旧する」を参照してください。

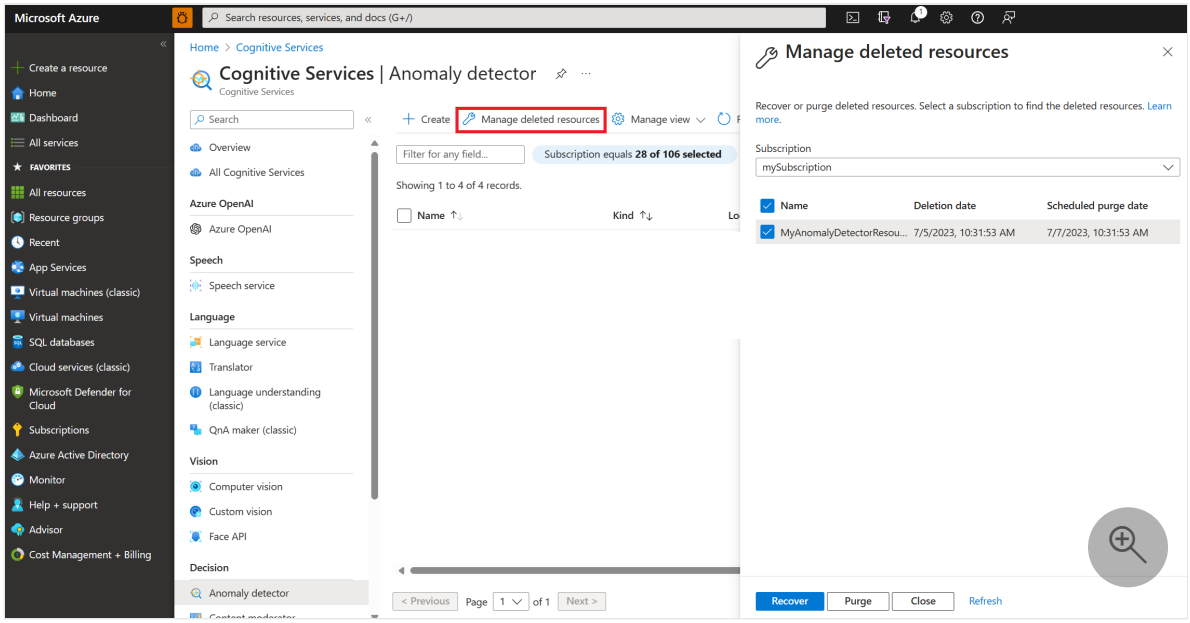
削除された Azure AI サービス リソースを復旧するには、次のコマンドを使用します。 該当する場合は、次のように置き換えます。

- `{subscriptionID}` は Azure サブスクリプション ID
- `{resourceGroup}` はリソース グループ
- `{resourceName}` はリソース名
- `{location}` はリソースの場所

Azure Portal

削除されたリソースを復旧する必要がある場合は、Azure AI サービス API の種類のハブに移動し、メニューから [Manage deleted resources] (削除されたリソースの管理) を選択します。 たとえば、"Anomaly Detector" リソースを復旧する場合は、検索バーで "Anomaly Detector" を検索し、サービスを選択します。 その後、**[削除されたリソースの管理]** を選択します。

ドロップダウン リストでサブスクリプションを選択して、復旧する削除されたリソースを見つけます。 削除されたリソースを 1 つ以上を選択し、**[復旧する]** を選択します。



> **注意**
>
> 削除されたリソースが復旧してリソースの一覧に表示されるまでに数分かかる場合があります。 メニューの **[最新の情報に更新]** ボタンを選択して、リソースの一覧を更新します。

削除されたリソースを消去する

サブスクリプションには、Cognitive Services 共同作成者または共同作成者などのリソースを消去するための `Microsoft.CognitiveServices/locations/resourceGroups/deletedAccounts/delete` アクセス許可が必要です。

`Contributor` を使用してリソースを消去する場合、ロールはサブスクリプション レベルで割り当てる必要があります。 ロールの割り当てがリソースまたはリソース グループ レベルでのみ存在する場合は、消去機能にアクセスできません。

削除された Azure AI サービス リソースを消去するには、次のコマンドを使用します。 該当する場合は、次のように置き換えます。

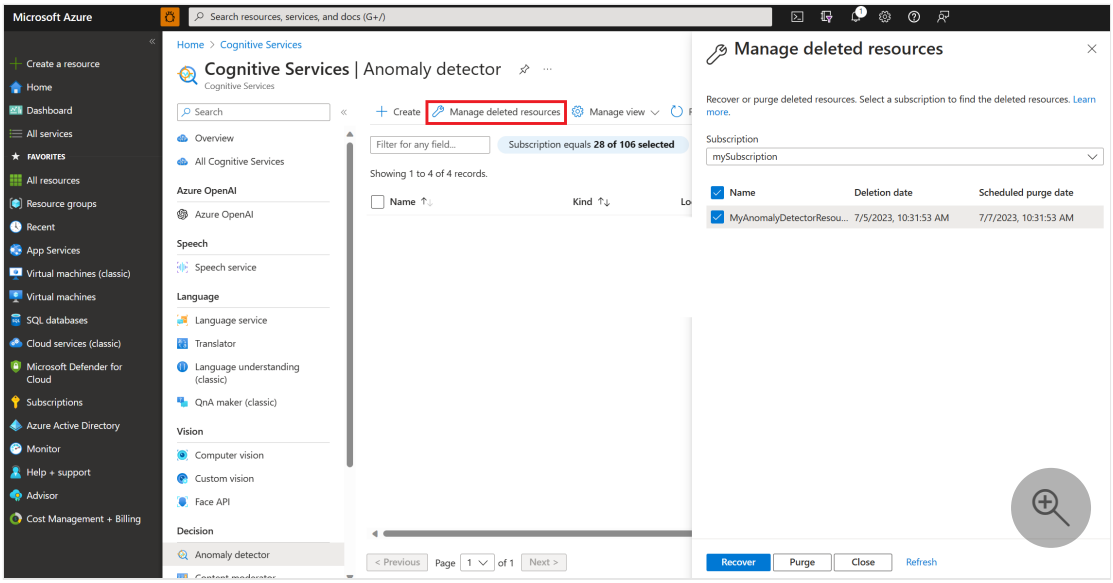
- `{subscriptionID}` は Azure サブスクリプション ID
- `{resourceGroup}` はリソース グループ
- `{resourceName}` はリソース名
- `{location}` はリソースの場所

> **注意**
>
> リソースが消去されると、完全に削除され、復元できなくなります。 リソースに関連付けられているすべてのデータとキーが失われます。

Azure Portal

削除されたリソースを消去する必要がある場合は、削除されたリソースの回復と同様の手順で行います。

1. 削除されたリソースの Azure AI サービス API の種類のハブに移動します。 たとえば、"Anomaly Detector" リソースを消去する場合は、検索バーで "Anomaly Detector" を検索し、サービスを選択します。 その後、メニューから **[削除されたリソースの管理]** を選択します。
2. ドロップダウン リストでサブスクリプションを選択して、消去する削除されたリソースを見つけます。
3. 削除されたリソースを 1 つ以上を選択し、**[削除]** を選択します。 消去すると、Azure AI サービス リソースが完全に削除されます。



関連項目

- マルチサービス リソースを作成する
- ARM テンプレートを使用して新しいリソースを作成する

Azure AI コンテナーとは

[アーティクル] • 2023/08/28

Azure AI サービスには、Docker コンテナーがいくつか用意されており、これにより、Azure で使用できるものと同じ API をオンプレミスで使用できます。 これらのコンテナーを使用すると、コンプライアンス、セキュリティ、またはその他の運用上の理由でデータの近くで Azure AI サービスを使用することが柔軟に可能になります。 現在、コンテナー サポートは Azure AI サービスのサブセットで利用できます。

https://www.youtube-nocookie.com/embed/hdfbn4Q8jbo

コンテナー化とは、アプリケーションまたはサービスとその依存関係や構成をコンテナー イメージとしてパッケージ化するソフトウェア配布のアプローチです。 コンテナー イメージは、ほとんどまたはまったく変更せずに、コンテナー ホストにデプロイできます。 コンテナーは、相互および基になるオペレーティング システムから分離され、仮想マシンよりもフット プリントが小さくなります。 短期間のタスクに対してコンテナーをコンテナー イメージからインスタンス化し、不要になったら削除できます。

機能とメリット

- **イミュータブル インフラストラクチャ**: DevOps チームが、一貫性と信頼性のある既知のシステム パラメーターのセットを活用しながら、変更に適応できるようにします。 コンテナーには、予測可能なエコシステム内でピボットして構成の誤差を回避できる柔軟性があります。
- **データの制御**: Azure AI サービスによってデータが処理される場所を選択します。これは、クラウドにはデータを送信できないものの、Azure AI サービスの API にアクセスする必要がある場合に不可欠です。 ハイブリッド環境でデータ、管理、ID、セキュリティの整合性をサポートします。
- **モデルの更新の制御**:ソリューションにデプロイされているモデルのバージョン管理と更新を柔軟に行うことができます。
- **移植可能なアーキテクチャ**:Azure、オンプレミス、エッジにデプロイできる移植可能なアプリケーション アーキテクチャを作成できます。 コンテナーは、Azure Kubernetes Service、Azure Container Instances、または Azure Stack にデプロイされた Kubernetes クラスターに直接デプロイできます。 詳しくは、「Kubernetes を Azure Stack にデプロイする」をご覧ください。
- **高スループット/低待ち時間**: アプリケーションのロジックとデータに物理的に近い場所で Azure AI サービスを実行できるようにすることで、高スループットと低遅延の要件に合わせてスケーリングできる機能を顧客に提供します。 コンテナーでは、1 秒あたりのトランザクション数 (TPS) は制限されません。必要なハードウェア リソースを提供した場合は、コンテナーのスケールアップとスケールアウトの両方を行って需要を処理することができます。

- **スケーラビリティ**:コンテナー化とコンテナー オーケストレーション ソフトウェア (Kubernetes など) がますます普及し、スケーラビリティは、技術進歩の最前線にあります。 スケーラブルなクラスター基盤の上に構築されたアプリケーション開発は、高可用性に対応します。

Azure AI サービスのコンテナー

Azure AI コンテナーでは、次の Docker コンテナー セットが提供されます。各コンテナーには、Azure AI サービスのサービスの機能のサブセットが含まれます。 以下の表で説明とイメージの場所を確認できます。

> ⓘ **注意**
>
> **Azure AI Document Intelligence** コンテナーの手順とイメージの場所については、Intelligence **コンテナーのインストールと実行に関するドキュメント**を参照してください。

デシジョン コンテナー

サービス	コンテナー	説明	可用性
Anomaly Detector	**Anomaly Detector** (イメージ)	Anomaly Detector API では、機械学習を利用することで、時系列データを監視し、その中の異常を検出できます。	一般公開

言語コンテナー

サービス	コンテナー	説明	可用性
LUIS	**LUIS** (イメージ)	トレーニング済みまたは発行済みの Language Understanding モデル ("LUIS アプリ" と呼ばれます) を Docker コンテナーに読み込みます。ユーザーは、そのコンテナーの API エンドポイントからクエリ予測を利用することができます。 コンテナーからクエリのログを収集し、それらを LUIS ポータル に再度アップロードすることで、アプリの予測精度を高めることができます。	一般提供されています。 このコンテナーは、切断された環境でも実行できます。
言語サービス	**キー フレーズ抽出** (イメージ)	主なポイントを識別するキー フレーズを抽出します。 たとえば、「食べ物はおいしくて、すばらしいスタッフがいた」というテキストを入力すると、このコンテ	一般提供されています。 このコンテ

サービス	コンテナー	説明	可用性
		API は話題の中心として "食べ物" と "すばらしいスタッフ" を返します。	ナーは、切断された環境でも実行できます。
言語サービス	**テキスト言語検出** (イメージ)	最大 120 の言語に対して、入力テキストが書かれている言語を検出し、要求で送信されたドキュメントごとに 1 つの言語コードを報告します。 言語コードは、評価値の強度を示すスコアと組みになります。	一般提供されています。 このコンテナーは、切断された環境でも実行できます。
言語サービス	**感情分析** (イメージ)	肯定的または否定的な感情の手がかりを探して未加工のテキストを分析します。 このバージョンの感情分析からは、各ドキュメントとその中の文のセンチメント ラベル (たとえば、"肯定的"、"否定的") が返されます。	一般提供されています。 このコンテナーは、切断された環境でも実行できます。
言語サービス	**Text Analytics for Health** (画像)	構造化されていない臨床テキストから医療情報を抽出してラベル付けします。	一般公開
言語サービス	**カスタム固有表現認識** (イメージ)	データを使用して作成するカスタム モデルを使用して、テキストから固有表現を抽出します。	プレビュー
Language サービス	**概要作成** (画像)	さまざまなソースからテキストの概要を作成します。	一般提供されています。 このコンテナーは、切断された環境でも実行できます。
Translator	**Translator** (画像)	複数の言語と方言にテキストを翻訳できます。	一般提供されています。 限定的 - アクセス権を要求してください。 このコンテ

サービス	コンテナー	説明	可用性
			ナーは、切断された環境でも実行できます。

音声コンテナー

サービス	コンテナー	説明	可用性
Speech Service API	**音声テキスト変換** (イメージ)	連続するリアルタイムの音声をテキストに書き起こします。	一般提供されています。 このコンテナーは、切断された環境でも実行できます。
Speech Service API	**カスタム音声テキスト変換** (イメージ)	カスタム モデルを使用して、連続するリアルタイムの音声をテキストに書き起こします。	一般公開 このコンテナーは、切断された環境でも実行できます。
Speech Service API	**ニューラル テキスト読み上げ** (イメージ)	ディープ ニューラル ネットワーク テクノロジを使用してテキストを自然な響きの音声に変換することで、合成音声がより自然なものになります。	一般提供されています。 このコンテナーは、切断された環境でも実行できます。
Speech Service API	**音声言語検出** (イメージ)	音声の言語を特定します。	プレビュー

ビジョン コンテナー

サービス	コンテナー	説明	可用性
Azure AI Vision	**Read OCR** (イメージ)	Read OCR コンテナーを使用すると、JPEG、PNG、BMP、PDF、TIFF の各ファイル形式をサポートするイメージとドキュメントから、印刷されたテキストおよび手書きのテキストを抽出できます。 詳細については、Read API のドキュメントに関する記事を参照してください。	一般提供。 このコンテナーは、切断された環境でも実行できます。

サービス	コンテナー	説明	可用性
空間分析	**空間分析** (イメージ)	リアルタイム ストリーミング ビデオを分析して、ユーザーとその動きの間の空間関係、および物理的な環境内のオブジェクトの相互作用を把握します。	プレビュー

さらに、一部のコンテナーは、Azure AI サービスの マルチサービス リソース オファリング内でサポートされています。 単一の Azure AI サービスの オールインワン リソースを作成し、次のサービスに対してサポートされているサービス全体で同じ課金キーを使用できます。

- Azure AI Vision
- LUIS
- 言語サービス

前提条件

Azure AI コンテナーを使用する前に、次の前提条件を満たす必要があります。

Docker エンジン: Docker エンジンをローカルにインストールしている必要があります。 Docker には、macOS、Linux、Windows 上で Docker 環境を構成するパッケージが用意されています。 Windows では、Linux コンテナーをサポートするように Docker を構成する必要があります。 Docker コンテナーは、Azure Kubernetes Service または Azure Container Instances に直接デプロイできます。

コンテナーが Azure に接続して課金データを送信できるように、Docker を構成する必要があります。

Microsoft Container Registry と Docker に関する知識: レジストリ、リポジトリ、コンテナー、コンテナー イメージなどの Microsoft Container Registry と Docker の両方の概念の基本的な理解に加えて、基本的な `docker` コマンドの知識が必要です。

Docker やコンテナーの基礎に関する入門情報については、「Docker overview」(Docker の概要) を参照してください。

個々のコンテナーには、サーバーやメモリ割り当ての要件など、独自の要件もある場合があります。

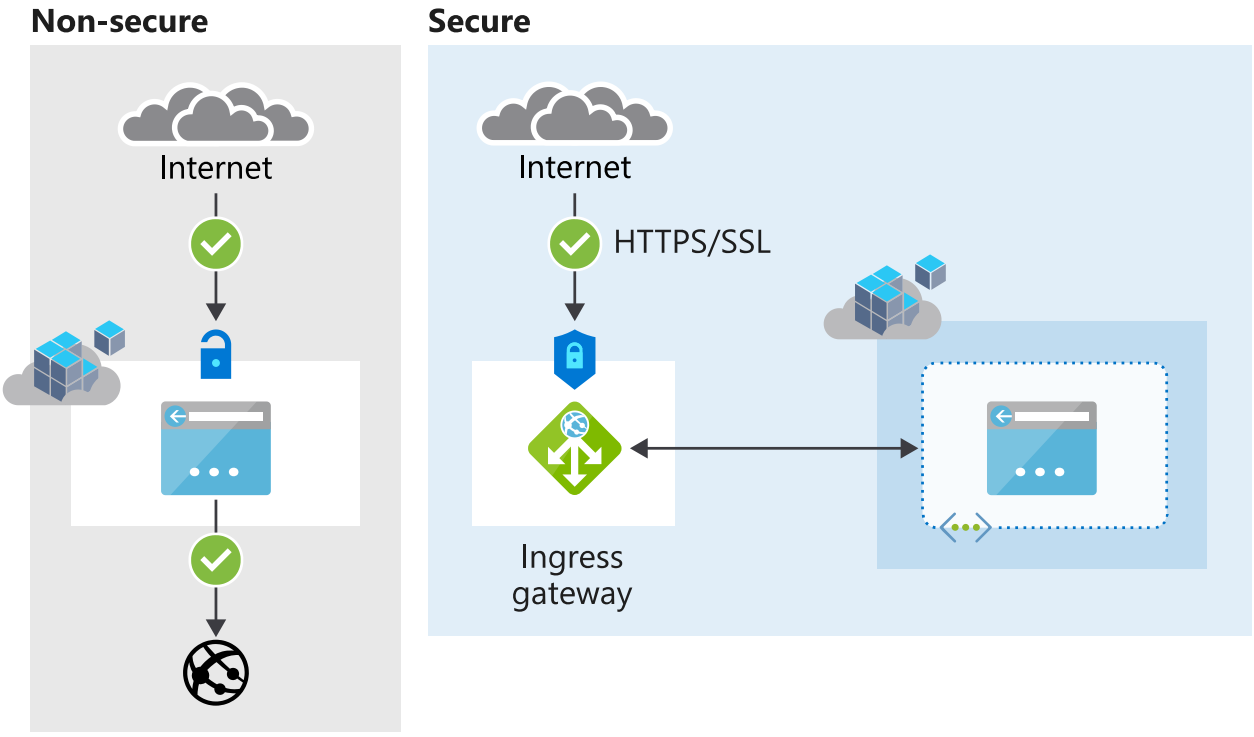
Azure AI サービス コンテナーのセキュリティ

アプリケーションを開発するときは常にセキュリティを重視する必要があります。 セキュリティの重要性は成功の指標です。 Azure AI コンテナーを含むソフトウェア ソリ

ューションを設計する場合は、制限と使用できる機能を理解しておくことが重要です。 ネットワーク セキュリティの詳細については、「Azure AI サービスの仮想ネットワークを構成する」を参照してください。

> **ⓘ 重要**
>
> 既定では、Azure AI サービス コンテナー API に "セキュリティはありません"。 この理由は、ほとんどの場合、ネットワーク ブリッジによって外部から保護されるポッドの一部としてコンテナーが実行されるためです。 ただし、ユーザーは、**クラウドベースの Azure AI サービス**にアクセスするときに使用される認証方法に近似している独自の認証インフラストラクチャを構築できます。

次の図は、**セキュリティで保護されていない**既定のアプローチを示しています。



別の "セキュリティで保護された" アプローチの例として、Azure AI コンテナーのコンシューマーでは、コンテナー エンドポイントを非公開に保ちながら、前面のコンポーネントを使用してコンテナーを補強できます。 イングレス ゲートウェイとして Istio を使用するシナリオについて考えてみましょう。 Istio では、HTTPS/TLS およびクライアント証明書の認証がサポートされます。 このシナリオでは、Istio のフロントエンドでコンテナー アクセスが公開され、事前に Istio で承認されているクライアント証明書が提示されています。

Nginx は、同じカテゴリにあるもう 1 つの一般的な選択肢です。 Istio と Nginx はどちらもサービス メッシュとして機能し、負荷分散、ルーティング、レート制御などの追加機能が提供されます。

コンテナー ネットワーク

Azure AI コンテナーは、課金のために使用状況測定情報を送信する必要があります。 Azure AI コンテナーが依存しているさまざまなネットワーク チャネルを許可リストに載せないと、コンテナーは動作しなくなります。

Azure AI サービスのドメインとポートを許可リストに載せる

ポート 443 と次のドメインをホストの許可リストに載せる必要があります。

- `*.cognitive.microsoft.com`
- `*.cognitiveservices.azure.com`

ディープ パケット インスペクションを無効にする

ディープ パケット インスペクション (DPI) は、コンピューター ネットワーク経由で送信されるデータを詳細に検査するデータ処理の一種であり、通常は、状況に応じてブロック、再ルーティング、またはログ記録を行うことによってアクションを実行します。

Azure AI コンテナーによって Microsoft サーバーに作成される、セキュリティで保護されたチャネルでは DPI を無効にします。 そうしないと、コンテナーは正しく機能しません。

開発者向けサンプル

開発者向けサンプルは、GitHub リポジトリから入手できます。

次のステップ

Azure AI サービスで使用できるコンテナー レシピについて学習します。

Azure AI サービスのコンテナーによって提供される機能をインストールして確認します。

- Anomaly Detector コンテナー
- Azure AI Vision コンテナー
- Language Understanding (LUIS) コンテナー
- Speech Service API コンテナー
- 言語サービス コンテナー
- Translator コンテナー

- [概要作成コンテナー][su-containers]

Azure AI コンテナーに関するよくあるご質問

よく寄せられる質問

一般的な質問

何を利用できますか。

Azure AI コンテナーを使用すると、開発者は Azure で利用できるものと同じインテリジェントな API を使用できますが、それに加えてコンテナ化のベネフィットも得られます。 一部のコンテナーは制限プレビューとして提供され、利用するには申請が必要になる場合があります。 他のコンテナーは、ゲートなしプレビューとして公開されているか、一般提供されています。 コンテナーとその可用性の完全な一覧については、Azure AI サービスでのコンテナーのサポートに関する記事を参照してください。 Microsoft Container Registry (MCR) でコンテナーを表示することもできます。

Azure AI サービス クラウドとコンテナーには違いがありますか?

Azure AI コンテナーは Azure AI サービス クラウドの代替物です。 コンテナーからは、それに対応するクラウド サービスと同じ機能が提供されます。 お客様はオンプレミスまたは Azure でコンテナーをデプロイできます。 中心となる AI テクノロジ、価格レベル、API キー、API 署名は、コンテナーとそれに対応するクラウドサービスの間で同じです。 それに対応するクラウド サービスではなく、コンテナーを選択すると、次のような機能と利点が与えられます。

限定的なプレビュー コンテナーにアクセスして使用するにはどうすればよいですか?

これまで、限定的なプレビュー コンテナーは `containerpreview.azurecr.io` リポジトリでホストされていました。 2020 年 9 月 22 日現在、これらのコンテナーは Microsoft Container Registry でホストされています。 それらをダウンロードするために、`docker login` コマンドを使用する必要はありません。 承認済みの Azure サブスクリプション ID を使用して Azure リソースが作成されている場合は、限定的なプレビュー コンテナーを実行できます。 要求フォームへの入力が完了しても、Azure サブスクリプションが承認されていない場合は、コンテナーを実行することはできません。

コンテナーはすべての Azure AI サービス オファリングで利用できますか? また、次に期待できるコンテナー セットは何ですか?

Microsoft では、より多くの Azure AI サービス オファリングをコンテナーとして利用できるようにしたいと考えています。 新しいコンテナーのリリースに関する最新情報や Azure AI サービス関連のその他のお知らせについては、お住まいの地域の Microsoft アカウント マネージャーにお問い合わせください。

Azure AI コンテナーのサービス レベル アグリーメント (SLA) は何ですか?

> ⓘ **重要**
>
> Azure AI サービスのサービスレベル アグリーメントの詳細については、**Microsoft の SLA のページ** を参照してください。

Azure AI には、クラウドでホストされるサービスに関する SLA が用意されており、SLA のページで確認することができます。

ただし、コンテナー内の Azure AI サービスはオンプレミス ソフトウェアであるため、SLA は提供されません。 Azure AI サービス コンテナーのリソース構成はお客様が管理します。そのため、Microsoft では一般提供 (GA) のための SLA を提供することはできません。 お客様がオンプレミスでコンテナーを自由にデプロイし、ホスト環境を定義します。

これらのコンテナーはソブリン クラウドで利用できますか。

標準の Azure AI コンテナーは、ソブリン クラウドで使用できます。 コンテナーは認可されると、これらのクラウド内で実行でき、課金エンドポイントに接続できますが、コンテナー イメージはパブリック クラウド コンテナー レジストリからプルする必要があります。 Translator やカスタム音声テキスト変換など、実行時にダウンロードされた言語モデルに依存するコンテナーも、パブリック エンドポイントからモデルをプルするように構成されます。

現在、ソブリン クラウドでは、切断されたコンテナーの購入はサポートされていません。 切断されたコンテナーとすべての依存関係をパブリック クラウドで購入し、ソブ

リン クラウドに転送して、ソブリン クラウド インフラストラクチャで実行することができます。

バージョン管理

コンテナーはどのような方法で最新バージョンに更新されますか。

お客様は、自分がデプロイしたコンテナーを更新するタイミングを選択できます。 最新のバージョンを示すために、コンテナーには `latest` のような標準 Docker タグ のマークが付けられます。 最新バージョンのコンテナーがリリースされたら、それらをプルすることをお勧めします。 イメージが更新されたときに通知を受け取る方法について詳しくは、Azure Container Registry Webhook に関するページを参照してください。

コンテナー ライセンス ファイルは、各コンテナー イメージ内の特定のファイルを復号化するためのキーとして使用されます。 これらの暗号化されたファイルが新しいコンテナー イメージ内で誤って更新された場合、お使いのライセンス ファイルは、コンテナー イメージの以前のバージョンでは動作していた場合でも、コンテナーの起動に失敗する可能性があります。 この問題を回避するには、mcr.microsoft.com から新しいイメージ バージョンをプルした後、Azure portal で提供されるコンテナーのリソース エンドポイントから新しいライセンス ファイルをダウンロードすることをお勧めします。

新しいライセンス ファイルをダウンロードするには、ライセンス マウント、API キー、課金エンドポイントと共に docker run コマンドに `DownloadLicense=True` を追加します。 詳しい手順については、コンテナーのドキュメントをご覧ください。

どのバージョンがサポートされていますか?

通常、コンテナーの現在のバージョンのみがサポートされます。 お客様には、常に最新のパッチとテクノロジを入手することをお勧めしています。

更新プログラムはどのようにバージョン管理されますか?

メジャー バージョンの変更は、API 署名に破壊的変更があることを示します。 通常、この指示は、対応する Azure AI サービス クラウド オファリングのメジャー バージョン変更と一致すると予想されます。 マイナー バージョンの変更は、バグ修正、モデル更新、または API 署名に破壊的変更を加えない新機能を示します。

技術的なご質問

デプロイ環境で発生する可能性のあるエラーはどのようにして診断できますか?

Azure AI サービス コンテナーの実行で問題が発生している場合は、Microsoft 診断コンテナーを使用してみることができます。 このコンテナーを使用して、Azure AI コンテナーが想定どおりに機能しなくなる可能性がある、展開環境での一般的なエラーを診断します。

コンテナーを取得するには、次の `docker pull` コマンドを使用します。

Bash

```
docker pull mcr.microsoft.com/azure-cognitive-services/diagnostic
```

その後で、コンテナーを実行します。 `{ENDPOINT_URI}` をエンドポイントに置き換え、`{API_KEY}` をリソースへのキーに置き換えます。

Bash

```
docker run --rm mcr.microsoft.com/azure-cognitive-services/diagnostic \
eula=accept \
Billing={ENDPOINT_URI} \
ApiKey={API_KEY}
```

コンテナーは、課金エンドポイントへのネットワーク接続をテストします。

Azure AI コンテナーを IoT デバイスで実行するにはどうすればいいですか?

信頼性の高いインターネット接続が利用できない場合、帯域幅コストを節約したい場合、低遅延の要件がある場合、オンサイトで分析する必要がある機密データを扱っている場合のいずれであっても、Azure IoT Edge と Azure AI コンテナー を使用することでクラウドとの一貫性を確保できます。

これらのコンテナーは OpenShift と互換性がありますか?

OpenShift ではコンテナーをテストしませんが、通常、Azure AI コンテナーは Docker イメージをサポートする任意のプラットフォームで実行する必要があります。 OpenShift を使用している場合は、`root-user` としてコンテナーを実行することをお勧めします。

製品フィードバックや機能推奨はどのような方法で提供しますか?

お客様には公の場で懸念を表明することと、同じ問題を投稿した他のユーザーに賛成票を投じることをお勧めしています。 フィードバック ツールは、製品フィードバックと機能推奨の両方にご利用いただけます。

Azure AI コンテナーから返されるステータス メッセージとエラーとは？

ステータス メッセージとエラーを次に示します。

テーブルを展開する

Status	説明
`Valid`	API キーは有効です。 対処は必要ありません。
`Invalid`	API キーが無効です。 コンテナーを実行するには、有効な API キーを指定する必要があります。 Azure portal の Azure AI サービス リソースの **[Keys and Endpoint](キーとエンドポイント)** セクションで、API キーとサービス リージョンを確認してください。
`Mismatch`	別の種類の Azure AI サービス リソースの API キーまたはエンドポイントが指定されました。 Azure portal の Azure AI サービス リソースの **[Keys and Endpoint](キーとエンドポイント)** セクションで、API キーとサービス リージョンを確認してください。
`CouldNotConnect`	コンテナーは課金エンドポイントに接続できませんでした。 `Retry-After` 値を確認し、この期

Status	説明
	間が終了するまで待ってから、追加の要求を行ってください。
`OutOfQuota`	API キーがクォータを超えました。 価格レベルをアップグレードすることも、追加のクォータが使用可能になるまで待つこともできます。 Azure portal の Azure AI サービス リソースの **[価格レベル]** セクションで、お使いのレベルを見つけます。
`BillingEndpointBusy`	課金エンドポイントが現在ビジー状態です。 `Retry-After` 値を確認し、この期間が終了するまで待ってから、追加の要求を行ってください。
`ContainerUseUnauthorized`	指定された API キーは、このコンテナーでの使用が承認されていません。 限定的なコンテナーを使用している可能性があるため、オンライン リクエスト を送信して、Azure サブスクリプション ID が承認されていることを確認してください。
`[ERROR] Failed to download: context deadline exceeded`	サーバーへのモデル ファイルのダウンロード要求がタイムアウトしました。必要なすべてのファイルを 1 時間以内にダウンロードできる強力なインターネット接続があることを確認してください。 モデルのダウンロードは、テキスト翻訳と一部の音声サービス コンテナーに適用されます。
`The provided license path was not found. Please ensure a volume is mounted and a directory exists at the location specified by Mounts:License`	**切断されたコンテナーのみ。** docker run コマンドで指定された場所に、ローカルに保存されているライセンス ファイルがありません。 ライセンス ボリュームを誤ってマウントしている可能性があります。 docker run コマンドで -v 引数を使用して、ローカル ファイル システムをチェックし、目的のライセンス ファイルのローカルの保存場所への有効なファイルパスを指定するようにしてください。
`Unknown`	現在、サーバーは課金要求を処理することができません。

サポートを利用するにはどうすればよいですか?

カスタマー サポート チャネルは、Azure AI サービスのクラウドベースの API の場合と同じです。 すべての Azure AI コンテナーには、Microsoft やコミュニティがお客様をサポートする際に役立つログ機能が含まれています。 その他のサポートのオプションを次に示します。

- 該当する Azure サポート プラン から連絡先情報を見つけます。
- プログラミングのプロフェッショナルや愛好家のための質疑応答サイト、スタック オーバーフロー で、次の領域に関する問題の解決を試みます。
  - Azure AI サービス
  - Microsoft Cognitive

請求のしくみを教えてください。

Azure AI サービス クラウドと同様に、お客様には、使用量に基づいて料金が請求されます。 コンテナーは、Azure に測定データを送信するように構成する必要があります。構成後、トランザクションに対して適宜課金されます。 ホステッド サービスとオンプレミス サービスの間で使用されるリソースは、価格が階層化された単一クォータに追加されます。集計は両方の使用量に対して行われます。 詳細については、使用しているコンテナーの課金に関するセクションを参照してください。

> **ⓘ 重要**
>
> Azure AI コンテナーには、Azure に接続せずに計測を実行するための "ライセンスが与えられていません"。 お客様は、課金情報をコンテナーから測定サービスに常に送信できるようにする必要があります。 Azure AI コンテナーが顧客データを Microsoft に送信することはありません。

コンテナーが計測のために伝える情報の例を次に示します。

JSON

```
usageRequestBody": {
  "id": "1234abcd-1234-56ab-ab12-1234abcd",
  "containerType": "<container-type>",
  "containerVersion": "<container-version>",
  "containerId": "<contianer-id>",
  "meter": {
    "name": "<meter-name>",
    "quantity": 0.0
  },
  "requestTime": 12345687890,
```

```
    "apiType": "<api-type>"
  },
```

コンテナーの現在のサポート保証はどのようになっていますか?

Microsoft のエンタープライズ ソフトウェアに対する標準保証は、一般提供 (GA) として正式に発表されたすべてのコンテナーに適用されます。 プレビューには保証はありません。

インターネット接続が失われると、Azure AI コンテナーはどうなりますか?

Azure AI コンテナーには、Azure に接続せずに計測を実行するための "ライセンスが与えられていません"。 お客様は、コンテナーと測定サービスが常に通信できるようにする必要があります。

Azure に接続されていない状態でどのくらいの時間、コンテナーを運用できますか?

Azure AI コンテナーには、Azure に接続せずに計測を実行するための "ライセンスが与えられていません"。 お客様は、コンテナーと測定サービスが常に通信できるようにする必要があります。

これらのコンテナーを実行するために必要なハードウェアは何ですか?

Azure AI コンテナーは、x64 Linux Docker コンテナーをサポートする互換性のある Linux ノード、VM、エッジ デバイスを実行できる x64 ベースのコンテナーです。 それらすべてで CPU プロセッサを必要とします。 詳細については、使用しているコンテナーのコンテナーの要件と推奨事項に関するセクションを参照してください。

これらのコンテナーは Windows で現在サポートされていますか?

Azure AI コンテナーは Linux コンテナーですが、Windows では Linux コンテナーがサポートされています。 Windows で Linux コンテナーを実行する方法については、Docker ドキュメントを参照してください。

Azure AI コンテナーは、AWS や Google のオファリングと比べてどうですか?

Microsoft は、事前にトレーニングした AI モデルをコンテナーに導入した最初のクラウド プロバイダーです。トランザクション単位の簡単な請求機能を採用し、まるで 1 つのクラウド サービスを利用しているような印象をお客様に与えます。 Microsoft は、ハイブリッド クラウドはお客様に与える選択肢を増やすものと考えています。

コンテナーにはどのようなコンプライアンス認定がありますか?

Azure AI コンテナーにはコンプライアンス認定がありません。

Azure AI コンテナーはどのリージョンで利用できますか?

コンテナーはあらゆるリージョンのあらゆる場所で実行できますが、キーを必要とし、また、測定のために Azure にコールバックする必要があります。 クラウド サービスでサポートされているリージョンはすべて、コンテナーの測定呼び出しでサポートされています。

- 切断された環境で Azure AI コンテナーを使用する方法

切断された環境での Docker コンテナーの使用

[アーティクル] • 2023/07/28

コンテナーを使用すると、独自の環境で Azure AI サービス API を実行でき、特定のセキュリティとデータ ガバナンスの要件に最適です。 切断されたコンテナーを使用すると、これらの API のいくつかをインターネットから切断して使用できます。 現時点では、次のコンテナーをこの方法で実行できます。

- 音声テキスト変換
- カスタム音声テキスト変換
- ニューラル テキスト読み上げ
- テキスト翻訳 (標準)
- Azure AI 言語
  - 感情分析
  - キー フレーズ抽出
  - 言語検出
- Azure AI Vision - 読み取り
- Document Intelligence

オフライン環境で Docker コンテナーの実行を試みる前に、コンテナーを正常にダウンロードして使用するための手順がわかっていることを確認してください。 次に例を示します。

- ホスト コンピューターの要件と推奨事項。
- コンテナーをダウンロードするために使用する Docker `pull` コマンド。
- コンテナーが実行されていることを検証する方法。
- 実行後に、コンテナーのエンドポイントにクエリを送信する方法。

切断された環境でコンテナーを使用するためのアクセスを要求する

インターネットから切断されたコンテナーへのアクセスを要求するには、要求フォームに記入して送信します。

このフォームでは、ユーザー、会社、コンテナーを使用するユーザー シナリオに関する情報が要求されます。 フォームを送信すると、Azure AI サービス チームがフォームをレビューし、10 営業日以内に決定を電子メールで送信します。

> ⓘ **重要**
>
> - このフォームでは、Azure サブスクリプション ID に関連付けられているメール アドレスを使用する必要があります。
> - コンテナーの実行に使用する Azure リソースは、承認された Azure サブスクリプション ID で作成されている必要があります。
> - Microsoft からのアプリケーションの状態に関する更新については、電子メール (受信トレイと迷惑フォルダーの両方) を確認してください。

承認されると、Microsoft Container Registry (MCR) からコンテナーをダウンロードしてから、そのコンテナーを実行できるようになります。これについては、記事の後半で説明します。

お使いの Azure サブスクリプションが承認されていない場合は、コンテナーを実行することができません。

アクセスできるのは、次の要件を満たすお客様に限定されます。

- 組織が、Microsoft の戦略的な顧客またはパートナーとして認定されている必要があります。
- 切断されたコンテナーは完全にオフラインで実行されることになるため、ユースケースは以下または同様の要件のいずれかを満たしている必要があります。
  - インターネットへの接続性がまったくない環境またはデバイス。
  - インターネットに断続的にアクセスできるリモートの場所。
  - どのような種類のデータもクラウドに返送しないという厳格な規制の下にある組織。
- 指示に従って申請を完了してください - 承認に必要なすべての情報を確実に提供するために、申請全体を通じて提供されるガイダンスに細心の注意を払ってください。

切断された環境でコンテナーを使用するためのコミットメント プランを購入する

新しいリソースを作成

1. Azure portal にサインインし、上記の該当する Azure AI サービスまたは Azure AI サービスの 1 つに対して [**新しいリソースの作成**] を選択します。

2. リソースを作成するための該当する情報を入力します。 価格レベルとして **[コミットメント レベルの切断済みコンテナー]** を選択してください。

   > ⓘ **注意**
   >
   > - お客様が Microsoft によって承認されている場合にのみ、コミットメント レベルを購入するオプションが表示されます。
   > - 価格の詳細は、単に例を示しているだけです。

3. ページの下部にある **[確認および作成]** を選択します。 情報を確認し、**[作成]** を選択します。

切断状態での使用のためにコンテナーを構成する

切断された使用のためにコンテナーをダウンロードして構成する手順については、次のドキュメントを参照してください。

- ビジョン - 読み取り
- Language Understanding (LUIS)
- テキスト翻訳 (標準)
- Document Intelligence

Speech サービス

- 音声テキスト変換
- カスタム音声テキスト変換
- ニューラル テキスト読み上げ

言語サービス

- 感情分析
- キー フレーズ抽出
- 言語検出

Kubernetes デプロイの環境変数名

一部の Azure AI コンテナー (Translator など) では、コンテナーの実行時にコロン (`:`) を含む環境変数名を渡す必要があります。 これは Docker を使用する場合は正常に機能しますが、Kubernetes では環境変数名にコロンを使用できません。 これを解決するには、Kubernetes にデプロイするときに、コロンを 2 つのアンダースコア文字 (`__`) に置き換えることができます。 環境変数名に使用できる形式の例を次に示します。

Kubernetes

```
        env:
        - name: Mounts__License
          value: "/license"
        - name: Mounts__Output
          value: "/output"
```

次の使用例は、docker run コマンドの 環境変数と `Mounts:Output` 環境変数の既定の形式`Mounts:License`を置き換えます。

コンテナー イメージとライセンスの更新

コンテナー ライセンス ファイルは、各コンテナー イメージ内の特定のファイルを復号化するためのキーとして使用されます。 これらの暗号化されたファイルが新しいコンテナー イメージ内で誤って更新された場合、お使いのライセンス ファイルは、コンテナー イメージの以前のバージョンでは動作していた場合でも、コンテナーの起動に失敗する可能性があります。 この問題を回避するには、mcr.microsoft.com から新しいイメージ バージョンをプルした後、Azure portal で提供されるコンテナーのリソース エンドポイントから新しいライセンス ファイルをダウンロードすることをお勧めします。

新しいライセンス ファイルをダウンロードするには、ライセンス マウント、API キー、課金エンドポイントと共に docker run コマンドに `DownloadLicense=True` を追加します。 詳しい手順については、コンテナーのドキュメントを参照してください。

使用状況レコード

切断された環境で Docker コンテナーを運用する場合、コンテナーは、使用状況レコードをボリュームに書き込んで、時間をかけて収集されるようにします。 REST エンドポイントを呼び出して、サービス使用状況に関するレポートを生成することもできます。

ログを格納するための引数

切断された環境で実行する場合は、使用状況ログを格納するために、コンテナーで出力マウントを利用できる必要があります。 たとえば、下の例では `-v /host/output:{OUTPUT_PATH}` と `Mounts:Output={OUTPUT_PATH}` を含め、`{OUTPUT_PATH}` をログが格納されるパスに置き換えます。

Docker

```
docker run -v /host/output:{OUTPUT_PATH} ... <image> ... Mounts:Output=
{OUTPUT_PATH}
```

コンテナー エンドポイントを使用してレコードを取得する

コンテナーには、その使用状況に関するレコードを返すための 2 つのエンドポイントが用意されています。

すべてのレコードを取得する

次のエンドポイントは、マウントされた課金レコード ディレクトリに収集されたすべての使用状況を要約するレポートを提供します。

HTTP

```
https://<service>/records/usage-logs/
```

下の例のような JSON が返されます。

JSON

```
{
  "apiType": "noop",
  "serviceName": "noop",
  "meters": [
    {
      "name": "Sample.Meter",
      "quantity": 253
    }
  ]
}
```

特定の月のレコードを取得する

次のエンドポイントは、特定の月と年の使用状況を要約するレポートを提供します。

HTTP

```
https://<service>/records/usage-logs/{MONTH}/{YEAR}
```

下の例のような JSON 応答が返されます。

JSON

```
{
  "apiType": "string",
  "serviceName": "string",
  "meters": [
    {
      "name": "string",
      "quantity": 253
    }
  ]
}
```

切断されたコンテナーのために別のコミットメント プランを購入する

切断されたコンテナーのコミットメント プランには、暦年のコミットメント期間があります。 プランを購入すると、すぐに価格の全額が課金されます。 コミットメント期間中にコミットメント プランを変更することはできませんが、年間の残りの日数については、日割り計算の価格で追加のユニットを購入できます。 コミットメントの最終日の午前 0 時 (UTC) までコミットメント プランを終了することができます。

リソースの [Commitment Tier pricing] (**コミットメント レベルの価格**) 設定で別のコミットメント プランを選択できます。

コミットメント プランを終了する

コミットメント プランの購入を継続しない場合、リソースの自動更新を [**自動更新しない**] に設定することができます。 コミットメント プランは、表示されたコミットメントの終了日に期限切れになります。 この日以降、コミットメント プランの料金は課金されません。 引き続き Azure リソースを使用して API を呼び出すことができ、従量課金制の料金で課金されます。 切断されたコンテナーについて、年の最終日の午前 0 時 (UTC) までコミットメント プランを終了することができ、その場合、翌年は課金されません。

トラブルシューティング

出力マウントとログを有効にした状態でコンテナーを実行すると、コンテナーによってログ ファイルが生成されます。これらはコンテナーの起動時または実行時に発生した問題のトラブルシューティングに役立ちます。

ヒント

トラブルシューティング情報とガイダンスの詳細については、「**切断されたコンテナーについてよくあるご質問 (FAQ)**」を参照してください。

次の手順

Azure AI サービス コンテナーの概要

Azure AI サービスの切断されたコンテナーに関する FAQ

よく寄せられる質問

一般的な質問

切断されたコンテナーとして使用できるサービスは何ですか?

Azure AI コンテナーを使用すると、開発者は Azure で利用できるものと同じインテリジェントな API を使用できますが、それに加えてコンテナ化のベネフィットも得られます。 切断されたコンテナーはコミットメント レベル価格を通じて提供されており、それぞれ従量課金制の価格モデルと比べて割引料金が提供されています。 コミットメント レベル価格では、次の Azure AI サービス機能を固定料金で使用できるようになり、これによってワークロードのニーズに基づく合計コストが予測可能になります。

- Azure AI 音声
  - 音声テキスト変換
  - カスタム音声テキスト変換
  - ニューラル テキスト読み上げ
- テキスト翻訳 (標準)
- Azure AI 言語
  - 感情分析
  - キー フレーズ抽出
  - 言語検出
  - 名前付きエンティティの認識 (NER)
- Azure AI Vision - 読み取り
- Document Intelligence

コミットメント レベル価格の詳細については、Microsoft アカウント チームに連絡するか、Microsoft にお問い合わせください。 azureaicontainergating@service.microsoft.com にメールを送信することもできます。

コンテナーは他の Azure AI サービス オファリングで利用できますか? また、次に期待できるコンテナー セットは何ですか?

Microsoft では、より多くの Azure AI サービス オファリングをコンテナーとして利用できるようにしたいと考えています。 新しいコンテナーのリリースに関する最新情報や Azure AI サービス関連のその他の告知については、お住まいの地域の Microsoft アカウント マネージャーにお問い合わせください。

切断されたコンテナーにアクセスするにはどうすればよいですか?

コンテナーへのアクセスを要求するには、要求フォーム に記入して送信します。 アクセスできるのは、次の要件を満たすお客様に限定されます。

- Enterprise Agreement または同等の契約を組織が結んでいる必要があります。また、Microsoft の戦略的な顧客またはパートナーとして認定されている必要があります。
- 有効なビジネス シナリオ/ユース ケース - 切断されたコンテナーは完全にオフラインで実行されることになるため、ユース ケースは以下または同様の要件のいずれかを満たしている必要があります。
  - インターネットへの接続性がまったくない環境またはデバイス。
  - インターネットに断続的にアクセスできるリモートの場所。
  - どのような種類のデータもクラウドに返送しないという厳格な規制の下にある組織。
- 指示に従って申請を完了してください - 承認に必要なすべての情報を確実に提供するために、申請全体を通じて提供されるガイダンスに細心の注意を払ってください。

ユース ケースが上記の要件を満たすことができない場合はどうすればよいですか?

ユース ケースが上記の要件を満たしていないが、オンプレミスでコンテナーを実行することに関心がある場合は、接続されたコンテナー を使用できる可能性があります。

アプリケーションが拒否される理由は何ですか?

申請が拒否される理由として考えられる原因は次のとおりです。

- 既存の Micosoft パートナーまたは Enterprise Agreement の顧客ではない
- Azure サブスクリプション ID が無効である。ID は申請者組織に属している必要があります。また、他の組織の代理で申請することはできません。
- 申請が個人のメール アドレス (@hotmail.com、@gmail.com、@yahoo.com など) を使って送信された

- 無効な理由またはビジネス シナリオが提示された
- その他のデータが欠落しているか、不正確である

申請が承認されて、切断されたコンテナーにアクセスできるまでにはどのくらいの時間が必要ですか?

フォームを送信すると、Azure AI サービス チームがこれを確認し、10 営業日以内に決定事項をメールで伝えます。

申請が承認されると、Azure AI サービス ゲーティング チームから、コミットメント レベル価格で購入するための詳細と、コンテナーをダウンロードして実行する手順について連絡します。

申請、制限プロセス、または必要なその他の情報について質問がある場合は、azureaicontainergating@service.microsoft.com にメールを送信してください。

切断されたコンテナーをダウンロードするにはどうすればよいですか?

これらのコンテナーは Microsoft Container Registry でホストされており、Microsoft アーティファクト レジストリ と Microsoft コンテナー レジストリ (MCR) でダウンロードできます。 要求フォームへの入力後も、Azure サブスクリプションが承認されていない場合は、コンテナーを実行することはできません。 承認されたら、「切断された環境での Docker コンテナーの使用」の手順に従ってください。

Azure AI コンテナーのサービス レベル アグリーメント (SLA) は何ですか?

使用されるリソースの構成はお客様が制御するため、Azure AI サービスの切断されたコンテナーには SLA が適用されません。 お客様がオンプレミスでコンテナーを自由にデプロイし、ホスト環境を定義します。

これらのコンテナーはソブリン クラウドで利用できますか。

ソブリン クラウドという用語になじみのない人もいるので、その定義から始めましょう。ソブリン クラウドは Azure Government、Azure Germany、21Vianet によって運営

される Microsoft Azure の各クラウドから成ります。 現在、お客様は、切断されたコンテナー リソースをパブリック クラウドから作成できます。

バージョン管理

コンテナーはどのような方法で最新バージョンに更新されますか。

お客様は、自分がデプロイしたコンテナーを更新するタイミングを選択できます。 最新のバージョンを示すために、コンテナーには latest のような標準 Docker タグのマークが付けられます。 最新バージョンのコンテナーがリリースされたら、それらをプルすることをお勧めします。 イメージが更新されたときに通知を受け取る方法について詳しくは、Azure Container Registry Webhook に関するページを参照してください。

サポートされるバージョンは何ですか。

コンテナーの現行の最新メジャー バージョンがサポートされます。 ただし、お客様には、準拠状態を維持するために、常に最新のテクノロジを入手することをお勧めしています。

更新プログラムはどのようにバージョン管理されますか?

メジャー バージョンの変更は、API 署名に破壊的変更があることを示します。 これは通常、それに対応する Azure AI サービス クラウド オファリングのメジャー バージョンの変更に一致するものと、Microsoft では予測しています。 マイナー バージョンの変更は、バグ修正、モデル更新、または API 署名に破壊的変更を加えない新機能を示します。

技術的なご質問

デプロイ環境で発生する可能性のあるエラーはどのようにして診断できますか?

Azure AI サービス コンテナーの実行で問題が発生している場合は、Microsoft 診断コンテナーを使用してみることができます。 このコンテナーを使用して、Azure AI コンテナーが想定どおりに機能しなくなる可能性がある、展開環境での一般的なエラーを診断します。

コンテナーを取得するには、次の `docker pull` コマンドを使用します。

Bash

```
docker pull mcr.microsoft.com/azure-cognitive-services/diagnostic
```

その後で、コンテナーを実行します。 `{ENDPOINT_URI}` をエンドポイントに置き換え、`{API_KEY}` をリソースへのキーに置き換えます。

Bash

```
docker run --rm mcr.microsoft.com/azure-cognitive-services/diagnostic \
eula=accept \
Billing={ENDPOINT_URI} \
ApiKey={API_KEY}
```

コンテナーは、課金エンドポイントへのネットワーク接続をテストします。

これらのコンテナーは OpenShift と互換性がありますか?

OpenShift ではコンテナーをテストしませんが、通常、Azure AI コンテナーは Docker イメージをサポートする任意のプラットフォームで実行する必要があります。
OpenShift を使用している場合は、ルート ユーザーとしてコンテナーを実行することをお勧めします。

製品フィードバックや機能推奨はどのような方法で提供しますか?

お客様には公の場で懸念を表明する ことと、同じ問題を投稿した他のユーザーに賛成票を投じることをお勧めしています。 フィードバック ツールは、製品フィードバックと機能推奨の両方にご利用いただけます。

Azure AI コンテナーから返されるステータス メッセージとエラーとは?

ステータス メッセージとエラーを次に示します。

テーブルを展開する

Status	説明
`Valid`	API キーは有効です。 対処は必要ありません。
`Invalid`	API キーが無効です。 切断された環境で使用するコンテナーを構成するには、有効な API キーを指定する必要があります。 Azure portal の Azure AI サービス リソースの **[Keys and Endpoint]**(**キーとエンドポイント**) セクションで、API キーとサービス リージョンを確認してください。
`Mismatch`	別の種類の Azure AI サービス リソースの API キーまたはエンドポイントが指定されました。 Azure portal の Azure AI サービス リソースの **[Keys and Endpoint]**(**キーとエンドポイント**) セクションで、API キーとサービス リージョンを確認してください。
`CouldNotConnect`	コンテナーはエンドポイントに接続できませんでした。
`OutOfQuota`	API キーがクォータを超えました。 価格レベルをアップグレードすることも、追加のクォータが使用可能になるまで待つこともできます。 Azure portal の Azure AI サービス リソースの **[価格レベル]** セクションで、お使いのレベルを見つけます。
`ContainerUseUnauthorized`	指定された API キーは、このコンテナーでの使用が承認されていません。 限定的なコンテナーを使用している可能性があるため、オンライン リクエストを送信して、Azure サブスクリプション ID が承認されていることを確認してください。
`Unknown`	現在、サーバーは要求を処理できません。

サポートを利用するにはどうすればよいですか?

カスタマー サポート チャネルは、Azure AI サービスのクラウドベースの API の場合と同じです。 すべての Azure AI コンテナーには、Microsoft とコミュニティサポートのお客様に役立つログフィーチャーが含まれています。 その他のサポートのオプションを次に示します。

- 該当する Azure サポート プランから連絡先情報を見つけます。
- プログラミングのプロフェッショナルや愛好家のための質疑応答サイト、スタック オーバーフローで、次の領域に関する問題の解決を試みます。

- Azure AI サービス
- Microsoft Cognitive

請求のしくみを教えてください。

お客様は、購入したコミットメント レベルに基づいて課金されます。 ワークロードのニーズに基づいて年間コミットメント プランを選択します。 いくつかのコミットメント レベル オプションのいずれかを選択して、"コミットメント レベルの切断済みコンテナー DC0" 価格レベルをカスタマイズできます。

各コミットメント レベルでは、従量課金制の価格モデルと比べて割引料金が提供されています。 コミットメント プランは、リソースが作成された日を基点にして年単位で課金されます。 追加のユニットは、その年の任意の時点で追加でき、課金年の残りの日数に基づいて日割り計算で課金されます。 詳細については、次の価格のページを参照してください。

> **ヒント**
>
> 切断されたコンテナーの価格情報をこれらの価格のページで確認するには、**[コンテナー レベル]** セクションまで下にスクロールします。

- Speech Services:
  - 音声テキスト変換
  - カスタム音声テキスト変換
  - ニューラル テキスト読み上げ
- テキスト翻訳 (標準)
- Azure AI 言語の価格:
- 感情分析
- キー フレーズ抽出
- 言語検出
- Azure AI Vision - 読み取り
- Document Intelligence - カスタム/請求書

コンテナーの使用状況を監視するにはどうすればよいですか?

切断された環境で実行される場合、Docker コンテナーは、使用状況レコードをボリュームに書き込んで、時間をかけて収集されるようにします。 これらのコンテナーは、使用状況に関するレポートを生成する REST エンドポイントも提供します。 詳細については、「切断された環境でのコンテナーの使用」を参照してください。

コンテナーの現在のサポート保証はどのようになっていますか?

Microsoft のエンタープライズ ソフトウェアに対する標準保証は、コンテナー イメージが一般提供 (GA) として正式に発表されたときに適用されます。 プレビュー段階のコンテナー イメージに対する保証はありません。

これらのコンテナーを実行するために必要なハードウェアは何ですか?

Azure AI コンテナーは、x64 Linux Docker コンテナーをサポートする互換性のある Linux ノード、VM、エッジ デバイスを実行できる x64 ベースのコンテナーです。 それらすべてで CPU プロセッサを必要とします。 コンテナー オファリング別の最小構成と推奨構成は次のページに記載されています。

- 以下の音声サービス。
  - 音声テキスト変換
  - カスタム音声テキスト変換
  - ニューラル テキスト読み上げ
- テキスト翻訳 (標準)
- Azure AI Language のドキュメント:
- 感情分析
- キー フレーズ抽出
- 言語検出
- 名前付きエンティティの認識
- Azure AI Vision - 読み取り
- Document Intelligence - カスタム/請求書

これらのコンテナーは Windows で現在サポートされていますか?

Azure AI コンテナーは Linux コンテナーですが、Windows では Linux コンテナーがサポートされています。 Windows で Linux コンテナーを実行する方法については、Docker ドキュメントを参照してください。

コンテナーにはどのようなコンプライアンス認定がありますか?

Azure AI コンテナーにはコンプライアンス認定がありません。

再利用するためのコンテナーを作成する

[アーティクル] • 2024/02/22

これらのコンテナー レシピを使用して、再利用できる Azure AI コンテナーを作成します。 コンテナーの起動時に必要に "ならない" ように、一部またはすべての構成設定を使用してコンテナーをビルドすることができます。

(設定を使用して) この新しいレイヤーのコンテナーを用意し、それをローカルでテストした後は、コンテナー レジストリにコンテナーを保存できます。 コンテナーが起動するときは、コンテナーに現在保存されていないそれらの設定のみが必要になります。 プライベート レジストリ コンテナーには、それらの設定を渡すための構成領域が用意されています。

Docker の実行構文

このドキュメント内の `docker run` の例はすべて、 `^` 行継続文字を使用する Windows コンソールを想定しています。 ご自分で使用する場合は、次の点を考慮してください。

- Docker コンテナーについて高度な知識がある場合を除き、引数の順序は変更しないでください。
- Windows 以外のオペレーティング システム、または Windows コンソール以外のコンソールを使用している場合は、お使いのコンソールおよびシステムに適したコンソール/ターミナル、マウント用のフォルダー構文、および行継続文字を使用します。 Azure AI サービス コンテナーは Linux オペレーティング システムであるため、ターゲット マウントでは Linux スタイルのフォルダー構文を使用します。
- `docker run` の例では、Windows 上のアクセス許可の競合を防ぐために、 `c:` ドライブのディレクトリを使用しています。 特定のディレクトリを入力ディレクトリとして使用する必要がある場合は、Docker サービスのアクセス許可の付与が必要なことがあります。

イメージに構成設定を保存しない

各サービスの例の `docker run` コマンドでは、コンテナーに構成設定を保存しません。 コンソールまたはレジストリ サービスからコンテナーを起動するときに、これらの構成設定を渡す必要があります。 プライベート レジストリ コンテナーには、それらの設定を渡すための構成領域が用意されています。

レシピの再利用: すべての構成設定をコンテナーに保存する

すべての構成設定を保存するために、それらの設定を使用して `Dockerfile` を作成します。

このアプローチの問題点:

- 新しいコンテナーには、元のコンテナーとは別の名前とタグがあります。
- これらの設定を変更するには、Dockerfile の値を変更し、イメージをリビルドし、レジストリに再発行する必要があります。
- 誰かがコンテナー レジストリまたはローカル ホストのアクセス権を取得すると、コンテナーを実行し、Azure AI サービス エンドポイントを使用することができます。
- 使用している Azure AI サービスで入力マウントが必要ない場合は、Dockerfile に `COPY` 行を追加しないでください。

使用する既存の Azure AI サービス コンテナーからプルして Dockerfile を作成してから、Dockerfile で docker コマンドを使用して、コンテナーに必要な情報を設定または取得します。

この例では次のとおりです。

- `ENV` を使用して、課金エンドポイント (ホストの環境キーの `{BILLING_ENDPOINT}`) を設定します。
- ENV を使用して、課金 API キー (ホストの環境キーの `{ENDPOINT_KEY}`) を設定します。

レシピの再利用: 課金設定をコンテナーに保存する

この例では、Dockerfile から言語サービスのセンチメント コンテナーをビルドする方法を示します。

Dockerfile

```
FROM mcr.microsoft.com/azure-cognitive-services/sentiment:latest
ENV billing={BILLING_ENDPOINT}
ENV apikey={ENDPOINT_KEY}
ENV EULA=accept
```

必要に応じて、ローカルで、またはプライベート レジストリ コンテナーからコンテナーをビルドして実行します。

レシピの再利用: 課金とマウントの設定をコンテナーに保存する

この例では、Language Understanding を使用して、Dockerfile の課金およびモデルを保存する方法を示します。

- `COPY` を使用して、ホストのファイル システムの Language Understanding (LUIS) モデル ファイルをコピーします。
- LUIS コンテナーは複数のモデルをサポートしています。 すべてのモデルが同じフォルダーに格納されている場合は、常に 1 つの `COPY` ステートメントが必要です。
- モデル入力ディレクトリの相対的な親から docker ファイルを実行します。 次の例では、`/input` の相対的な親から `docker build` および `docker run` コマンドを実行します。 `COPY` コマンドの最初の `/input` は、ホスト コンピューターのディレクトリです。 2 つ目の `/input` はコンテナーのディレクトリです。

Dockerfile

```
FROM <container-registry>/<cognitive-service-container-name>:<tag>
ENV billing={BILLING_ENDPOINT}
ENV apikey={ENDPOINT_KEY}
ENV EULA=accept
COPY /input /input
```

必要に応じて、ローカルで、またはプライベート レジストリ コンテナーからコンテナーをビルドして実行します。

ローカル ホスト上でコンテナーを使用する方法

Docker ファイルをビルドするには、`<your-image-name>` を新しいイメージ名に置き換えてから、次を使用します。

コンソール

```
docker build -t <your-image-name> .
```

イメージを実行し、コンテナーが停止したときにそれを削除するには (`--rm`):

コンソール

```
docker run --rm <your-image-name>
```

プライベート レジストリにコンテナーを追加する方法

Dockerfile を使用して新しいイメージをプライベート コンテナーのレジストリに配置するには、次の手順を実行します。

1. 再利用のレシピのテキストを使用して `Dockerfile` を作成します。 `Dockerfile` には拡張子がありません。

2. 山かっこ内のすべての値をご自分の値に置き換えます。

3. 次のコマンドを使用して、コマンド ラインまたはターミナルでファイルをイメージにビルドします。 山かっこ `<>` 内の値は、ご自分のコンテナー名とタグに置き換えます。

   タグ オプション `-t` は、コンテナーの変更内容に関する情報を追加する方法の 1 つです。 たとえば、コンテナー名 `modified-LUIS` は、元のコンテナーが階層化されていることを示します。 タグ名 `with-billing-and-model` は、Language Understanding (LUIS) コンテナーがどのように変更されたかを示します。

   Bash

   ```
   docker build -t <your-new-container-name>:<your-new-tag-name> .
   ```

4. コンソールから Azure CLI にサインインします。 このコマンドでブラウザーが開かれ、認証が要求されます。 認証されると、ブラウザーを閉じてコンソールで作業を続行することができます。

   Azure CLI

   ```
   az login
   ```

5. コンソールから Azure CLI を使用してプライベート レジストリにサインインします。

   山かっこ `<my-registry>` 内の値をご自分のレジストリ名に置き換えます。

   Azure CLI

   ```
   az acr login --name <my-registry>
   ```

   ご自分にサービス プリンシパルが割り当てられている場合は、docker login を使用してサインインすることもできます。

```
Bash

docker login <my-registry>.azurecr.io
```

6. コンテナーにプライベート レジストリの場所のタグを付けます。 山かっこ `<my-registry>` 内の値をご自分のレジストリ名に置き換えます。

```
Bash

docker tag <your-new-container-name>:<your-new-tag-name> <my-
registry>.azurecr.io/<your-new-container-name-in-registry>:<your-new-
tag-name>
```

   タグ名を使用しない場合は、`latest` が暗黙的に使用されます。

7. 新しいイメージをプライベート コンテナー レジストリにプッシュします。 プライベート コンテナー レジストリを表示すると、次の CLI コマンドで使用されるコンテナー名がリポジトリの名前になります。

```
Bash

docker push <my-registry>.azurecr.io/<your-new-container-name-in-
registry>:<your-new-tag-name>
```

次のステップ

Azure コンテナー インスタンスの作成と使用

Azure コンテナー インスタンスにコンテナーをデプロイして実行する

[アーティクル] • 2024/02/22

次の手順に従えば、Azure Container Instances を使用してクラウド内の Azure AI サービス アプリケーションを簡単にスケーリングすることができます。 コンテナー化により、インフラストラクチャを管理することにではなく、アプリケーションの構築に集中することができます。 コンテナーの使用方法の詳細については、「機能とメリット」を参照してください。

前提条件

レシピは、任意の Azure AI サービス コンテナーで機能します。 レシピを使用する前に、Azure AI サービス リソースを作成する必要があります。 コンテナーをサポートする各 Azure AI サービスには、コンテナーのサービスをインストールして構成するための "インストール方法" の記事があります。 一部のサービスにはコンテナーへの入力としてファイルまたは一連のファイルが必要です。このソリューションを使用する前に、コンテナーを正しく理解して使用していることが重要です。

- 使用している Azure AI サービスの Azure リソース。
- Azure AI サービス リソースの**エンドポイント URL** - Azure portal 内からエンドポイント URL が表示されている場所と正しい URL の形式の例を確認する方法については、お使いのサービスのコンテナーの "インストール方法" を確認してください。 正確な形式はサービスによって異なる可能性があります。
- Azure AI サービス リソース **キー** - キーは Azure リソースの **[キー]** ページにあります。 必要なのは 2 つのキーのうち 1 つだけです。 キーは 32 文字の英数字の文字列です。
- ローカル ホスト (コンピューター) 上の 1 つの Azure AI サービス コンテナー。 以下を実行できることを確認します。
  - `docker pull` コマンドでイメージをプルする。
  - `docker run` コマンドを使用し、必要なすべての構成設定を使用してローカル コンテナーを正常に実行する。
  - コンテナーのエンドポイントを呼び出し、HTTP 2xx の応答と JSON 応答が返される。

山かっこ `<>` 内のすべての変数は、ご自分の値に置き換える必要があります。 この置き換えには山かっこも含まれます。

ⓘ 重要

LUIS コンテナーには、実行時にでプルされる `.gz` モデル ファイルが必要です。 コンテナーからは、コンテナー インスタンスからのボリューム マウントを介してこのモデル ファイルにアクセスできる必要があります。 モデル ファイルをアップロードするには、次の手順を行います。

1. **Azure ファイル共有を作成します**。 後で必要になるため、Azure ストレージ アカウント名、キー、およびファイル共有名をメモします。
2. **LUIS モデル (パッケージ アプリ) を LUIS ポータルからエクスポートします**。
3. Azure portal で、ストレージ アカウント リソースの **[概要]** ページに移動し、**[ファイル共有]** を選択します。
4. 最近作成したファイル共有名を選択し、 **[アップロード]** を選択します。 次に、パッケージ アプリをアップロードします。

Azure Portal

Azure portal を使用して Azure コンテナー インスタンス リソースを作成する

1. コンテナー インスタンスの作成 のページに移動します。

2. **[基本]** タブで、以下の詳細を入力します。

テーブルを展開する

設定	値
サブスクリプション	サブスクリプションを選択します。
Resource group	利用可能なリソース グループを選択するか、新しいリソース グループを作成します (`cognitive-services` など)。
コンテナー名	`cognitive-container-instance` などの名前を入力します。 この名前は小文字である必要があります。
場所	デプロイのためのリージョンを選択します。

設定	値
イメージの種類	資格情報を必要としないコンテナー レジストリにコンテナー イメージが格納されている場合、`Public` を選択します。 コンテナー イメージにアクセスするとき、資格情報が必要な場合、`Private` を選択します。 コンテナー イメージが `Public` または `Private` ("パブリック プレビュー") であるかどうかに関する詳細は、「コンテナーのリポジトリとイメージ」を参照してください。
イメージ名	Azure AI サービス コンテナーの場所を入力します。 場所は `docker pull` コマンドの引数として使用される場所です。 使用可能なイメージ名と対応するリポジトリについては、コンテナーのリポジトリとイメージを参照してください。 イメージ名は、3 つの部分を指定する完全修飾名にする必要があります。 最初にコンテナー レジストリ、次にリポジトリ、最後にイメージ名 `<container-registry>/<repository>/<image-name>` です。 例を 1 つ挙げてみると、`mcr.microsoft.com/azure-cognitive-services/keyphrase` であれば、Microsoft Container Registry の Azure AI サービス リポジトリにあるキー フレーズ抽出イメージを指します。 もう 1 つの例を挙げると、`containerpreview.azurecr.io/microsoft/cognitive-services-speech-to-text` は、Container Preview コンテナー レジストリの Microsoft リポジトリの音声テキスト変換イメージです。
OS の種類	`Linux`
サイズ	特定の Azure AI コンテナーに対して推奨されるサイズに変更します。 2 CPU コア 4 GB

3. **[ネットワーク]** タブで、以下の詳細を入力します。

テーブルを展開する

設定	値
Port	TCP ポートを `5000` に設定します。 ポート 5000 上でコンテナーを公開します。

4. **[詳細]** タブで、Azure Container Instance リソースのコンテナー課金設定に必要な**環境変数**を入力します。

テーブルを展開する

Key	値
`ApiKey`	リソースの [**キーとエンドポイント**] ページからコピーされます。 スペースやダッシュを含まない 32 文字の英数字文字列 (`xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`) です。
`Billing`	リソースの [**キーとエンドポイント**] ページからコピーされたエンドポイント URL。
`Eula`	`accept`

5. [**確認と作成**] を選択します

6. 検証に合格した後、 [**作成**] をクリックして作成プロセスを終了します

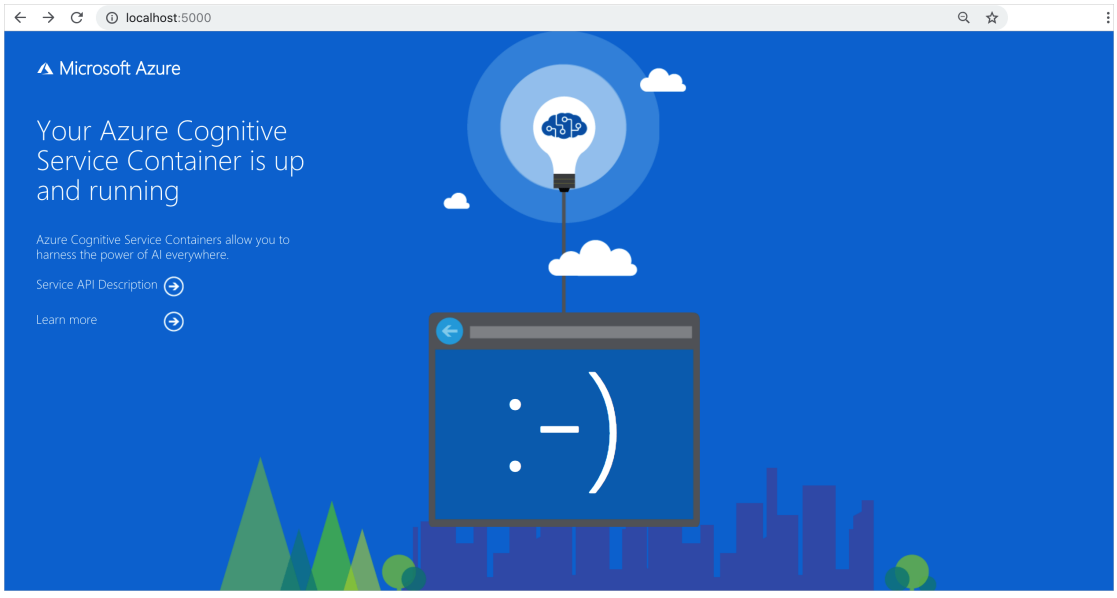
7. リソースが正常にデプロイされると、準備完了です

コンテナー インスタンスを使用する

Azure Portal

1. [**概要**] を選択し、IP アドレスをコピーします。 これは `55.55.55.55` のような数値の IP アドレスです。

2. 新しいブラウザー タブを開き、 `http://<IP-address>:5000` (`http://55.55.55.55:5000` のような IP アドレスを使用します。 コンテナーのホーム ページが表示され、コンテナーが実行中であることが示されます。



3. **[Service API Description](サービス API の説明)** を選択し、コンテナーの Swagger ページを表示します。

4. いずれかの **POST** API を選択して **[試してみる]** を選択します。入力を含むパラメーターが表示されます。 パラメーターを入力します。

5. **[実行]** を選択して、要求をコンテナー インスタンスに送信します。

   Azure コンテナー インスタンスへの Azure AI コンテナーの作成と使用は以上で完了です。

Azure Kubernetes Service に言語検出コンテナーをデプロイする

[アーティクル] • 2024/02/26

言語検出コンテナーをデプロイする方法について説明します。 この手順では、ローカルの Docker コンテナーを作成し、コンテナーを独自のプライベート コンテナー レジストリにプッシュし、Kubernetes クラスターでコンテナーを実行して、Web ブラウザーでテストする方法を示します。

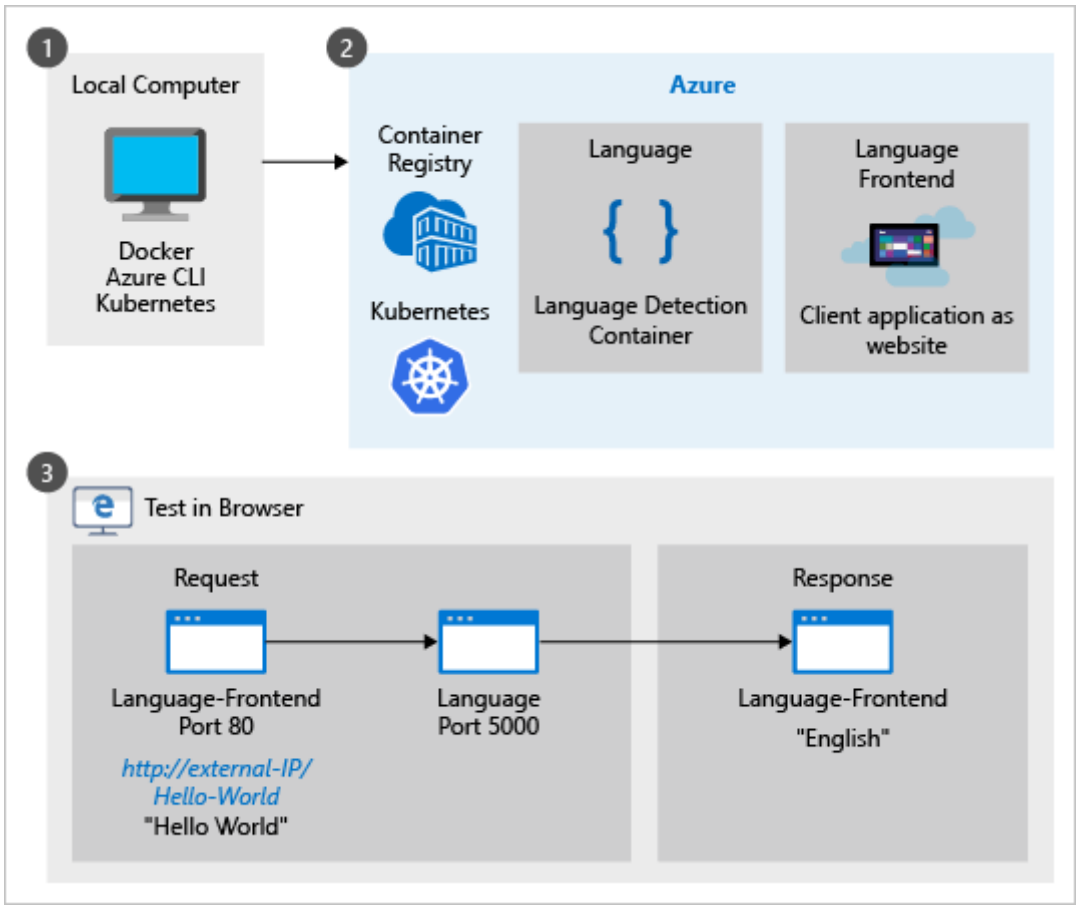
前提条件

この手順には、ローカルでインストールして実行する必要があるいくつかのツールが必要です。 Azure Cloud Shell は使用しないでください。

- Azure サブスクリプションを使用してください。 Azure サブスクリプションをお持ちでない場合は、開始する前に 無料アカウント を作成してください。
- この手順で使用するサンプル のクローンを作成できるよう、オペレーティング システム用の Git を使用してください。
- Azure CLI。
- Docker エンジン。Docker CLI がコンソール ウィンドウで動作することを確認します。
- kubectl 。
- 適切な価格レベルの Azure リソース。 すべての価格レベルでこのコンテナーを使用するわけではありません。
  - F0 または Standard 価格レベルのみの **言語**リソース。
  - S0 価格レベルの **Azure AI サービス** リソース。

サンプルの実行

この手順では、言語検出用の Azure AI サービス コンテナーのサンプルを読み込んで実行します。 このサンプルには、クライアント アプリケーション用と Azure AI サービス コンテナー用の 2 つのコンテナーがあります。 これらのイメージを両方とも Azure Container Registry にプッシュします。 独自のレジストリに設定したら、これらのイメージにアクセスしてコンテナーを実行する Azure Kubernetes Service を作成します。 コンテナーの実行中に、**kubectl** CLI を使用してコンテナーのパフォーマンスを監視します。 HTTP 要求を使用してクライアント アプリケーションにアクセスし、結果を確認します。



サンプルのコンテナー

このサンプルには 2 つのコンテナー イメージがあり、その 1 つはフロントエンドの Web サイトのイメージです。 2 つ目のイメージは、テキストの検出された言語 (カルチャ) を返す言語検出コンテナーです。 完了したら、両方のコンテナーが外部 IP からアクセス可能になります。

言語フロントエンド コンテナー

この Web サイトは、言語検出エンドポイントの要求を行う独自のクライアント側アプリケーションに相当します。 この手順が完了したら、`http://<external-IP>/<text-to-analyze>` を使用してブラウザーで Web サイトのコンテナーにアクセスして、検出された言語の文字の文字列を取得します。 この URL の例は `http://132.12.23.255/helloworld!` です。 ブラウザーでの結果は `English` です。

言語コンテナー

言語検出コンテナーは、この特定の手順では、外部の要求にアクセスできます。 このコンテナーは、標準の Azure AI サービス コンテナーに固有の言語検出 API を使用できるように、一切変更されていません。

このコンテナーの場合、その API は言語検出の POST 要求です。 すべての Azure AI コンテナーと同様、コンテナーの詳細については、ホストされている Swagger 情報 (`http://<external-IP>:5000/swagger/index.html`) を参照してください。

ポート 5000 は、Azure AI コンテナーで使用される既定のポートです。

Azure Container Registry サービスを作成する

Azure Kubernetes Service にコンテナーをデプロイするには、コンテナー イメージがアクセス可能である必要があります。 このイメージをホストする、独自の Azure Container Registry サービスを作成します。

1. Azure CLI にサインインする

   Azure CLI

   ```
   az login
   ```

2. `cogserv-container-rg` という名前のリソース グループを作成して、この手順で作成したすべてのリソースを保持します。

   Azure CLI

   ```
   az group create --name cogserv-container-rg --location westus
   ```

3. ご自分の名前とその後に `registry` が続く形式 (`pattyregistry` など) で、独自の Azure Container Registry を作成します。 名前にダッシュや下線の文字を使用しないでください。

   Azure CLI

   ```
   az acr create --resource-group cogserv-container-rg --name
   pattyregistry --sku Basic
   ```

   結果を保存して、**loginServer** プロパティを取得します。 これは、後で `language.yml` ファイルで使用する、ホストされているコンテナーのアドレスの一部となります。

   Azure CLI

   ```
   az acr create --resource-group cogserv-container-rg --name
   pattyregistry --sku Basic
   ```

出力

```
{
    "adminUserEnabled": false,
    "creationDate": "2019-01-02T23:49:53.783549+00:00",
    "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/cogserv-container-
rg/providers/Microsoft.ContainerRegistry/registries/pattyregistry",
    "location": "westus",
    "loginServer": "pattyregistry.azurecr.io",
    "name": "pattyregistry",
    "provisioningState": "Succeeded",
    "resourceGroup": "cogserv-container-rg",
    "sku": {
        "name": "Basic",
        "tier": "Basic"
    },
    "status": null,
    "storageAccount": null,
    "tags": {},
    "type": "Microsoft.ContainerRegistry/registries"
}
```

4. コンテナー レジストリにサイン インします。 レジストリにイメージをプッシュする前に、ログインする必要があります。

Azure CLI

```
az acr login --name pattyregistry
```

Web サイトの Docker イメージを取得する

1. この手順で使用するサンプル コードは、Azure AI コンテナーのサンプル リポジトリにあります。 リポジトリを複製して、サンプルのローカル コピーを作成します。

コンソール

```
git clone https://github.com/Azure-Samples/cognitive-services-
containers-samples
```

リポジトリがローカル コンピューターに作成されたら、\dotnet\Language\FrontendService ディレクトリで Web サイトを検索します。 この Web サイトは、言語検出コンテナーでホストされる言語検出 API を呼び出すクライアント アプリケーションとして機能します。

2. この Web サイトの Docker イメージをビルドします。 次のコマンドを実行するときに、Dockerfile がある \FrontendService ディレクトリにコンソールがあることを確認します。

```
コンソール

docker build -t language-frontend -t
pattiyregistry.azurecr.io/language-frontend:v1 .
```

コンテナー レジストリのバージョンを追跡するには、バージョン形式 (`v1` など) を含むタグを追加します。

3. コンテナー レジストリにイメージをプッシュします。 これには数分かかることがあります。

```
コンソール

docker push pattyregistry.azurecr.io/language-frontend:v1
```

`unauthorized: authentication required` エラーが表示された場合、`az acr login --name <your-container-registry-name>` コマンドを使用してログインします。

プロセスが完了すると、結果は次の例のようになります。

```
出力

The push refers to repository [pattyregistry.azurecr.io/language-
frontend]
82ff52ee6c73: Pushed
07599c047227: Pushed
816caf41a9a1: Pushed
2924be3aed17: Pushed
45b83a23806f: Pushed
ef68f6734aa4: Pushed
v1: digest:
sha256:31930445deee181605c0cde53dab5a104528dc1ff57e5b3b34324f0d8a0eb286
size: 1580
```

言語検出 Docker イメージを取得する

1. ローカル コンピューターに最新バージョンの Docker イメージをプルします。 これには数分かかることがあります。 このコンテナーの新しいバージョンがある場合は、値を `1.1.006770001-amd64-preview` から新しいバージョンに変更します。

```

```

コンソール

```
docker pull mcr.microsoft.com/azure-cognitive-
services/language:1.1.006770001-amd64-preview
```

2. コンテナー レジストリを含むイメージをタグ付けします。 最新バージョンを検索し、より新しいバージョンがある場合はバージョン `1.1.006770001-amd64-preview` を置き換えます。

コンソール

```
docker tag mcr.microsoft.com/azure-cognitive-services/language
pattiyregistry.azurecr.io/language:1.1.006770001-amd64-preview
```

3. コンテナー レジストリにイメージをプッシュします。 これには数分かかることがあります。

コンソール

```
docker push pattyregistry.azurecr.io/language:1.1.006770001-amd64-
preview
```

コンテナー レジストリの資格情報を取得する

次の手順は、この手順で後で作成する Azure Kubernetes Service で、コンテナー レジストリへの接続に必要な情報を取得するために必要です。

1. サービス プリンシパルを作成します。

Azure CLI

```
az ad sp create-for-rbac
```

手順 3 で割り当てたパラメーター `<appId>` の結果の値 `appId` を保存します。 次のセクションの client-secret パラメーター `<client-secret>` のために `password` を保存します。

出力

```
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "azure-cli-2018-12-31-18-39-32",
  "name": "http://azure-cli-2018-12-31-18-39-32",
  "password": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
```

```
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

2. コンテナー レジストリ ID を取得します。

Azure CLI

```
az acr show --resource-group cogserv-container-rg --name pattyregistry
--query "id" --output table
```

次の手順で、スコープ パラメーター値、`<acrId>` の出力を保存します。 次のように表示されます。

出力

```
/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/cogserv-container-
rg/providers/Microsoft.ContainerRegistry/registries/pattyregistry
```

このセクションの手順 3 の完全な値を保存します。

3. コンテナー イメージに格納されているイメージを使用するために、AKS クラスターに適切なアクセス権を付与するには、ロールの割り当てを作成します。 `<appId>` と `<acrId>` を、前の 2 つの手順で収集した値に置き換えます。

Azure CLI

```
az role assignment create --assignee <appId> --scope <acrId> --role
Reader
```

Azure Kubernetes Service を作成する

1. Kubernetes クラスターを作成します。 name パラメーターを除き、すべてのパラメーター値は前のセクションと同じです。 作成したユーザーとその目的を示す名前 (`patty-kube` など) を選択します。

Azure CLI

```
az aks create --resource-group cogserv-container-rg --name patty-kube -
-node-count 2  --service-principal <appId>  --client-secret <client-
secret>  --generate-ssh-keys
```

この手順には数分かかることがあります。 結果は次のとおりです。

出力


```
{
  "aadProfile": null,
  "addonProfiles": null,
  "agentPoolProfiles": [
    {
      "count": 2,
      "dnsPrefix": null,
      "fqdn": null,
      "maxPods": 110,
      "name": "nodepool1",
      "osDiskSizeGb": 30,
      "osType": "Linux",
      "ports": null,
      "storageProfile": "ManagedDisks",
      "vmSize": "Standard_DS1_v2",
      "vnetSubnetId": null
    }
  ],
  "dnsPrefix": "patty-kube--65a101",
  "enableRbac": true,
  "fqdn": "patty-kube--65a101-341f1f54.hcp.westus.azmk8s.io",
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourcegroups/cogserv-container-
rg/providers/Microsoft.ContainerService/managedClusters/patty-kube",
  "kubernetesVersion": "1.9.11",
  "linuxProfile": {
    "adminUsername": "azureuser",
    "ssh": {
      "publicKeys": [
        {
          "keyData": "ssh-rsa AAAAB3NzaC...ohR2d81mFC
        }
      ]
    }
  },
  "location": "westus",
  "name": "patty-kube",
  "networkProfile": {
    "dnsServiceIp": "10.0.0.10",
    "dockerBridgeCidr": "172.17.0.1/16",
    "networkPlugin": "kubenet",
    "networkPolicy": null,
    "podCidr": "10.244.0.0/16",
    "serviceCidr": "10.0.0.0/16"
  },
  "nodeResourceGroup": "MC_patty_westus",
  "provisioningState": "Succeeded",
  "resourceGroup": "cogserv-container-rg",
  "servicePrincipalProfile": {
    "clientId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "keyVaultSecretRef": null,
    "secret": null
```

```
  },
  "tags": null,
  "type": "Microsoft.ContainerService/ManagedClusters"
}
```

サービスが作成されますが、Web サイトのコンテナーや言語検出コンテナーはまだありません。

2. Kubernetes クラスターの資格情報を取得します。

Azure CLI

```
az aks get-credentials --resource-group cogserv-container-rg --name
patty-kube
```

Kubernetes サービスにオーケストレーションの定義を読み込む

このセクションでは、**kubectl** CLI を使用して Azure Kubernetes Service と通信します。

1. オーケストレーションの定義を読み込む前に、**kubectl** がノードにアクセスできることを確認します。

コンソール

```
kubectl get nodes
```

応答は次のようになります。

出力

```
NAME                       STATUS    ROLES     AGE       VERSION
aks-nodepool1-13756812-0   Ready     agent     6m        v1.9.11
aks-nodepool1-13756812-1   Ready     agent     6m        v1.9.11
```

2. 次のファイルをコピーし、`language.yml` という名前を付けます。 このファイルには、2 種類のコンテナー (`language-frontend` Web サイトのコンテナーと`language` 検出コンテナー) のそれぞれに、`service` セクションと `deployment` セクションがあります。

yml

```
# A service which exposes the .net frontend app container through a
dependable hostname: http://language-frontend:5000
apiVersion: v1
kind: Service
metadata:
  name: language-frontend
  labels:
    run: language-frontend
spec:
  selector:
    app: language-frontend
  type: LoadBalancer
  ports:
  - name: front
    port: 80
    targetPort: 80
    protocol: TCP
---
# A deployment declaratively indicating how many instances of the .net
frontend app container we want up
apiVersion: apps/v1beta1
kind: Deployment
metadata:
  name: language-frontend
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: language-frontend
    spec:
      containers:
      - name: language-frontend
        image: # < URI of the Frontend App image >
        ports:
        - name: public-port
          containerPort: 80
        livenessProbe:
          httpGet:
            path: /status
            port: public-port
          initialDelaySeconds: 30
          timeoutSeconds: 1
          periodSeconds: 10
      imagePullSecrets:
        - name: # < Name of the registry secret providing access to the
frontend image >
      automountServiceAccountToken: false
---
# A service which exposes the cognitive-service containers through a
dependable hostname: http://language:5000
apiVersion: v1
kind: Service
metadata:
```

```
  name: language
  labels:
    run: language
spec:
  selector:
    app: language
  type: LoadBalancer
  ports:
  - name: language
    port: 5000
    targetPort: 5000
    protocol: TCP
---
# A deployment declaratively indicating how many instances of the
cognitive-service container we want up
apiVersion: apps/v1beta1
kind: Deployment
metadata:
  name: language
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: language
    spec:
      containers:
      - name: language
        image: # < URI of the Language Image >
        ports:
        - name: public-port
          containerPort: 5000
        livenessProbe:
          httpGet:
            path: /status
            port: public-port
          initialDelaySeconds: 30
          timeoutSeconds: 1
          periodSeconds: 10
        args:
            - "eula=accept"
            - "apikey=" # < API Key for the Language Service >
            - "billing=" # < Language billing endpoint URI >

      imagePullSecrets:
        - name: # < Name of the registry secret providing access to the
Language image >

      automountServiceAccountToken: false
```

3. 次の表に基づいて `language.yml` の言語フロントエンドのデプロイの行を変更して、独自のコンテナー レジストリのイメージ名、クライアント シークレット、および言語サービスの設定を追加します。

テーブルを展開する

言語フロントエンドのデプロイ設定	目的
行 32 `image` プロパティ	コンテナー レジストリ内のフロントエンド イメージのイメージの場所 `<container-registry-name>.azurecr.io/language-frontend:v1`
行 44 `name` プロパティ	イメージの Container Registry シークレット (前のセクションでは `<client-secret>` と呼ばれています)。

4. 次の表に基づいて `language.yml` の言語のデプロイの行を変更して、独自のコンテナー レジストリのイメージ名、クライアント シークレット、および言語サービスの設定を追加します。

テーブルを展開する

言語のデプロイの設定	目的
行 78 `image` プロパティ	コンテナー レジストリ内の言語イメージのイメージの場所 `<container-registry-name>.azurecr.io/language:1.1.006770001-amd64-preview`
行 95 `name` プロパティ	イメージの Container Registry シークレット (前のセクションでは `<client-secret>` と呼ばれています)。
行 91 `apiKey` プロパティ	言語サービスのリソース キー
行 92 `billing` プロパティ	言語サービス リソースの課金エンドポイント。 `https://westus.api.cognitive.microsoft.com/text/analytics/v2.1`

apiKey と **課金エンドポイント**は、Kubernetes オーケストレーションの定義の一部として設定されているため、Web サイト コンテナーがこれらについて認識したり要求の一部として渡したりする必要はありません。 Web サイト コンテナーは、そのオーケストレーター名 `language` によって言語検出コンテナーを示します。

5. このサンプルのオーケストレーションの定義ファイルを、`language.yml` を作成して保存したフォルダーから読み込みます。

コンソール

```
kubectl apply -f language.yml
```

応答は次のとおりです。

出力

```
service "language-frontend" created
deployment.apps "language-frontend" created
service "language" created
deployment.apps "language" created
```

コンテナーの外部 IP を取得する

2 つのコンテナーについて、`language-frontend` と `language` のサービスが実行中であることを確認し、外部 IP アドレスを取得します。

コンソール

```
kubectl get all
```

出力

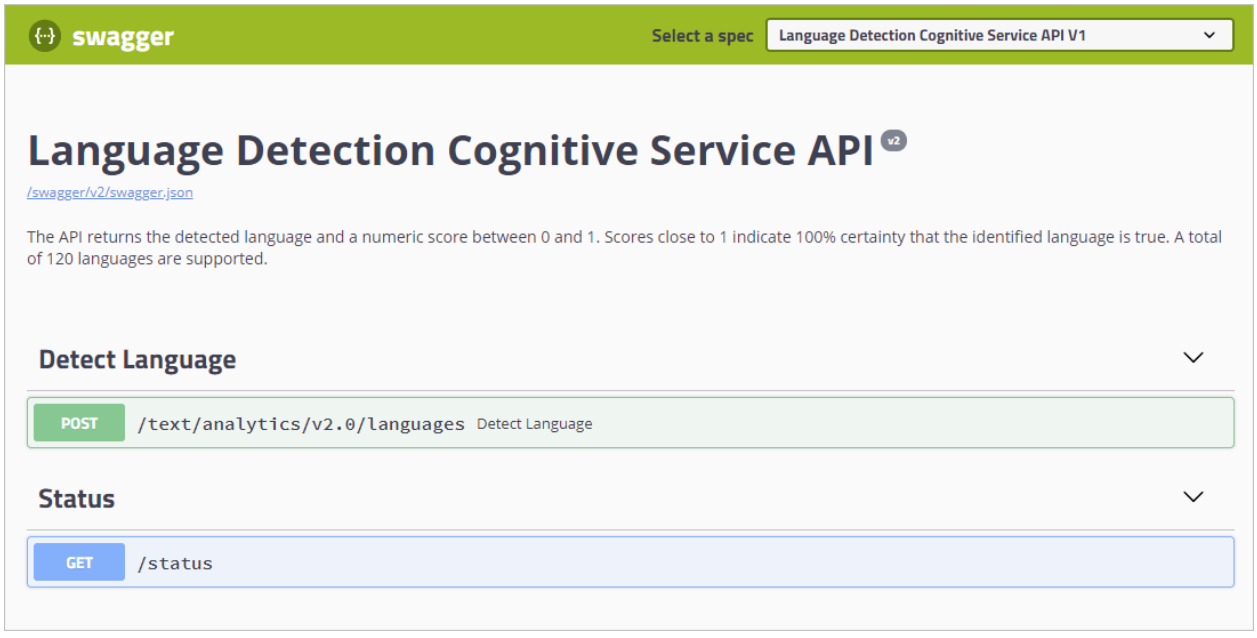
```
NAME                                     READY     STATUS    RESTARTS   AGE
pod/language-586849d8dc-7zvz5            1/1       Running   0          13h
pod/language-frontend-68b9969969-bz9bg   1/1       Running   1          13h

NAME                         TYPE           CLUSTER-IP    EXTERNAL-IP
PORT(S)          AGE
service/kubernetes           ClusterIP      10.0.0.1      <none>
443/TCP          14h
service/language             LoadBalancer   10.0.39.169   104.42.172.68
5000:30161/TCP   13h
service/language-frontend    LoadBalancer   10.0.42.136   104.42.37.219
80:30943/TCP     13h

NAME                                    DESIRED   CURRENT   UP-TO-DATE
AVAILABLE   AGE
deployment.extensions/language             1         1         1            1
13h
deployment.extensions/language-frontend    1         1         1            1
13h

NAME                                               DESIRED   CURRENT
READY     AGE
replicaset.extensions/language-586849d8dc            1         1         1
13h
replicaset.extensions/language-frontend-68b9969969   1         1         1
```

```
13h

NAME                                  DESIRED   CURRENT   UP-TO-DATE
AVAILABLE   AGE
deployment.apps/language              1         1         1            1
13h
deployment.apps/language-frontend     1         1         1            1
13h

NAME                                           DESIRED   CURRENT   READY
AGE
replicaset.apps/language-586849d8dc            1         1         1
13h
replicaset.apps/language-frontend-68b9969969   1         1         1
13h
```

サービスの `EXTERNAL-IP` が保留中として表示される場合は、次の手順に進む前に、IP アドレスが表示されるまでコマンドを再実行します。

言語検出コンテナーをテストする

ブラウザーを開いて、前のセクションの `language` コンテナーの外部 IP (`http://<external-ip>:5000/swagger/index.html`) に移動します。 API の `Try it` 機能を使用して、言語検出エンドポイントをテストすることができます。



クライアント アプリケーション コンテナーをテストする

`http://<external-ip>/helloworld` の形式を使用して、ブラウザーで URL を `language-frontend` コンテナーの外部 IP に変更します。 `helloworld` の英語のカルチャ テキストは `English` と予測されます。

リソースをクリーンアップする

クラスターの作業が終了したら、Azure リソース グループを削除します。

Azure CLI

```
az group delete --name cogserv-container-rg
```

関連情報

- Docker ユーザーのための kubectl

次のステップ

Azure AI コンテナー

Docker Compose を使用して複数のコンテナーをデプロイする

[アーティクル] • 2024/02/22

この記事では、複数の Azure AI コンテナーをデプロイする方法について説明します。 具体的には、Docker Compose を使用して複数の Docker コンテナー イメージをオーケストレーションする方法について説明します。

> Docker Compose は、マルチコンテナー Docker アプリケーションを定義して実行するためのツールです。 Compose では、YAML ファイルを使用してアプリケーションのサービスを構成します。 次に、1 つのコマンドを実行することによって、構成からすべてのサービスを作成して開始します。

1 台のホスト コンピューター上で複数のコンテナー イメージをオーケストレーションすると便利な場合があります。 この記事では、読み取りおよび Document Intelligence のコンテナーをまとめます。

前提条件

この手順には、ローカルでインストールして実行する必要があるいくつかのツールが必要です。

- Azure サブスクリプション。 お持ちでない場合は、開始する前に無料アカウントを作成してください。
- Docker エンジン。 Docker CLI がコンソール ウィンドウで動作することを確認します。
- 適切な価格レベルの Azure リソース。 このコンテナーでは次の価格レベルのみが有効です。
  - F0 または Standard 価格レベルのみの **Azure AI Vision** リソース。
  - F0 または Standard 価格レベルのみの **Document Intelligence** リソース。
  - S0 価格レベルの **Azure AI サービス** リソース。
- ゲート プレビュー コンテナーを使用している場合、オンライン要求フォームに入力して使用する必要があります。

Docker Compose ファイル

YAML ファイルには、デプロイされるすべてのサービスが定義されています。 これらのサービスは、`DockerFile` または既存のコンテナー イメージのどちらかに依存しま

す。 この例では、2 つのプレビュー イメージを使用します。 次の YAML ファイルをコピーして貼り付け、*docker-compose.yaml* という名前で保存します。 ファイルで適切な **apikey**、**billing**、および **EndpointUri** の値を指定します。

YAML

```yaml
version: '3.7'
services:
  forms:
    image: "mcr.microsoft.com/azure-cognitive-services/form-recognizer/layout"
    environment:
       eula: accept
       billing: # < Your Document Intelligence billing URL >
       apikey: # < Your Document Intelligence API key >
       FormRecognizer__ComputerVisionApiKey: # < Your Document Intelligence API key >
       FormRecognizer__ComputerVisionEndpointUri: # < Your Document Intelligence URI >
    volumes:
       - type: bind
         source: E:\publicpreview\output
         target: /output
       - type: bind
         source: E:\publicpreview\input
         target: /input
    ports:
      - "5010:5000"

  ocr:
    image: "mcr.microsoft.com/azure-cognitive-services/vision/read:3.1-preview"
    environment:
      eula: accept
      apikey: # < Your Azure AI Vision API key >
      billing: # < Your Azure AI Vision billing URL >
    ports:
      - "5021:5000"
```

> **ⓘ 重要**
>
> ホスト マシン上に、**volumes** ノード以下に指定されているディレクトリを作成します。 ボリューム バインドを使用してイメージをマウントする前にディレクトリが存在している必要があるので、この方法が必要です。

構成された Docker Compose サービスを開始する

Docker Compose ファイルを使用すると、定義されたサービスのライフ サイクルのすべての段階 (サービスの開始、停止、再構築、サービス状態の表示、ログのストリーミング) を管理できます。 プロジェクト ディレクトリ (docker-compose.yaml ファイルがある場所) からコマンドライン インターフェイスを開きます。

> ⓘ **注意**
>
> エラーを避けるために、ホスト マシンと Docker エンジンがドライブを適切に共有していることを確認します。 たとえば、*E:\publicpreview* が *docker-compose.yaml* ファイルのディレクトリとして使用されている場合、ドライブ **E** を Docker と共有します。

コマンドライン インターフェイスから次のコマンドを実行して、*docker-compose.yaml* ファイルに定義されているすべてのサービスを開始 (または再開) します。

コンソール

```
docker-compose up
```

この構成を使用して **docker-compose up** コマンドを初めて実行するとき、Docker は **services** ノード下に構成されているイメージを取得してから、それらをダウンロードしてマウントします。

コンソール

```
Pulling forms (mcr.microsoft.com/azure-cognitive-services/form-
recognizer/layout:)...
latest: Pulling from azure-cognitive-services/form-recognizer/layout
743f2d6c1f65: Pull complete
72befba99561: Pull complete
2a40b9192d02: Pull complete
c7715c9d5c33: Pull complete
f0b33959f1c4: Pull complete
b8ab86c6ab26: Pull complete
41940c21ed3c: Pull complete
e3d37dd258d4: Pull complete
cdb5eb761109: Pull complete
fd93b5f95865: Pull complete
ef41dcbc5857: Pull complete
4d05c86a4178: Pull complete
34e811d37201: Pull complete
Pulling ocr (mcr.microsoft.com/azure-cognitive-services/vision/read:3.1-
preview:)...
latest: Pulling from /azure-cognitive-services/vision/read:3.1-preview
f476d66f5408: Already exists
8882c27f669e: Already exists
d9af21273955: Already exists
```

```
f5029279ec12: Already exists
1a578849dcd1: Pull complete
45064b1ab0bf: Download complete
4bb846705268: Downloading [=========================================>
]  187.1MB/222.8MB
c56511552241: Waiting
e91d2aa0f1ad: Downloading [==============================================>
]  162.2MB/176.1MB
```

イメージがダウンロードされると、イメージ サービスが開始されます。

コンソール

```
Starting docker_ocr_1   ... done
Starting docker_forms_1 ... doneAttaching to docker_ocr_1,
docker_forms_1forms_1  | forms_1  | forms_1  | Notice: This Preview is made
available to you on the condition that you agree to the Supplemental Terms
of Use for Microsoft Azure Previews [https://go.microsoft.com/fwlink/?
linkid=2018815], which supplement your agreement
[https://go.microsoft.com/fwlink/?linkid=2018657] governing your use of
Azure. If you do not have an existing agreement governing your use of Azure,
you agree that your agreement governing use of Azure is the Microsoft Online
Subscription Agreement [https://go.microsoft.com/fwlink/?linkid=2018755]
(which incorporates the Online Services Terms
[https://go.microsoft.com/fwlink/?linkid=2018760]). By using the Preview you
agree to these terms.
forms_1  |
forms_1  |
forms_1  | Using '/input' for reading models and other read-only data.
forms_1  | Using '/output/forms/812d811d1bcc' for writing logs and other
output data.
forms_1  | Logging to console.
forms_1  | Submitting metering to
'https://westus2.api.cognitive.microsoft.com/'.
forms_1  | WARNING: No access control enabled!
forms_1  | warn: Microsoft.AspNetCore.Server.Kestrel[0]
forms_1  |       Overriding address(es) 'http://+:80'. Binding to endpoints
defined in UseKestrel() instead.
forms_1  | Hosting environment: Production
forms_1  | Content root path: /app/forms
forms_1  | Now listening on: http://0.0.0.0:5000
forms_1  | Application started. Press Ctrl+C to shut down.
ocr_1    |
ocr_1    |
ocr_1    | Notice: This Preview is made available to you on the condition
that you agree to the Supplemental Terms of Use for Microsoft Azure Previews
[https://go.microsoft.com/fwlink/?linkid=2018815], which supplement your
agreement [https://go.microsoft.com/fwlink/?linkid=2018657] governing your
use of Azure. If you do not have an existing agreement governing your use of
Azure, you agree that your agreement governing use of Azure is the Microsoft
Online Subscription Agreement [https://go.microsoft.com/fwlink/?
linkid=2018755] (which incorporates the Online Services Terms
[https://go.microsoft.com/fwlink/?linkid=2018760]). By using the Preview you
```

```
agree to these terms.
ocr_1    |
ocr_1    |
ocr_1    | Logging to console.
ocr_1    | Submitting metering to
'https://westcentralus.api.cognitive.microsoft.com/'.
ocr_1    | WARNING: No access control enabled!
ocr_1    | Hosting environment: Production
ocr_1    | Content root path: /
ocr_1    | Now listening on: http://0.0.0.0:5000
ocr_1    | Application started. Press Ctrl+C to shut down.
```

サービスの可用性を確認する

ヒント

docker images コマンドを使用して、ダウンロードしたコンテナー イメージを一覧表示できます。 たとえば、次のコマンドは、ダウンロードした各コンテナー イメージの ID、リポジトリ、およびタグが表として書式設定されて表示されます。

```
docker images --format "table {{.ID}}\t{{.Repository}}\t{{.Tag}}"

IMAGE ID         REPOSITORY                TAG
<image-id>       <repository-path/name>    <tag-name>
```

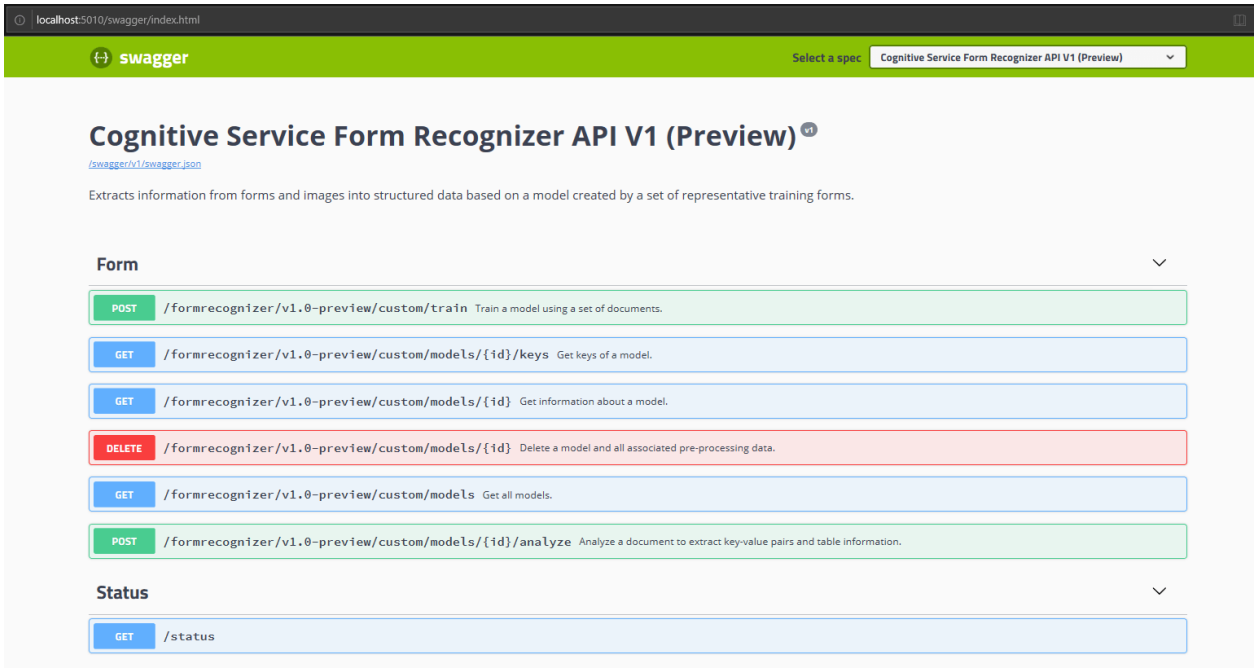
出力例を次に示します。

```
IMAGE ID            REPOSITORY
TAG
2ce533f88e80        mcr.microsoft.com/azure-cognitive-services/form-
recognizer/layout          latest
4be104c126c5        mcr.microsoft.com/azure-cognitive-
services/vision/read:3.1-preview         latest
```

テスト コンテナー

ホスト マシンでブラウザーを開き、*docker-compose.yaml* ファイルで指定されたポート (http://localhost:5021/swagger/index.html. など) を使用して **localhost** にアクセスします。 たとえば、API の **[使ってみる]** 機能を使用して、Document Intelligence エンドポ

イントをテストできます。 両方のコンテナーの swagger ページを使用およびテストできます。



次のステップ

Azure AI コンテナー

チュートリアル:Azure Container Instances へのデプロイに使用するコンテナー イメージを作成する

[アーティクル] • 2023/06/01

Azure Container Instances では、仮想マシンをプロビジョニングしたり、上位レベルのサービスを採用したりせずに、Azure のインフラストラクチャ上に Docker コンテナーをデプロイすることができます。 このチュートリアルでは、小さな Node.js Web アプリケーションを、Azure Container Instances を使用して実行できるコンテナー イメージにパッケージ化します。

シリーズの第 1 部となるこの記事では、次の内容を学習します。

- ✓ GitHub からアプリケーション ソース コードを複製する
- ✓ アプリケーション ソースからコンテナー イメージを作成する
- ✓ ローカル Docker 環境でイメージをテストする

チュートリアルのパート2 およびパート 3 では、Azure Container Registry にイメージをアップロードした後、Azure Container Instances にデプロイします。

始める前に

このチュートリアルを完了するには、次の要件を満たす必要があります。

Azure CLI:ローカル コンピューターに Azure CLI バージョン 2.0.29 以降がインストールされている必要があります。 バージョンを確認するには、`az --version` を実行します。 インストールまたはアップグレードが必要な場合は、Azure CLI のインストールに関するページを参照してください。

Docker:このチュートリアルの前提として、コンテナー、コンテナー イメージ、基本 `docker` コマンドなど、Docker のコア概念を基本的に理解している必要があります。 Docker やコンテナーの基礎に関する入門情報については、「Docker overview」(Docker の概要) を参照してください。

Docker:このチュートリアルを完了するには、Docker がローカル環境にインストールされている必要があります。 Docker には、macOS、Windows、Linux 上で Docker 環境の構成を行うパッケージが用意されています。

> ⓘ **重要**

Azure Cloud Shell には Docker デーモンが含まれていないため、このチュートリアルを完了するためには、Azure CLI と Docker エンジンの両方を自分でローカル コンピューターにインストールする必要があります。 このチュートリアルで Azure Cloud Shell を使用することはできません。

アプリケーションのコードを入手する

このチュートリアルのサンプル アプリケーションは、Node.js で構築した単純な Web アプリです。 このアプリケーションは、次のスクリーンショットに示したような静的 HTML ページを返します。

次のように、Git を使ってサンプル アプリケーションのリポジトリを複製します。

```
git clone https://github.com/Azure-Samples/aci-helloworld.git
```

GitHub から直接 ZIP アーカイブをダウンロードすることもできます。

コンテナー イメージを構築する

サンプル アプリケーションに含まれる Dockerfile は、コンテナーの構築方法を示しています。 その方法は、Alpine Linux に基づく公式 Node.js イメージから始まります。これは、コンテナーで使用するのに適した小規模なディストリビューションです。次に、アプリケーション ファイルをコンテナーにコピーし、ノード パッケージ マネー

ジャーを使用して依存関係をインストールして、最後にアプリケーションを起動します。

Dockerfile

```
FROM node:8.9.3-alpine
RUN mkdir -p /usr/src/app
COPY ./app/* /usr/src/app/
WORKDIR /usr/src/app
RUN npm install
CMD node /usr/src/app/index.js
```

docker build コマンドを使用してコンテナー イメージを作成し、これを *aci-tutorial-app* としてタグ付けします。

Bash

```
docker build ./aci-helloworld -t aci-tutorial-app
```

docker build コマンドの出力は次のようになります (わかりやすくするために切り詰められています)。

Bash

```
docker build ./aci-helloworld -t aci-tutorial-app
```

出力

```
Sending build context to Docker daemon  119.3kB
Step 1/6 : FROM node:8.9.3-alpine
8.9.3-alpine: Pulling from library/node
88286f41530e: Pull complete
84f3a4bf8410: Pull complete
d0d9b2214720: Pull complete
Digest:
sha256:c73277ccc763752b42bb2400d1aaecb4e3d32e3a9dbedd0e49885c71bea07354
Status: Downloaded newer image for node:8.9.3-alpine
 ---> 90f5ee24bee2
...
Step 6/6 : CMD node /usr/src/app/index.js
 ---> Running in f4a1ea099eec
 ---> 6edad76d09e9
Removing intermediate container f4a1ea099eec
Successfully built 6edad76d09e9
Successfully tagged aci-tutorial-app:latest
```

docker images コマンドを使用して、構築されたイメージを確認します。

Bash

```
docker images
```

新しく構築したイメージがリストに表示されます。

Bash

```
docker images
```

出力

```
REPOSITORY          TAG       IMAGE ID        CREATED           SIZE
aci-tutorial-app    latest    5c745774dfa9    39 seconds ago    68.1 MB
```

コンテナーをローカルで実行する

Azure Container Instances にコンテナーをデプロイする前に、docker run を使ってローカルでコンテナーを実行し、コンテナーが動作することを確認します。 `-d` スイッチを使用すると、コンテナーをバックグラウンドで実行できます。一方、`-p` スイッチでは、コンピューター上の任意のポートをコンテナーのポート 80 にマップすることができます。

Bash

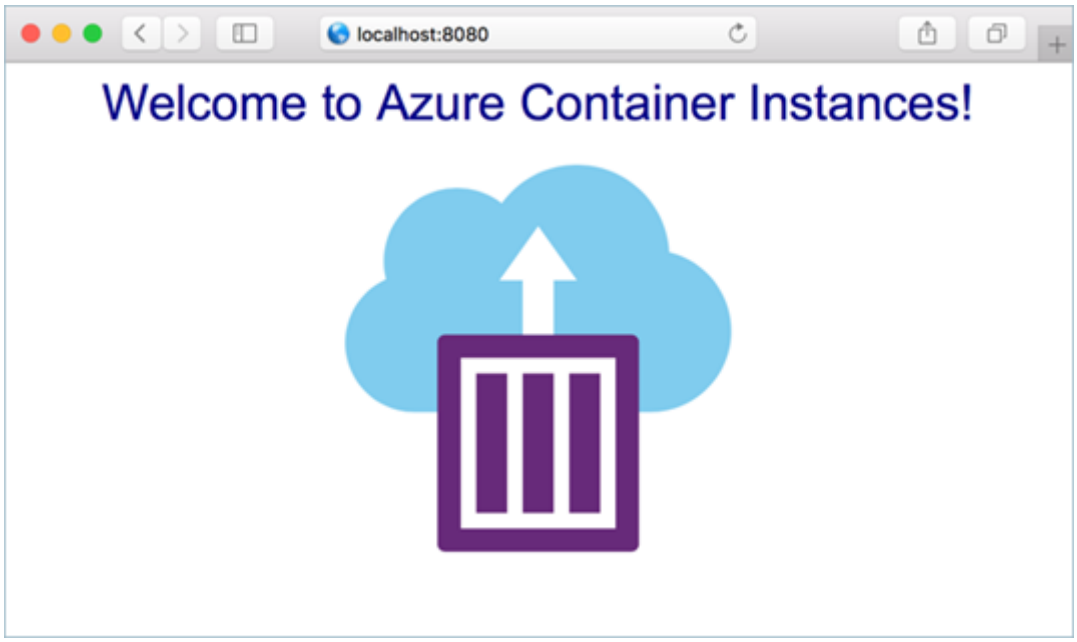
```
docker run -d -p 8080:80 aci-tutorial-app
```

`docker run` コマンドが成功した場合、コマンドからの出力に、実行中のコンテナーの ID が表示されます。

Bash

```
docker run -d -p 8080:80 aci-tutorial-app
```output
a2e3e4435db58ab0c664ce521854c2e1a1bda88c9cf2fcff46aedf48df86cccf
```

今度は、ブラウザーで `http://localhost:8080` に移動し、コンテナーが実行されていることを確認します。 次のような Web ページが表示されます。
```



次の手順

このチュートリアルでは、Azure Container Instances にデプロイできるコンテナー イメージを作成し、ローカルで実行されていることを確認しました。 ここで行った作業は次のとおりです。

- ✓ GitHub からのアプリケーション ソースの複製
- ✓ アプリケーション ソースからのコンテナー イメージの作成
- ✓ コンテナーのローカルでのテスト

シリーズの次のチュートリアルに進んで、Azure Container Registry にコンテナー イメージを格納する方法について学習します。

Azure Container Registry へのイメージのプッシュ

クイック スタート:Azure CLI を使用したプライベート コンテナー レジストリの作成

[アーティクル] • 2023/10/31

Azure Container Registry は、コンテナー イメージおよび関連アーティクルのビルド、保管、管理をするための、プライベート レジストリ サービスです。 このクイックスタートでは、Azure CLI を使用して Azure コンテナー レジストリ インスタンスを作成します。 次に、Docker コマンドを使用してコンテナー イメージをレジストリにプッシュし、最後にレジストリからイメージをプルして実行します。

このクイック スタートでは、Azure CLI を実行している必要があります (バージョン 2.0.55 以降を推奨)。 バージョンを確認するには、`az --version` を実行します。 インストールまたはアップグレードする必要がある場合は、Azure CLI のインストールに関するページを参照してください。

Docker もローカルにインストールする必要があります。 Docker では、macOS、Windows、または Linux システムで Docker を簡単に構成できるパッケージが提供されています。

Azure Cloud Shell には、必要な Docker コンポーネント (`dockerd` デーモン) すべてが含まれていないため、このクイックスタートで Cloud Shell を使用することはできません。

リソース グループを作成する

az group create コマンドを使用して、リソース グループを作成します。 Azure リソース グループとは、Azure リソースのデプロイと管理に使用する論理コンテナーです。

次の例では、*myResourceGroup* という名前のリソース グループを *eastus* に作成します。

Azure CLI

```
az group create --name myResourceGroup --location eastus
```

コンテナー レジストリの作成

このクイック スタートでは、*Basic* レジストリを作成します。これは、Azure Container Registry について学習している開発者にとって、コストが最適なオプションです。 利用可能なサービス レベルの詳細については、コンテナー レジストリのサービス レベルに関するページを参照してください。

az acr create コマンドを使用して ACR インスタンスを作成します。 レジストリ名は Azure 内で一意であり、5 から 50 文字の小文字の英数字を含める必要があります。 次の例では、*mycontainerregistry* を使用します。 これを一意の値に更新します。

Azure CLI

```
az acr create --resource-group myResourceGroup \
  --name mycontainerregistry --sku Basic
```

レジストリが作成されると、出力は次のようになります。

JSON

```
{
  "adminUserEnabled": false,
  "creationDate": "2019-01-08T22:32:13.175925+00:00",
  "id": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/myResourceGroup/providers/Microsoft.ContainerReg
istry/registries/mycontainerregistry",
  "location": "eastus",
  "loginServer": "mycontainerregistry.azurecr.io",
  "name": "mycontainerregistry",
  "provisioningState": "Succeeded",
  "resourceGroup": "myResourceGroup",
  "sku": {
    "name": "Basic",
    "tier": "Basic"
  },
  "status": null,
  "storageAccount": null,
  "tags": {},
  "type": "Microsoft.ContainerRegistry/registries"
}
```

出力の `loginServer` をメモしておいてください。これは、完全修飾レジストリ名です (すべて小文字)。 以降このクイックスタートでは、コンテナー レジストリ名のプレースホルダーとして `<registry-name>` を、レジストリのログイン サーバー名のプレースホルダーとして `<login-server>` を使用します。

ヒント

このクイック スタートでは、*Basic* レジストリを作成します。これは、Azure Container Registry について学習している開発者にとって、コストが最適なオプションです。 ストレージとイメージのスループットを向上させる他のレベルと、**プライベート エンドポイント** を使用した接続などの機能を選択します。 利用可能なサービス レベル (SKU) の詳細については、**コンテナー レジストリのサービス レベル**に関するページを参照してください。

レジストリへのログイン

コンテナー イメージをプッシュしたりプルしたりするには、あらかじめレジストリにログインしておく必要があります。 そのためには、az acr login コマンドを使用します。 Azure CLI でログインする際は、レジストリ リソース名のみを指定します。 完全修飾ログイン サーバー名は使用しません。

Azure CLI

```
az acr login --name <registry-name>
```

例:

Azure CLI

```
az acr login --name mycontainerregistry
```

このコマンドが完了すると、`Login Succeeded` というメッセージが返されます。

レジストリにイメージをプッシュする

Azure Container Registry にイメージをプッシュするには、まずイメージを用意する必要があります。 ローカル コンテナー イメージがまだない場合は、次の docker pull コマンドを実行して、既存のパブリック イメージをプルします。 この例では、Microsoft Container Registry から `hello-world` イメージをプルします。

```
docker pull mcr.microsoft.com/hello-world
```

イメージをレジストリにプッシュするには、レジストリのログイン サーバーの完全修飾名を使用して、そのイメージにタグを付けておく必要があります。 ログイン サーバ

ー名は、*<registry-name>.azurecr.io* (すべて小文字にする必要があります) という形式です (*mycontainerregistry.azurecr.io* など)。

docker tag コマンドを使用してイメージにタグ付けします。 `<login-server>` を ACR インスタンスのログイン サーバー名で置き換えます。

```
docker tag mcr.microsoft.com/hello-world <login-server>/hello-world:v1
```

例:

```
docker tag mcr.microsoft.com/hello-world
mycontainerregistry.azurecr.io/hello-world:v1
```

最後に、docker push を使用して、レジストリ インスタンスにイメージをプッシュします。 `<login-server>` をレジストリ インスタンスのログイン サーバー名で置き換えます。 この例では、**hello-world** レポジトリを作成します。これには、`hello-world:v1` イメージが含まれています。

```
docker push <login-server>/hello-world:v1
```

コンテナー レジストリにイメージをプッシュした後は、ローカルの Docker 環境から `hello-world:v1` イメージを削除します (この docker rmi コマンドは、Azure コンテナー リポジトリ内の **hello-world** リポジトリからイメージを削除しないことに注意してください)。

```
docker rmi <login-server>/hello-world:v1
```

コンテナー イメージの一覧表示

次の例は、レジストリ内のリポジトリを一覧表示します。

Azure CLI

```
az acr repository list --name <registry-name> --output table
```

出力:

```
Result
----------------
hello-world
```

次の例は、**hello-world** リポジトリのタグを一覧表示します。

Azure CLI

```azurecli
az acr repository show-tags --name <registry-name> --repository hello-world
--output table
```

出力:

```
Result
--------
v1
```

レジストリからイメージを実行する

ここで、docker run を使用して、コンテナー レジストリから `hello-world:v1` コンテナー イメージをプルして実行できます。

```
docker run <login-server>/hello-world:v1
```

出力例:

```
Unable to find image 'mycontainerregistry.azurecr.io/hello-world:v1' locally
v1: Pulling from hello-world
Digest:
sha256:662dd8e65ef7ccf13f417962c2f77567d3b132f12c95909de6c85ac3c326a345
Status: Downloaded newer image for mycontainerregistry.azurecr.io/hello-
world:v1

Hello from Docker!
This message shows that your installation appears to be working correctly.
```

```
[...]
```

リソースをクリーンアップする

必要がなくなったら、az group delete コマンドを使用して、リソース グループ、コンテナー レジストリ、そこに格納されているコンテナー イメージを削除できます。

Azure CLI

```
az group delete --name myResourceGroup
```

次のステップ

このクイック スタートでは、Azure CLI を使って Azure Container Registry を作成し、レジストリにコンテナー イメージをプッシュしてから、レジストリからイメージをプルして実行しました。 Azure Container Registry のチュートリアルに進んで、ACR についての理解を深めましょう。

Azure Container Registry のチュートリアル

Azure Container Registry タスクのチュートリアル

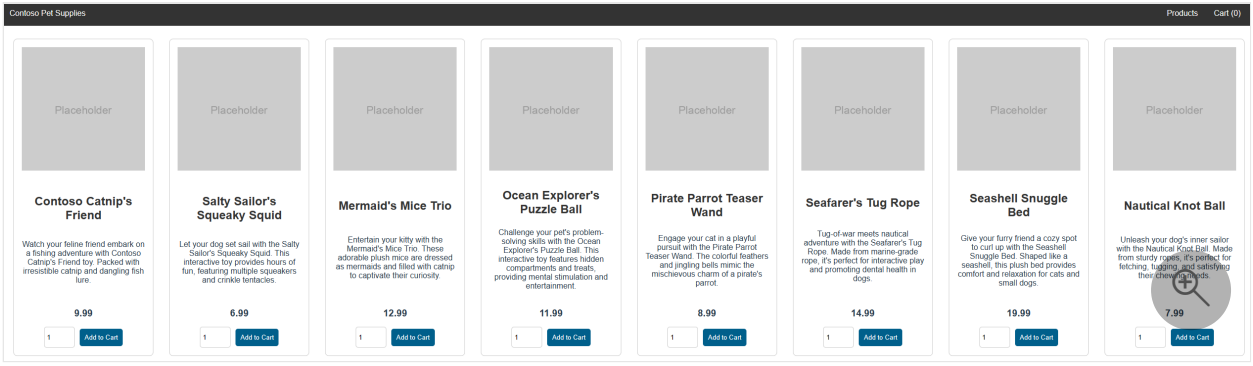
チュートリアル - Azure Kubernetes Service (AKS) 用のアプリケーションを準備する

[アーティクル] • 2024/03/10

7 つのパートのうちの 1 番目であるこのチュートリアルでは、複数コンテナー アプリケーションを Kubernetes で使用する準備をします。 Docker Compose などの既存の開発ツールを使用して、アプリケーションをローカルでビルドしてテストします。 以下の方法について説明します。

- ✓ GitHub からサンプル アプリケーション ソースを複製する。
- ✓ サンプル アプリケーション ソースからコンテナー イメージを作成します。
- ✓ ローカル Docker 環境でマルチコンテナー アプリケーションをテストします。

完了後、次のアプリケーションがローカル開発環境で実行されます。



後続のチュートリアルでは、コンテナー イメージを Azure Container Registry (ACR) にアップロードしてから、AKS クラスターにデプロイします。

開始する前に

このチュートリアルの前提として、コンテナー、コンテナー イメージ、`docker` コマンドなど、Docker のコア概念を基本的に理解している必要があります。 Docker の入門 に関するドキュメントでコンテナーの基礎についての入門情報を参照してください。

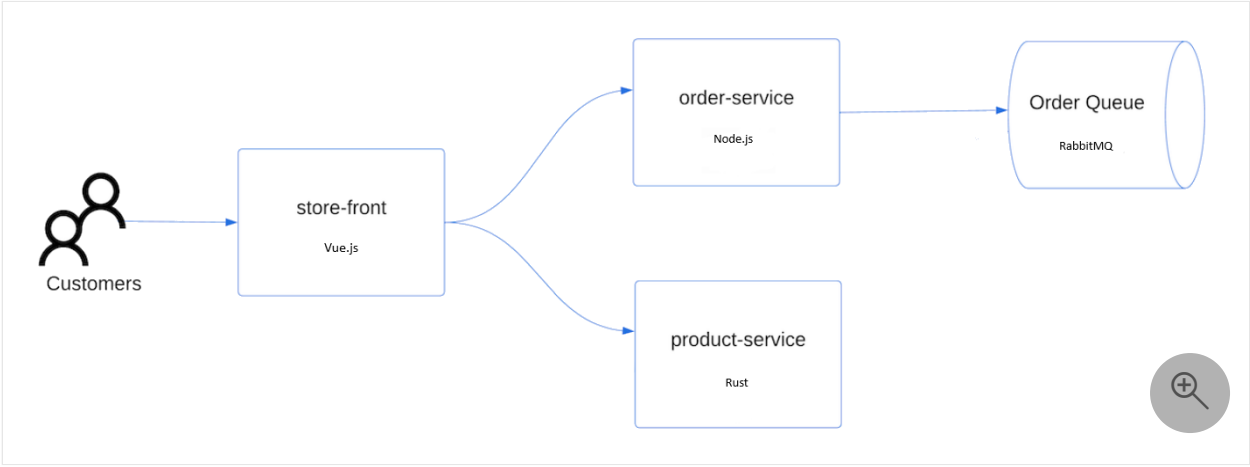
このチュートリアルを完了するには、Linux コンテナーを実行するローカルの Docker 開発環境が必要です。 Docker では、Mac、Windows、または Linux システム上に Docker を構成するパッケージが提供されています。

> ⓘ **注意**

Azure Cloud Shell には、これらのチュートリアルのすべてのステップを完了するために必要な Docker コンポーネントは含まれていません。 そのため、完全な Docker 開発環境の使用をお勧めします。

アプリケーションのコードを入手する

このチュートリアルで使用される サンプル アプリケーション は、次の Kubernetes デプロイとサービスを含む基本的なストア フロント アプリです：



- **ネットショップ**: 顧客が製品を見て注文するための Web アプリケーション。
- **製品サービス**: 製品情報が表示されます。
- **注文サービス**: 注文を行います。
- **Rabbit MQ**: 注文キューのメッセージ キュー。

Git

1. サンプル アプリケーションを開発環境に複製するには、git を使用します。

   コンソール

   ```
   git clone https://github.com/Azure-Samples/aks-store-demo.git
   ```

2. クローンされたディレクトリに移動します。

   コンソール

   ```
   cd aks-store-demo
   ```

Docker Compose ファイルを確認する

このチュートリアルで作成するサンプル アプリケーションでは、複製したリポジトリの *docker-compose-quickstart*YAML ファイルを使用します。

YAML

```yaml
version: "3.7"
services:
  rabbitmq:
    image: rabbitmq:3.11.17-management-alpine
    container_name: 'rabbitmq'
    restart: always
    environment:
      - "RABBITMQ_DEFAULT_USER=username"
      - "RABBITMQ_DEFAULT_PASS=password"
    ports:
      - 15672:15672
      - 5672:5672
    healthcheck:
      test: ["CMD", "rabbitmqctl", "status"]
      interval: 30s
      timeout: 10s
      retries: 5
    volumes:
      - ./rabbitmq_enabled_plugins:/etc/rabbitmq/enabled_plugins
    networks:
      - backend_services
  orderservice:
    build: src/order-service
    container_name: 'orderservice'
    restart: always
    ports:
      - 3000:3000
    healthcheck:
      test: ["CMD", "wget", "-O", "/dev/null", "-q",
"http://orderservice:3000/health"]
      interval: 30s
      timeout: 10s
      retries: 5
    environment:
      - ORDER_QUEUE_HOSTNAME=rabbitmq
      - ORDER_QUEUE_PORT=5672
      - ORDER_QUEUE_USERNAME=username
      - ORDER_QUEUE_PASSWORD=password
      - ORDER_QUEUE_NAME=orders
      - ORDER_QUEUE_RECONNECT_LIMIT=3
    networks:
      - backend_services
    depends_on:
      rabbitmq:
        condition: service_healthy
  productservice:
```

```
    build: src/product-service
    container_name: 'productservice'
    restart: always
    ports:
      - 3002:3002
    healthcheck:
      test: ["CMD", "wget", "-O", "/dev/null", "-q",
"http://productservice:3002/health"]
      interval: 30s
      timeout: 10s
      retries: 5
    networks:
      - backend_services
  storefront:
    build: src/store-front
    container_name: 'storefront'
    restart: always
    ports:
      - 8080:8080
    healthcheck:
      test: ["CMD", "wget", "-O", "/dev/null", "-q",
"http://storefront:80/health"]
      interval: 30s
      timeout: 10s
      retries: 5
    environment:
      - VUE_APP_PRODUCT_SERVICE_URL=http://productservice:3002/
      - VUE_APP_ORDER_SERVICE_URL=http://orderservice:3000/
    networks:
      - backend_services
    depends_on:
      - productservice
      - orderservice
networks:
  backend_services:
    driver: bridge
```

コンテナー イメージを作成してアプリケーションを実行する

Docker

Docker Compose を使用して、コンテナー イメージの構築とマルチコンテナー アプリケーションのデプロイを自動化できます。

Docker

1. コンテナー イメージを作成し、Redis イメージをダウンロードし、`docker compose` コマンドを使用してアプリケーションを起動します:

   コンソール

   ```
   docker compose -f docker-compose-quickstart.yml up -d
   ```

2. docker images コマンドを使用して、作成されたイメージを表示します。

   コンソール

   ```
   docker images
   ```

   次の要約された出力例は、作成されたイメージを示しています：

   出力

   ```
   REPOSITORY                          TAG                                 IMAGE
   ID
   aks-store-demo-productservice       latest
   2b66a7e91eca
   aks-store-demo-orderservice         latest
   54ad5de546f9
   aks-store-demo-storefront           latest
   d9e3ac46a225
   rabbitmq                            3.11.17-management-alpine
   79a570297657
   ...
   ```

3. docker ps コマンドを使用して、実行中のコンテナーを表示します。

   コンソール

   ```
   docker ps
   ```

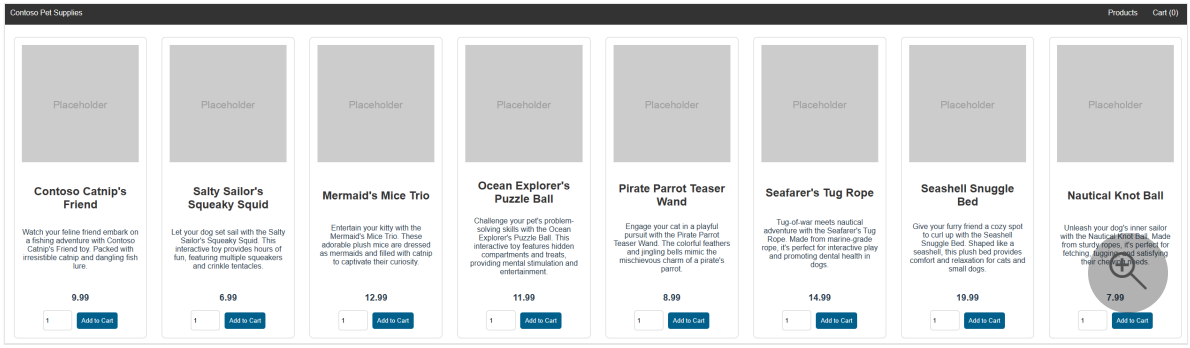
   次の要約された出力例は、実行中の 4 つのコンテナーを示しています：

   出力

   ```
   CONTAINER ID        IMAGE
   21574cb38c1f        aks-store-demo-productservice
   c30a5ed8d86a        aks-store-demo-orderservice
   d10e5244f237        aks-store-demo-storefront
   94e00b50b86a        rabbitmq:3.11.17-management-alpine
   ```

ローカルでアプリケーションをテストする

実行中のアプリケーションを表示するには、ローカルの Web ブラウザーで `http://localhost:8080` に移動します。 次の例で示すように、サンプル アプリケーションが読み込まれます。



このページでは、製品を表示し、カートに追加して注文することができます。

リソースをクリーンアップする

アプリケーションの機能を検証したので、実行中のコンテナーを停止および削除できます。 **コンテナー イメージ を削除しないでください**。次のチュートリアルで使用します。

- docker-compose down コマンドを使用して、コンテナー インスタンスとリソースを停止して削除します。

  コンソール

  ```
  docker compose down
  ```

次のステップ

Azure CLI

このチュートリアルでは、サンプル アプリケーションを作成し、アプリケーションのコンテナー イメージを作成してから、アプリケーションをテストしました。 以下の方法を学習しました。

- ✓ GitHub からサンプル アプリケーション ソースを複製する。
- ✓ サンプル アプリケーション ソースからコンテナー イメージを作成します。
- ✓ ローカル Docker 環境でマルチコンテナー アプリケーションをテストします。

次のチュートリアルでは、ACR にコンテナー イメージを保存する方法について説明します。

Azure Container Registry にイメージをプッシュする

Azure AI サービスのセキュリティ

[アーティクル] • 2024/01/20

すべてのアプリケーションにおいて、開発のときはセキュリティを最優先に考える必要があり、人工知能対応のアプリケーションが拡大すると、セキュリティはさらに重要になります。 この記事では、Azure AI サービスで使用できるさまざまなセキュリティ機能について説明します。 各機能は特定の責任に対処するため、同じワークフローで複数の機能を使用できます。

Azure サービスのセキュリティに関する推奨事項の包括的な一覧については、Azure AI サービスのセキュリティ ベースラインに関する記事をご覧ください。

セキュリティ機能

テーブルを展開する

機能	説明
トランスポート層セキュリティ (TLS)	HTTP 経由で公開されるすべての Azure AI サービス エンドポイントでは、TLS 1.2 プロトコルが適用されます。 セキュリティ プロトコルが適用されている場合、Azure AI サービス エンドポイントを呼び出そうとするコンシューマーは、次のガイドラインに従う必要があります。 • クライアント オペレーティング システム (OS) では、TLS 1.2 がサポートされている必要があります。 • HTTP の呼び出しに使用される言語 (およびプラットフォーム) では、要求の一部として TLS 1.2 を指定する必要があります 言語とプラットフォームに応じて、TLS の指定は暗黙的または明示的に行われます。 • .NET ユーザーの場合は、トランスポート層セキュリティに関するベスト プラクティスを検討してください
認証オプション	認証とは、ユーザーの ID を検証することです。 それに対し、認可とは、特定の ID に対してリソースへのアクセス権と特権を指定することです。 ID はプリンシパル に関する情報のコレクションであり、プリンシパルは個々のユーザーまたはサービスのいずれかです。 既定では、提供されているサブスクリプション キーを使って、Azure AI サービスへの呼び出しの認証を行います。これは最も簡単な方法ですが、最も安全ではありません。 最も安全な認証方法は、Microsoft Entra ID のマネージド ロールを使うことです。 この認証オプションとその他の認証オプションについては、「Azure AI サービスに対する要求の認証」を参照してください。
キーのローテ	各 Azure AI サービス リソースには、シークレットのローテーションを有効にする 2 つの API キーがあります。 これは、サービスにアクセスできるキーを定期的に変更し、キーが漏洩した場合でもサービスのプライバシーを保護できるセキュリティ上の

機能	説明
ーション	予防措置です。 これとその他の認証オプションについては、キーのローテーションに関するページを参照してください。
環境変数	環境変数は名前と値のペアであり、特定の開発環境内に格納されます。 コードで値をハードコーディングする代わりにこの方法を使うと、資格情報をいっそう安全に格納できます。 ただし、環境が侵害された場合、環境変数も侵害されるため、これは最も安全な方法ではありません。 コードで環境変数を使う方法については、環境変数のガイドに関する記事をご覧ください。
カスタマー マネージド キー (CMK)	この機能は、顧客の保存データを (48 時間より長く) 格納するサービスを対象としています。 このデータは Azure サーバーで既に二重に暗号化されていますが、ユーザーは自分で管理するキーを使ってさらに暗号化レイヤーを追加することで、セキュリティを強化できます。 サービスを Azure Key Vault にリンクし、そこでデータ暗号化キーを管理できます。 CMK を使用できるのは一部のサービスのみです。カスタマー マネージド キーに関するページでサービスを探してください。
仮想ネットワーク	仮想ネットワークを使うと、リソースに対する API 呼び出しを行うことができるエンドポイントを指定できます。 Azure サービスは、ネットワーク外のデバイスからの API 呼び出しを拒否します。 許可されるネットワークの式ベースの定義を設定することも、許可するエンドポイントの完全な一覧を定義することもできます。 これはセキュリティのもう 1 つのレイヤーであり、他と組み合わせて使用できます。
データ損失の防止	データ損失防止機能を使うと、管理者は、Azure リソースが入力として受け取ることのできる URI の種類を決定できます (入力として URI を受け取る API 呼び出しの場合)。 これを行うことで、会社の機密データが流出する可能性を防ぐことができます。会社が URL パラメーターに機密情報 (顧客のプライベート データなど) を格納している場合、社内の不適切なアクターが機密 URL を Azure サービスに送信し、そのデータを社外に公開する可能性があります。 データ損失防止を使うと、到着した特定の URI フォームを拒否するようにサービスを構成できます。
カスタマー ロックボックス	カスタマー ロックボックス機能は、お客様がデータ アクセス要求をレビューして承認または拒否するためのインターフェイスを提供します。 これは、Microsoft のエンジニアがサポート リクエストの際に顧客データにアクセスする必要がある場合に使用されます。 カスタマー ロックボックス要求の開始、追跡、後のレビューと監査のための保存の方法に関する詳細については、カスタマー ロックボックス ガイドを参照してください。 カスタマー ロックボックスは、次のサービスで使用できます。 • Azure OpenAI • Translator • 会話言語理解 • カスタム テキスト分類 • カスタム固有表現認識 • オーケストレーション ワークフロー

機能	説明
BYOS (ストレージ持ち込み)	Speech サービスでは、現在、カスタマー ロックボックスはサポートされていません。 ただし、BYOS (ストレージ持ち込み) を使って、サービス固有のデータが独自のストレージ リソースに格納されるようにすることができます。 BYOS を使うと、カスタマー ロックボックスと似たデータ コントロールを実現できます。 Azure Cognitive Service for Speech サービスのデータは、Azure Cognitive Service for Speech リソースが作成された Azure リージョンで保持されて処理されることに注意してください。 これは、保存データと転送中のデータに適用されます。 Custom Speech や Custom Voice などのカスタマイズ機能では、お客様のすべてのデータは、Azure Cognitive Service for Speech サービス リソースと BYOS リソース (使っている場合) が存在しているのと同じリージョンで転送、格納、処理されます。 Azure Cognitive Service for Speech で BYOS を使うには、保存データの音声暗号化に関するガイドに従ってください。 音声モデルを改善するため、Microsoft がお客様のデータを使用することはありません。 また、エンドポイントのログが無効になっていて、カスタマイズが使われていない場合、お客様のデータが Azure Cognitive Service for Speech によって格納されることはありません。

次のステップ

- Azure AI サービスについて調べて、使用を開始するサービスを選択します。

Azure AI サービスに対する要求の認証

[アーティクル] • 2023/10/30

Azure AI サービスに対する各要求には、認証ヘッダーが含まれている必要があります。このヘッダーを使用して、リソース キーまたは認証トークンを渡します。これは、サービスまたはサービスのグループについてお客様のサブスクリプションを検証するために使用されます。 この記事では、要求を認証するための 3 つの方法と、そのそれぞれの要件について学習します。

- 単一サービス または マルチ サービス のリソース キーで認証
- トークンによる認証
- Microsoft Entra ID を使用して認証する

前提条件

要求を行うには、Azure アカウントと Azure AI サービス サブスクリプションが必要になります。 既にアカウントをお持ちの場合は、次のセクションまでスキップして進んでください。 アカウントをお持ちでない場合は、数分で設定を行えるガイドをご覧ください。「マルチサービス リソースの作成」を参照してください。

アカウントの作成 後に、Azure portal からリソース キーを取得できます。

認証ヘッダー

Azure AI サービスで使用できる認証ヘッダーについて簡単に確認しましょう。

Header	説明
Ocp-Apim-Subscription-Key	特定のサービスのリソース キーまたはマルチサービスのリソース キーを使用して認証するには、このヘッダーを使用します。
Ocp-Apim-Subscription-Region	このヘッダーは、Translator サービスと共にマルチサービスのリソース キーを使用する場合にのみ必要です。 このヘッダーを使用して、リソース リージョンを指定します。
認可	アクセス トークンを使用する場合、このヘッダーを使用します。 トークンの交換を実行する手順については、以降のセクションで詳しく説明されています。 値は `Bearer <TOKEN>` 形式で指定します。

単一サービスのリソース キーを使用した認証

1 つ目の方法では、Translator などの特定のサービスに対してリソース キーを使用して要求を認証します。 お客様が作成したそれぞれのリソースについて、Azure portal でキーを取得できます。 リソース キーを使用して要求を認証するには、それを `Ocp-Apim-Subscription-Key` ヘッダーとして渡す必要があります。

以下のサンプル要求は、`Ocp-Apim-Subscription-Key` ヘッダーの使用方法を示しています。 このサンプルを使用する際は有効なリソース キーを含める必要があることに注意してください。

これは、Translator サービスの呼び出しの例です。

cURL

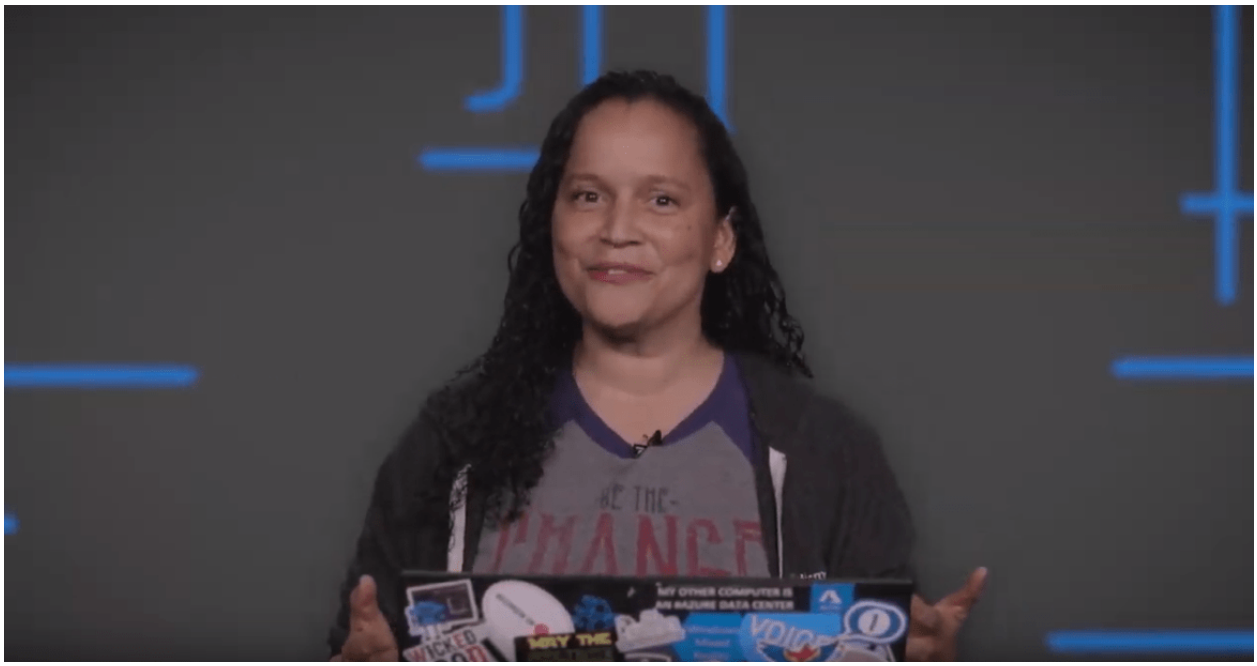
```
curl -X POST 'https://api.cognitive.microsofttranslator.com/translate?api-version=3.0&from=en&to=de' \
-H 'Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY' \
-H 'Content-Type: application/json' \
--data-raw '[{ "text": "How much for the cup of coffee?" }]' | json_pp
```

次のビデオでは、Azure AI サービス キーの使用を示しています。

マルチサービス リソース キーを使用した認証

マルチサービス リソース キーを使用して要求を認証できます。 主な違いは、マルチサービス リソース キーが特定のサービスに関連付けられておらず、単一のキーを使用して複数の Azure AI サービスに対する要求を認証できることです。 リージョン別の提供状況、サポートされている機能、および価格については、「Azure AI サービスの価格」を参照してください。

リソース キーは、各要求内で `Ocp-Apim-Subscription-Key` ヘッダーとして指定されます。



サポートされているリージョン

マルチサービスのリソース キーを使用して `api.cognitive.microsoft.com` に対する要求を実行するときは、URL にリージョンを含める必要があります。 (例: `westus.api.cognitive.microsoft.com`)。

Azure AI 翻訳 でマルチサービス リソース キーを使用するとき、`Ocp-Apim-Subscription-Region` ヘッダーでリソース リージョンを指定する必要があります。

マルチサービス認証は、以下のリージョンでサポートされています。

- `australiaeast`
- `brazilsouth`
- `canadacentral`
- `centralindia`
- `eastasia`
- `eastus`
- `japaneast`
- `northeurope`
- `southcentralus`
- `southeastasia`
- `uksouth`
- `westcentralus`
- `westeurope`
- `westus`
- `westus2`

- `francecentral`
- `koreacentral`
- `northcentralus`
- `southafricanorth`
- `uaenorth`
- `switzerlandnorth`

サンプルの要求

これは、Translator サービスの呼び出しの例です。

cURL

```
curl -X POST 'https://api.cognitive.microsofttranslator.com/translate?api-version=3.0&from=en&to=de' \
-H 'Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY' \
-H 'Ocp-Apim-Subscription-Region: YOUR_SUBSCRIPTION_REGION' \
-H 'Content-Type: application/json' \
--data-raw '[{ "text": "How much for the cup of coffee?" }]' | json_pp
```

アクセス トークンを使用して認証する

一部の Azure AI サービスはアクセス トークンを受け入れ、また場合によってはアクセス トークンは必須です。 現在、以下のサービスでアクセス トークンがサポートされています。

- Text Translation API
- 音声サービス: Speech to text API
- 音声サービス: Text to speech API

> ⓘ **注意**
>
> QnA Maker でも Authorization ヘッダーが使用されますが、エンドポイント キーが必要です。 詳細については、**QnA Maker でナレッジ ベースから回答を取得する**方法に関するページを参照してください。

> ⚠ **警告**

アクセス トークンをサポートするサービスは時間の経過と共に変わる可能性があります。この認証方法を使用する前に、サービスの API リファレンスを確認してください。

単一サービスのリソース キーとマルチサービスのリソース キーは、どちらも認証トークンと交換できます。 認証トークンは 10 分間有効です。 これらは JSON Web Token (JWT) 形式で格納され、JWT ライブラリ を使用してプログラムで照会することができます。

アクセス トークンは、`Authorization` ヘッダーとして要求に組み込まれます。 指定されるトークンの値の前には `Bearer` が付いている必要があります (例: `Bearer YOUR_AUTH_TOKEN`)。

サンプルの要求

リソース キーをアクセス トークンと交換するには、以下の URL を使用します: `https://YOUR-REGION.api.cognitive.microsoft.com/sts/v1.0/issueToken`。

cURL

```
curl -v -X POST \
"https://YOUR-REGION.api.cognitive.microsoft.com/sts/v1.0/issueToken" \
-H "Content-type: application/x-www-form-urlencoded" \
-H "Content-length: 0" \
-H "Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY"
```

以下のマルチサービスのリージョンで、トークンの交換がサポートされています。

- `australiaeast`
- `brazilsouth`
- `canadacentral`
- `centralindia`
- `eastasia`
- `eastus`
- `japaneast`
- `northeurope`
- `southcentralus`
- `southeastasia`
- `uksouth`
- `westcentralus`
- `westeurope`

- `westus`
- `westus2`

アクセス トークンを取得したら、各要求内でそれを `Authorization` ヘッダーとして渡す必要があります。 これは、Translator サービスの呼び出しの例です。

cURL

```
curl -X POST 'https://api.cognitive.microsofttranslator.com/translate?api-version=3.0&from=en&to=de' \
-H 'Authorization: Bearer YOUR_AUTH_TOKEN' \
-H 'Content-Type: application/json' \
--data-raw '[{ "text": "How much for the cup of coffee?" }]' | json_pp
```

Microsoft Entra ID を使用して認証する

> **ⓘ 重要**
>
> Microsoft Entra 認証は常に、Azure リソースのカスタム サブドメイン名と共に使用される必要があります。 **リージョン エンドポイント**では、Microsoft Entra 認証がサポートされていません。

前のセクションでは、Azure AI サービスに対して単一サービスまたはマルチサービスのサブスクリプション キーを使用して認証する方法を説明しました。 これらのキーを使用すると、開発を迅速かつ簡単に開始できますが、Azure ロールベースのアクセス制御 (Azure RBAC) を必要とするより複雑なシナリオでは不十分です。 Microsoft Entra ID を使用して認証を行うために何が必要なのかを確認しましょう。

以降のセクションでは、Azure Cloud Shell 環境または Azure CLI を使用してサブドメインを作成し、ロールを割り当てて、Azure AI サービスを呼び出すベアラー トークンを取得します。 問題が発生した場合は、各セクションに、Azure Cloud Shell/Azure CLI の各コマンドで使用可能なすべてのオプションへのリンクが提供されています。

> **ⓘ 重要**
>
> 組織で Microsoft Entra ID を介した認証を行っている場合は、組織内のユーザーが常に Microsoft Entra ID を使う必要があるように、**ローカル認証 (キーによる認証) を無効にする**ことをお勧めします。

カスタム サブドメインを使用してリソースを作成する

最初の手順で、カスタム サブドメインを作成します。 カスタム サブドメイン名のない既存の Azure AI サービスリソースを使用する場合は、「Azure AI サービス カスタム サブドメイン」の手順に従って、リソースのカスタム サブドメインを有効にします。

1. まず、Azure Cloud Shell を開きます。 サブスクリプションを選択します。

   PowerShell

   ```
   Set-AzContext -SubscriptionName <SubscriptionName>
   ```

2. 次に、カスタム サブドメインを使用して Azure AI サービス リソースを作成します。 サブドメイン名は、グローバルに一意である必要があり、"."、"!"、"," などの特殊文字を含めることはできません。

   PowerShell

   ```
   $account = New-AzCognitiveServicesAccount -ResourceGroupName
   <RESOURCE_GROUP_NAME> -name <ACCOUNT_NAME> -Type <ACCOUNT_TYPE> -
   SkuName <SUBSCRIPTION_TYPE> -Location <REGION> -CustomSubdomainName
   <UNIQUE_SUBDOMAIN>
   ```

3. 成功すると、**エンドポイント**にリソースに固有のサブドメイン名が表示されます。

サービス プリンシパルにロールを割り当てる

これで、カスタム サブドメインがリソースに関連付けられたので、ロールをサービス プリンシパルに割り当てる必要があります。

> ⓘ **注意**
>
> Azure ロールの割り当ての反映には最大で 5 分かかる場合があることに留意してください。

1. まず、Microsoft Entra アプリケーションを登録しましょう。

   PowerShell

   ```
   $SecureStringPassword = ConvertTo-SecureString -String <YOUR_PASSWORD>
   -AsPlainText -Force

   $app = New-AzureADApplication -DisplayName <APP_DISPLAY_NAME> -
   IdentifierUris <APP_URIS> -PasswordCredentials $SecureStringPassword
   ```

次の手順では、**ApplicationId** が必要になります。

2. 次に、Microsoft Entra アプリケーションのサービス プリンシパルを作成する必要があります。

```
PowerShell

New-AzADServicePrincipal -ApplicationId <APPLICATION_ID>
```

> ⓘ **注意**
>
> Azure portal でアプリケーションを登録したら、この手順は完了です。

3. 最後の手順では、(リソースにスコープが設定された) サービス プリンシパルに "Cognitive Services ユーザー" ロールを割り当てます。 ロールを割り当てて、このリソースにサービス プリンシパル アクセス権を付与します。 同じサービス プリンシパル アクセスをサブスクリプション内の複数のリソースに対して許可できます。

> ⓘ **注意**
>
> アプリケーションの ObjectId ではなく、サービス プリンシパルの ObjectId が使用されます。 ACCOUNT_ID は、作成した Azure AI サービス アカウントの Azure リソース ID になります。 Azure portal でリソースの "プロパティ" から Azure リソース ID を検索できます。

```
Azure CLI

New-AzRoleAssignment -ObjectId <SERVICE_PRINCIPAL_OBJECTID> -Scope
<ACCOUNT_ID> -RoleDefinitionName "Cognitive Services User"
```

要求のサンプル

このサンプルでは、サービス プリンシパルの認証にパスワードが使用されています。 次に、指定されたトークンを使用して Computer Vision API を呼び出します。

1. **TenantId** を取得します。

```
PowerShell

$context=Get-AzContext
```

```
$context.Tenant.Id
```

2. トークンを取得します。

> **注意**
>
> Azure Cloud Shell を使用している場合、`SecureClientSecret` クラスは使用できません。

PowerShell

PowerShell

```
$authContext = New-Object
"Microsoft.IdentityModel.Clients.ActiveDirectory.AuthenticationCont
ext" -ArgumentList "https://login.windows.net/<TENANT_ID>"
$secureSecretObject = New-Object
"Microsoft.IdentityModel.Clients.ActiveDirectory.SecureClientSecret
" -ArgumentList $SecureStringPassword
$clientCredential = New-Object
"Microsoft.IdentityModel.Clients.ActiveDirectory.ClientCredential"
-ArgumentList $app.ApplicationId, $secureSecretObject
$token=$authContext.AcquireTokenAsync("https://cognitiveservices.az
ure.com/", $clientCredential).Result
$token
```

3. Computer Vision API を呼び出します。

PowerShell

```
$url = $account.Endpoint+"vision/v1.0/models"
$result = Invoke-RestMethod -Uri $url  -Method Get -Headers
@{"Authorization"=$token.CreateAuthorizationHeader()} -Verbose
$result | ConvertTo-Json
```

または、証明書を使用してサービス プリンシパルを認証することもできます。 サービス プリンシパルの他に、別の Microsoft Entra アプリケーションから委任されたアクセス許可を持つことで、ユーザー プリンシパルもサポートされます。 この場合、パスワードまたは証明書の代わりに、ユーザーはトークンを取得するときに 2 要素認証が求められます。

マネージド ID へのアクセスを認証する

Azure AI サービスでは、Azure リソースのマネージド ID を使用した Microsoft Entra 認証がサポートされています。 Azure リソースのマネージド ID では、Azure 仮想マシン (VM)、関数アプリ、仮想マシン スケール セットなどのサービスで実行されているアプリケーションから Azure AI サービス リソースへのアクセスを、Microsoft Entra 資格情報を使用して承認することができます。 Azure リソースのマネージド ID と Microsoft Entra 認証を併用すると、クラウドで実行されるアプリケーションに資格情報を保存することを避けることができます。

VM 上のマネージド ID を有効にする

Azure リソースのマネージド ID を使用して、ご利用の VM から Azure AI サービス リソースへのアクセスを承認するには、VM 上で Azure リソースのマネージド ID を有効にする必要があります。 Azure リソースのマネージド ID を有効にする方法については、次を参照してください。

- Azure Portal
- Azure PowerShell
- Azure CLI
- Azure Resource Manager テンプレート
- Azure Resource Manager クライアント ライブラリ

マネージド ID の詳細については、Azure リソースのマネージド ID に関するページを参照してください。

Azure Key Vault を使用して資格情報に安全にアクセスする

Azure Key Vault を使用して、Azure AI サービス アプリケーションを安全に開発できます。 Key Vault を使用すると、認証資格情報をクラウドに格納でき、アプリケーションにセキュリティ情報を格納しないため、シークレットが誤って漏洩する可能性が低くなります。

認証は Microsoft Entra ID によって行われます。 認可は、Azure ロールベースのアクセス制御 (Azure RBAC) または Key Vault のアクセス ポリシーを使用して行うことができます。 Azure RBAC は、コンテナーの管理と、コンテナーに格納されているデータへのアクセスの両方に使用できます。一方、Key Vault のアクセス ポリシーは、コンテナーに格納されているデータにアクセスしようとするときにのみ使用できます。

関連項目

- Azure AI サービスとは
- Azure AI サービスの価格
- カスタム サブドメイン

Azure AI サービスでローカル認証を無効にする

[アーティクル] • 2023/12/21

Azure AI サービスでは、すべてのリソースに対して Microsoft Entra 認証がサポートされています。 これにより、組織はローカル認証方法を無効にし、Microsoft Entra 認証を適用することができます。 この機能は、ID とリソース資格情報の集中制御と管理が必要な場合にシームレスな統合が可能になります。

ローカル認証を無効にするには、Azure ポリシー Cognitive Services アカウントでローカル認証方法を無効にする必要があります。 サブスクリプション レベルまたはリソース グループ レベルで設定して、サービスのグループに対してポリシーを適用できます。

Bicep または ARM テンプレートを使ってアカウントを作成している場合は、プロパティ `disableLocalAuth` を `true` に設定してローカル認証を無効にすることができます。 詳細については、「Microsoft.CognitiveServices アカウント」の「Bicep」、「ARM テンプレート」、「Terraform」を参照してください

ローカル認証を無効にしても、すぐに効果が現れるわけではありません。 このサービスによって将来の認証要求がブロックされるようになるまで数分かかります。

PowerShell を使用して、ローカル認証ポリシーが現在有効になっているかどうかを確認できます。 最初に `Connect-AzAccount` コマンドを使用してサインインします。 次に、コマンドレット **Get-AzCognitiveServicesAccount** を使用してリソースを取得し、`DisableLocalAuth` プロパティを確認します。 `true` の値は、ローカル認証が無効になっていることを示します。

ローカル認証を再び有効にする

ローカル認証を有効にするには、パラメーター `-DisableLocalAuth false` を指定して PowerShell コマンドレット **Set-AzCognitiveServicesAccount** を実行します。 このサービスによってローカル認証要求を許可する変更が受け入れられるまで数分かかります。

次のステップ

- Azure AI サービスに対する要求の認証

Azure AI サービスでキーをローテーションする

[アーティクル] • 2024/01/29

各 Azure AI サービス リソースには、シークレットのローテーションを有効にする 2 つの API キーがあります。 これは、サービスにアクセスできるキーを定期的に変更し、キーが漏洩した場合でもリソースのプライバシーを保護できるセキュリティ上の予防措置です。

キーをローテーションする方法

次の手順を実行してキーをローテーションできます。

1. 運用環境で両方のキーを使用している場合は、1 つのキーのみが使用されるようにコードを変更します。 このガイドでは、それがキー 1 であると仮定します。

   キーが再生成されると、そのキーの古いバージョンはすぐに機能しなくなるため、これは必要な手順です。 これにより、古いキーを使っているクライアントで `401 access denied` エラーが発生します。

2. 使用されているのがキー 1 のみになったら、キー 2 を再生成できます。 Azure portal でリソースのページに移動し、**[キーとエンドポイント]** タブを選択し、ページの上部にある **[キー 2 の再生成]** ボタンを選択します。

3. 次に、新しく生成されたキー 2 を使用するようにコードを更新します。

   先に進む前に、キーのユーザーがキー 1 からキー 2 への切り替えを正常に完了したことを確認するためのログまたは可用性を用意しておくと便利です。

4. これで、同じプロセスを使ってキー 1 を再生成できます。

5. 最後に、新しいキー 1 を使用するようにコードを更新します。

関連項目

- Azure AI サービスとは
- Azure AI サービスのセキュリティ機能

Azure AI サービスで環境変数を使用する

[アーティクル] • 2024/01/20

このガイドでは、アプリケーションをテストするときに、環境変数を設定および取得して、Azure AI サービス サブスクリプションの資格情報をより安全な方法で処理する方法について説明します。

環境変数を設定する

環境変数を設定するには、次のいずれかのコマンドを使用します。
`ENVIRONMENT_VARIABLE_KEY` は名前付きのキーであり、`value` は環境変数に格納される値です。

コマンド ライン

次のコマンドを使用して、入力値を指定して永続化された環境変数を作成して割り当てます。

CMD

```
:: Assigns the env var to the value
setx ENVIRONMENT_VARIABLE_KEY "value"
```

コマンド プロンプトの新しいインスタンスで、次のコマンドを使用して環境変数を読み取ります。

CMD

```
:: Prints the env var value
echo %ENVIRONMENT_VARIABLE_KEY%
```

ヒント

環境変数を設定した後、統合開発環境 (IDE) を再起動して、新しく追加した環境変数を使用できることを確認します。

環境変数を取得する

コード内で環境変数を使用するには、メモリに読み込む必要があります。 使用している言語に応じて、次のいずれかのコード スニペットを使用します。 これらのコード スニペットでは、`ENVIRONMENT_VARIABLE_KEY` で指定された環境変数を取得し、その値を `value` という名前のプログラム変数に代入する方法が示されています。

C#

詳細については、「Environment.GetEnvironmentVariable 」を参照してください。

C#

```
using static System.Environment;

class Program
{
    static void Main()
    {
        // Get the named env var, and assign it to the value variable
        var value =
            GetEnvironmentVariable(
                "ENVIRONMENT_VARIABLE_KEY");
    }
}
```

次の手順

- Azure AI サービスについて調べて、使用を開始するサービスを選択します。

暗号化用のカスタマー マネージド キー

[アーティクル] • 2023/11/18

Azure AI は、複数の Azure サービスの上に構築されています。 データは Microsoft が提供する暗号化キーを使用して安全に格納されますが、独自の (カスタマー マネージド) キーを提供することでセキュリティを強化できます。 提供されたキーは、Azure Key Vault を使用して安全に保存されます。

前提条件

- Azure サブスクリプション。
- Azure Key Vault インスタンス。 キー コンテナーには、サービスの暗号化に使用されるキーが格納されます。
    - キー コンテナー インスタンスでは、論理的な削除と消去保護を有効にする必要があります。
    - カスタマー マネージド キーによって保護されるサービスのマネージド ID には、キー コンテナーに次のアクセス許可が必要です。
        - キーを折り返す
        - キーの折り返しを解除
        - get

      たとえば、Azure Cosmos DB のマネージド ID は、キー コンテナーに対してこれらのアクセス許可が必要です。

メタデータの格納方法

次のサービスは、Azure AI リソースとプロジェクトのメタデータを格納するために Azure AI によって使用されます:

サービス	これは何に使用されますか？	例
Azure Cosmos DB	Azure AI プロジェクトとツールのメタデータを格納する	フロー作成タイムスタンプ、デプロイ タグ、評価メトリック
Azure AI Search	AI Studio コンテンツのクエリに使用されるインデックスを格納します。	モデル デプロイ名に基づくインデックス
Azure Storage アカウント	Azure AI プロジェクトとツールによって作成された成果物を格納する	微調整されたモデル

上記のサービスはすべて、Azure AI リソースを最初に作成したときと同じキーを利用して暗号化され、Azure AI リソースとそれに関連付けられるプロジェクト セットごとに 1 回、お使いのサブスクリプションで管理対象リソース グループに設定されます。 Azure AI リソースとプロジェクトは、マネージド ID を使用してデータの読み取りと書き込みを行います。 マネージド ID には、データ リソースに対するロールの割り当て (Azure ロールベースのアクセス制御) を使用して、リソースへのアクセス権が付与されます。 ユーザーが指定する暗号化キーが、Microsoft が管理するリソースに格納されるデータを暗号化するために使用されます。 また、実行時に作成される Azure AI Search のインデックスを作成するためにも使用されます。

カスタマー マネージド キー

カスタマー マネージド キーを使用しない場合、Microsoft は Microsoft 所有の Azure サブスクリプションでこれらのリソースを作成および管理し、Microsoft マネージド キーを使用してデータを暗号化します。

カスタマー マネージド キーを使用する場合、これらのリソースはお使いの *Azure* サブスクリプションに保存され、指定のキーで暗号化されます。 これらのリソースはお客様のサブスクリプションに存在しますが、Microsoft によって管理されます。 Azure AI リソースを作成するときに、自動的に作成および構成されます。

> **ⓘ 重要**
>
> カスタマー マネージド キーを使用する場合、これらのリソースはサブスクリプション内にあるため、サブスクリプションのコストが高くなります。 コストを見積もるには、**Azure 料金計算ツール** を使用してください。

これらの Microsoft が管理するリソースは、サブスクリプションに作成される新しい Azure リソース グループに配置されます。 このグループは、プロジェクトのリソース グループに追加されます。 このリソース グループには、キーが使用される Microsoft マネージド リソースが含まれます。 リソース グループには、`<Azure AI resource group name><GUID>` 形式を使用して名前が付けられます。 この管理対象リソース グループ内のリソースの名前規則を変更することはできません。

> **ヒント**
>
> - Azure Cosmos DB の**要求ユニット**は、必要に応じて自動的にスケーリングされます。
> - AI リソースでプライベート エンドポイントを使用している場合、このリソース グループには Microsoft が管理する Azure Virtual Network も含まれます。

この VNet は、マネージド サービスとプロジェクト間の通信をセキュリティで保護するために使用されます。 Microsoft により管理されるリソースで使用するための独自の VNet を指定することはできません。 また、仮想ネットワークを変更することはできません。 たとえば、使用される IP アドレスの範囲を変更することはできません。

> **ⓘ 重要**
>
> サブスクリプションにこれらのサービス用の十分なクォータがない場合、エラーが発生します。

> **⚠ 警告**
>
> この Azure Cosmos DB インスタンス、またはこのグループに自動的に作成されたリソースが含まれる管理対象リソース グループを削除しないでください。 このリソース グループまたはその中の Microsoft が管理するサービスを削除する必要がある場合は、それを使用する Azure AI リソースを削除してください。 関連付けられている AI リソースが削除されると、リソース グループのリソースは削除されます。

Azure AI サービス用に Azure Key Vault でカスタマー マネージド キーを有効にするプロセスは、製品ごとに異なります。 サービス固有の手順については、以下のリンクを使用してください。

- 保存データの Azure OpenAI 暗号化
- Custom Vision による保存データの暗号化
- Face サービスによる保存データの暗号化
- 保存データのドキュメント インテリジェンス暗号化
- Translator による保存データの暗号化
- 言語サービスによる保存データの暗号化
- 音声による保存データの暗号化
- Content Moderator による保存データの暗号化
- Personalizer による保存データの暗号化

コンピューティング データの格納方法

Azure AI では、モデルを微調整したり、フローを構築したりするときに、コンピューティング インスタンスとサーバーレス コンピューティングにコンピューティング リソー

スを使用します。 次の表では、コンピューティング オプションと、それぞれでデータを暗号化する方法について説明します。

Compute	暗号化
コンピューティング インスタンス	ローカル スクラッチ ディスクは暗号化されます。
サーバーレス コンピューティング	OS ディスクは Microsoft マネージド キーを使用して Azure Storage で暗号化されます。 一時ディスクは暗号化されます。

コンピューティング インスタンス コンピューティング インスタンスの OS ディスクは、Microsoft マネージド ストレージ アカウント内の Microsoft によって管理されるキーを使用して暗号化されます。 `hbi_workspace` パラメーターを `TRUE` に設定してプロジェクトを作成した場合、コンピューティング インスタンスのローカル一時ディスクは Microsoft マネージド キーで暗号化されます。 カスタマー マネージド キーによる暗号化は、OS と一時ディスクについてはサポートされていません。

サーバーレス コンピューティング: Azure Storage に格納されている各コンピューティング ノードの OS ディスクは、Microsoft によって管理されるキーを使用して暗号化されます。 このコンピューティング先は一時的なものであり、キューに入れられたジョブがない場合、通常はクラスターがスケールダウンされます。 基になる仮想マシンのプロビジョニングは解除され、OS ディスクは削除されます。 OS ディスクでは Azure Disk Encryption はサポートされません。

各仮想マシンにも、OS 操作用にローカルな一時ディスクがあります。 必要に応じて、ディスクを使用してトレーニング データをステージできます。 この環境は有効期間が短く (ジョブ中のみ)、暗号化のサポートはシステムマネージド キーのみに制限されています。

制限事項

- Azure AI リソースで構成されているとき、暗号化キーは、Azure AI リソースから Azure AI Services や Azure Storage などの依存リソースに渡されることはありません。 暗号化は、各リソースで明確に設定する必要があります。
- 暗号化用のカスタマー マネージド キーは、同じ Azure Key Vault インスタンス内のキーにのみ更新できます。
- デプロイ後、Microsoft マネージド キーからカスタマー マネージド キーに、またはその逆に切り替えることはできません。
- サブスクリプション内の Microsoft が管理する Azure リソース グループに作成されたリソースは、ユーザーが変更したり、既存のリソースとして作成時に提供したりすることはできません。

- プロジェクトも削除するのでなければ、カスタマー マネージド キーに使用される Microsoft 管理対象リソースを削除することはできません。

次のステップ

- Speech と Content Moderator には、Azure AI サービスのカスタマー マネージド キー要求フォーム が引き続き必要になります。
- Azure Key Vault とは

Azure AI サービスの仮想ネットワークを構成する

[アーティクル] • 2024/03/25

Azure AI サービスは、多層型のセキュリティ モデルを採用しています。 このモデルでは、ネットワークの特定のサブセットに、Azure AI サービス アカウントを固定することができます。 ネットワーク ルールを構成すると、指定したネットワークのセットを経由してデータを要求しているアプリケーションのみが、アカウントにアクセスできます。 要求フィルターを使用してリソースへのアクセスを制限して、Azure 仮想ネットワーク内の指定した IP アドレス、IP 範囲、またはサブネットのリストから発信された要求のみを許可することができます。

ネットワーク ルールが有効なときに Azure AI サービス リソースにアクセスするアプリケーションでは、認可が必要です。 承認は、Microsoft Entra ID 資格情報、または有効な API キーによりサポートされます。

> **ⓘ 重要**
>
> Azure AI サービス アカウントのファイアウォール規則をオンにすると、既定ではデータの受信要求がブロックされます。 要求を通すよう許可するには、次のいずれかの条件を満たしている必要があります。
>
> - 要求は、ターゲットの Azure AI サービス アカウントの許可されたサブネットの一覧にある Azure 仮想ネットワーク内で動作するサービスから発信されます。 仮想ネットワークを発信元とする要求のエンドポイントは、Azure AI サービス アカウントの**カスタム サブドメイン**として設定する必要があります。
> - 要求は、許可された IP アドレスのリストから発信されます。
>
> ブロックされる要求には、他の Azure サービスからの要求、Azure portal からの要求、ログおよびメトリック サービスからの要求が含まれます。

> **ⓘ 注意**
>
> Azure を操作するには、Azure Az PowerShell モジュールを使用することをお勧めします。 作業を開始するには、**Azure PowerShell のインストール**に関する記事を参照してください。 Az PowerShell モジュールに移行する方法については、「**AzureRM から Az への Azure PowerShell の移行**」を参照してください。

シナリオ

Azure AI サービス リソースをセキュリティで保護するには、最初に、(インターネット トラフィックを含む) すべてのネットワークからのトラフィックに対して既定でアクセスを拒否するように、ルールを構成する必要があります。 次に、特定の仮想ネットワークからのトラフィックにアクセスを許可するルールを構成します。 この構成では、アプリケーションに対してセキュリティで保護されたネットワーク境界を構築することができます。 また、選択したパブリック インターネット IP アドレス範囲からのトラフィックにアクセスを許可して、インターネットやオンプレミスの特定のクライアントからの接続を有効にすることもできます。

Azure AI サービスに対して、REST や WebSocket などのすべてのネットワーク プロトコルにネットワーク ルールが適用されます。 Azure のテスト コンソールのようなツールを使用してデータにアクセスするには、明示的なネットワーク ルールを構成する必要があります。 既存の Azure AI サービス リソース、または新しい Azure AI サービス リソースを作成するときに、ネットワークルールを適用できます。 ネットワーク ルールが適用されると、そのルールはすべての要求に対して適用されます。

サポートされているリージョンとサービス内容

仮想ネットワークは、Azure AI サービスが使用可能なリージョン でサポートされます。 Azure AI サービスは、ネットワーク ルールの構成用のサービス タグをサポートしています。 こちらに示すサービスは、`CognitiveServicesManagement` サービス タグに含まれています。

- ✓ Anomaly Detector
- ✓ Azure OpenAI
- ✓ Content Moderator
- ✓ Custom Vision
- ✓ Face
- ✓ Language Understanding (LUIS)
- ✓ Personalizer
- ✓ Speech サービス
- ✓ Language
- ✓ QnA Maker
- ✓ Translator

> **注意**
>
> Azure OpenAI、LUIS、Speech Services、または言語サービスを使用している場合、`CognitiveServicesManagement` タグを指定しても、SDK または REST API を使用

してサービスを使用できるようになるだけです。 仮想ネットワークから Azure OpenAI Studio、LUIS ポータル、Speech Studio または言語サービスにアクセスして使用するには、次のタグを使用する必要があります。

- `AzureActiveDirectory`
- `AzureFrontDoor.Frontend`
- `AzureResourceManager`
- `CognitiveServicesManagement`
- `CognitiveServicesFrontEnd`
- `Storage` (Speech Studio のみ)

既定のネットワーク アクセス ルールの変更

既定では、Azure AI サービス リソースは任意のネットワーク上のクライアントからの接続を受け入れます。 選択したネットワークへのアクセスを制限するには、まず既定のアクションを変更する必要があります。

> ⚠ **警告**
>
> ネットワーク ルールを変更すると、Azure AI サービスに接続するアプリケーションの機能に影響が及ぶことがあります。 既定のネットワーク ルールを拒否に設定すると、アクセスを許可する特定のネットワーク ルールも合わせて適用されていない限り、データへのアクセスがすべてブロックされます。
>
> アクセスを拒否する既定のルールを変更する前に、ネットワーク ルールを使用して、許可されたネットワークへのアクセスを許可するようにしてください。 オンプレミス ネットワークの IP アドレスを一覧表示することを許可する場合は、オンプレミス ネットワークから発信することができるすべてのパブリック IP アドレスを追加してください。

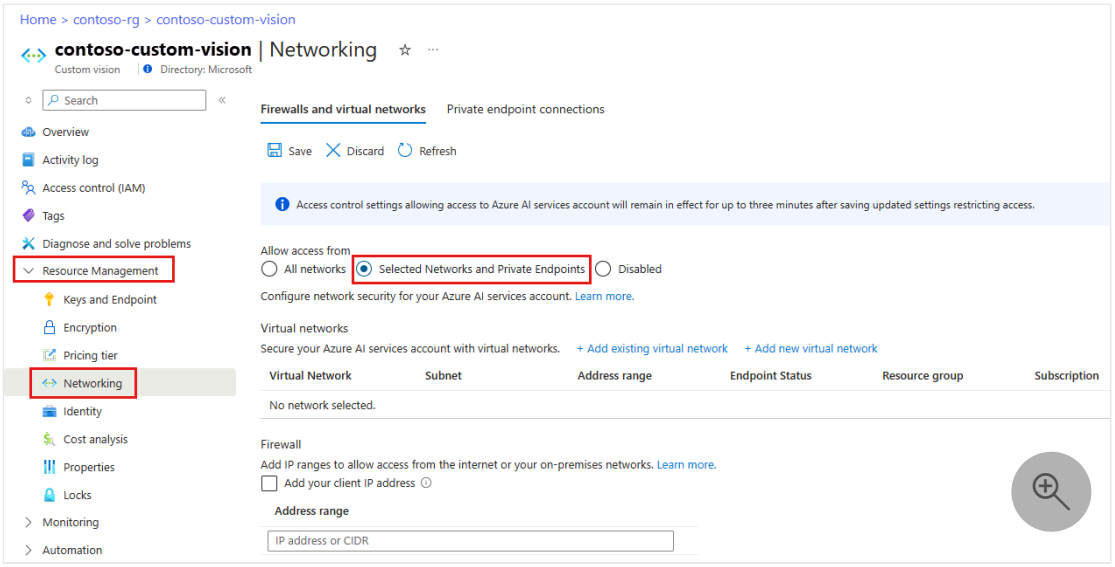
既定のネットワーク アクセス ルールを管理する

Azure AI サービス リソースの規定のネットワーク アクセス ルールは、Azure portal、PowerShell、または Azure CLI で管理できます。

Azure Portal

1. セキュリティで保護する Azure AI サービス リソースにアクセスします。

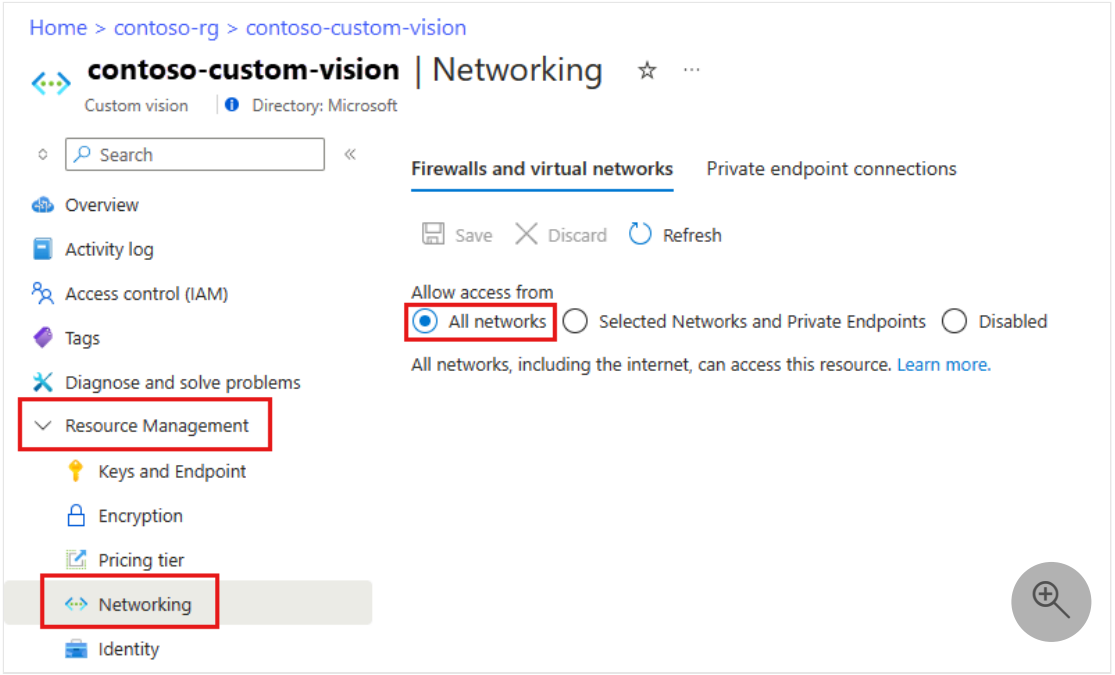
2. [**リソース管理**] を選択して展開し、[**ネットワーク**] を選択します。



3. 既定でアクセスを拒否するには、[**ファイアウォールと仮想ネットワーク**] で、[**選択したネットワークとプライベート エンドポイント**] を選択します。

   この設定のみ行った状態で、[仮想ネットワーク] または [アドレス範囲] を構成していない場合 - すべてのアクセスが効率的に拒否されます。 すべてのアクセスが拒否された場合、Azure AI サービス リソースを使用しようとしている要求は許可されません。 これまで通り、Azure portal、Azure PowerShell または Azure CLI を使用して Azure AI サービス リソースを構成することもできます。

4. すべてのネットワークからのトラフィックを許可するには、[**すべてのネットワーク**] を選択します。



5. [**保存**] を選択して変更を保存します。

仮想ネットワークからアクセスの許可

パブリック インターネットの特定のサブネットからのアクセスのみを許可するように、Azure AI サービス リソースを構成できます。 許可されたサブネットは、同じサブスクリプションの仮想ネットワークに属する場合や、異なるサブスクリプションに属する場合があります。 他のサブスクリプションは、別の Microsoft Entra テナントに属することができます。 サブネットが別のサブスクリプションに属している場合、Microsoft.CognitiveServices リソース プロバイダーもそのサブスクリプションに登録されている必要があります。

仮想ネットワーク内の Azure AI サービスに対するサービス エンドポイントを有効にすることができます。 サービス エンドポイントを使用すると、最適なパスを経由して、仮想ネットワークから Azure AI サービスへトラフィックがルーティングされます。 詳細については、「仮想ネットワーク サービス エンドポイント」を参照してください。

サブネットと仮想ネットワークの ID も、各要求と一緒に転送されます。 管理者は、その後、仮想ネットワーク内の特定のサブネットからの要求を許可するネットワーク規則を、Azure AI サービス リソースに対して構成できます。 これらのネットワーク ルールによってアクセスを許可されたクライアントがデータにアクセスするには、Azure AI サービス リソースの認可要件を引き続き満たす必要があります。

各 Azure AI サービス リソースでは最大 100 個の 仮想ネットワーク ルールがサポートされ、それを IP ネットワーク規則と組み合わせることができます。 詳細については、この記事で後述する「インターネットの IP 範囲からのアクセスを許可する」を参照してください。

必要なアクセス許可を設定する

Azure AI サービス リソースに仮想ネットワーク規則を適用するには、追加されるサブネットに対する適切なアクセス許可が必要です。 必要なアクセス許可は、既定の共同作成者ロール、または *Cognitive Services* 共同作成者ロールです。 必要なアクセス許可をカスタム ロール定義に追加することもできます。

Azure AI サービス リソースおよびアクセスを許可された仮想ネットワークは、他の Azure AD テナントの一部であるサブスクリプションなどの、異なるサブスクリプションに含まれる場合があります。

> ⓘ **注意**

異なる Microsoft Entra テナントの一部である仮想ネットワーク内のサブネットへのアクセスを許可するルールの構成は、現在、PowerShell、Azure CLI、REST API でのみサポートされています。 これらの規則は Azure portal に表示できますが、構成することはできません。

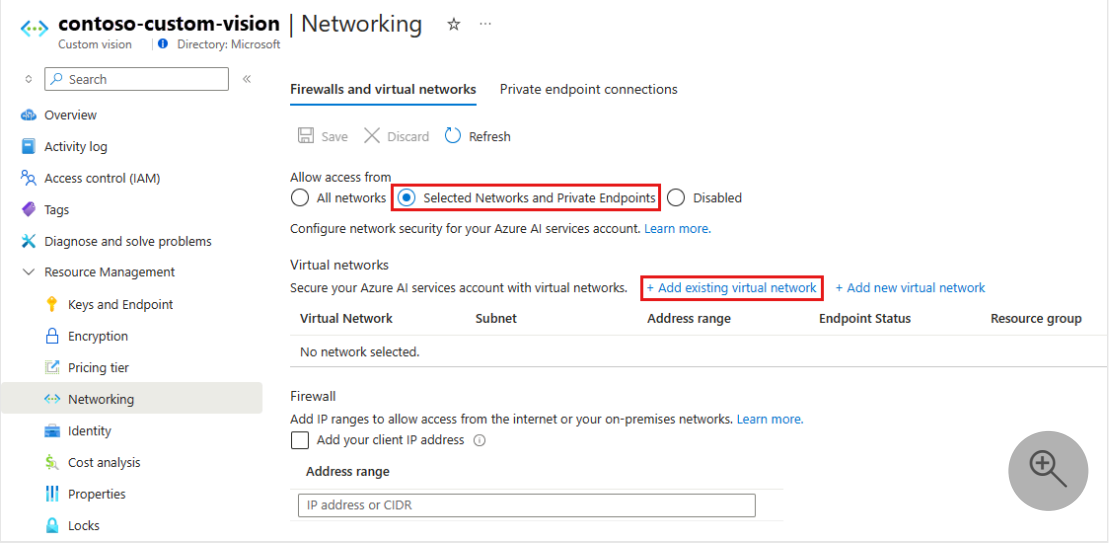
仮想ネットワーク規則を構成する

Azure AI サービス リソースの 仮想ネットワーク規則は、Azure portal、PowerShell、または Azure CLI で管理できます。

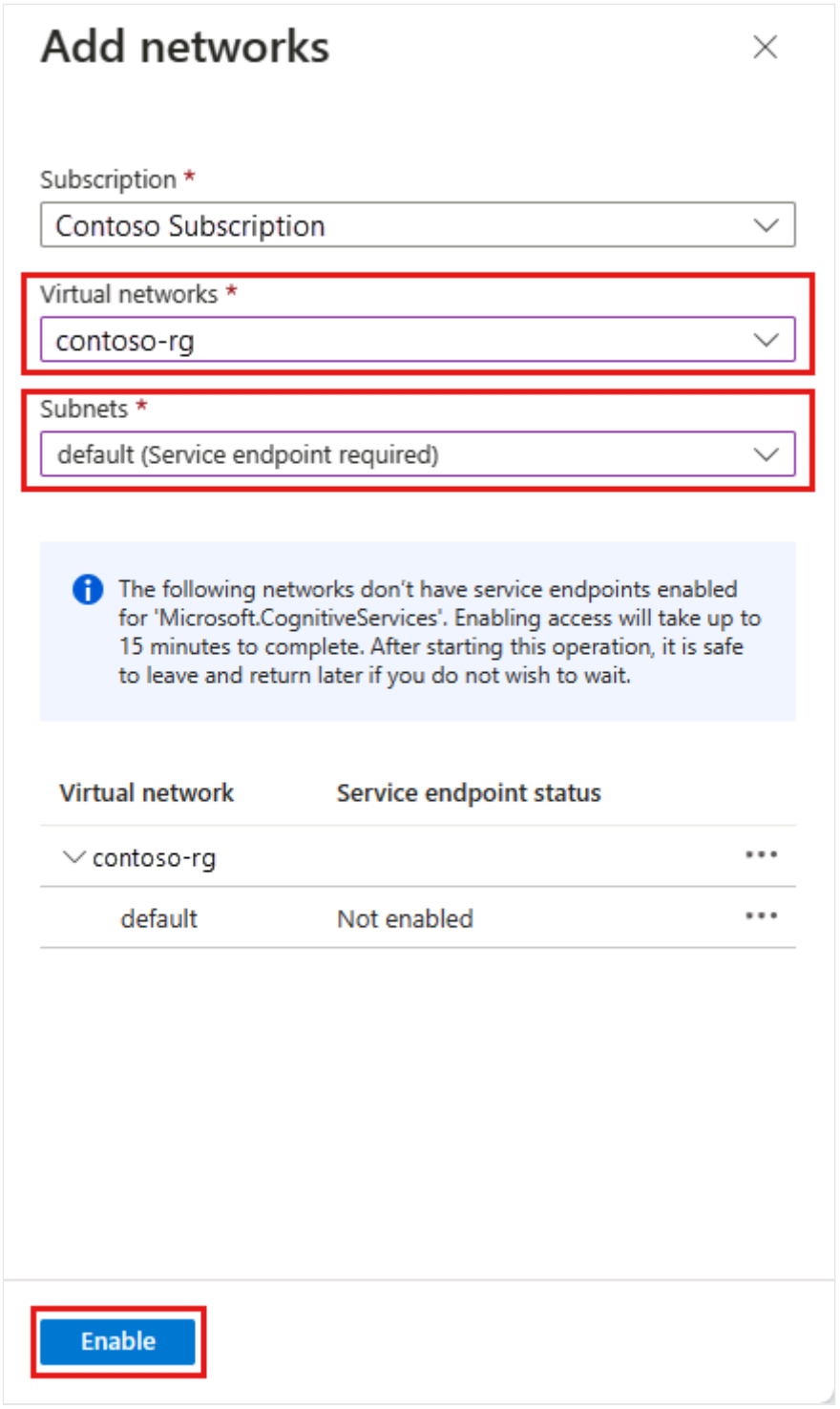
Azure Portal

既存のネットワーク規則を使用して仮想ネットワークへのアクセスを許可するには、次のようにします。

1. セキュリティで保護する Azure AI サービス リソースにアクセスします。
2. [**リソース管理**] を選択して展開し、[**ネットワーク**] を選択します。
3. 選択した [**選択されたネットワークとプライベート エンドポイント**] を確認します。
4. [**許可するアクセス元**] で、[**既存の仮想ネットワークを追加**] を選択します。



5. [**仮想ネットワーク**] と [**サブネット**] オプションを選択して、 [**有効化**] を選択します。



注意

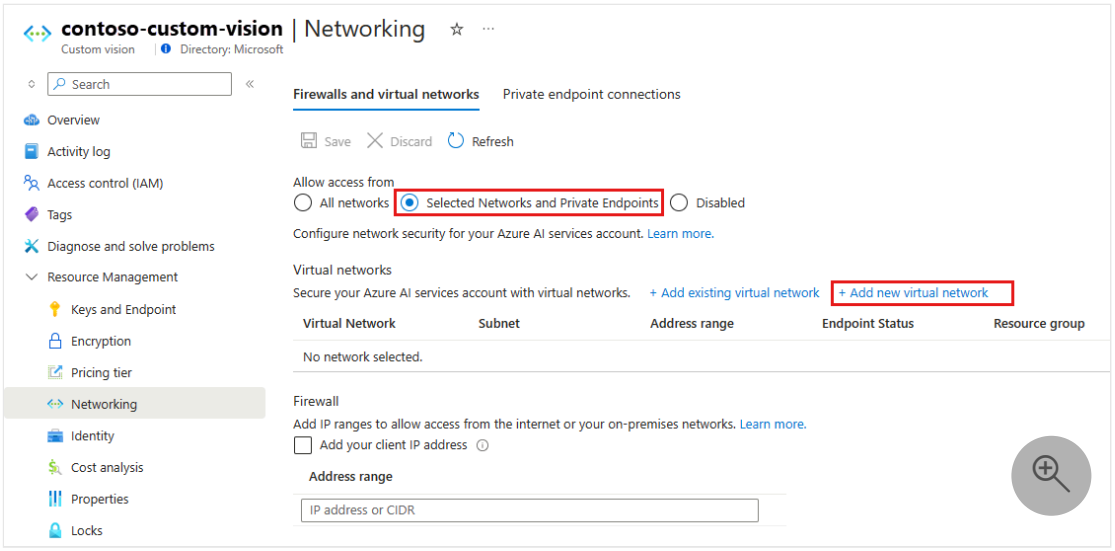
Azure AI サービス用のサービス エンドポイントが、選択した仮想ネットワークとサブネットに対してまだ構成されていない場合は、この操作の中で構成することができます。

現在、同じ Microsoft Entra テナントに属する仮想ネットワークのみが、ルールの作成時に選択可能です。 別のテナントに属する仮想ネットワーク内のサブネットにアクセスを許可するには、PowerShell、Azure CLI、または REST API を使用します。

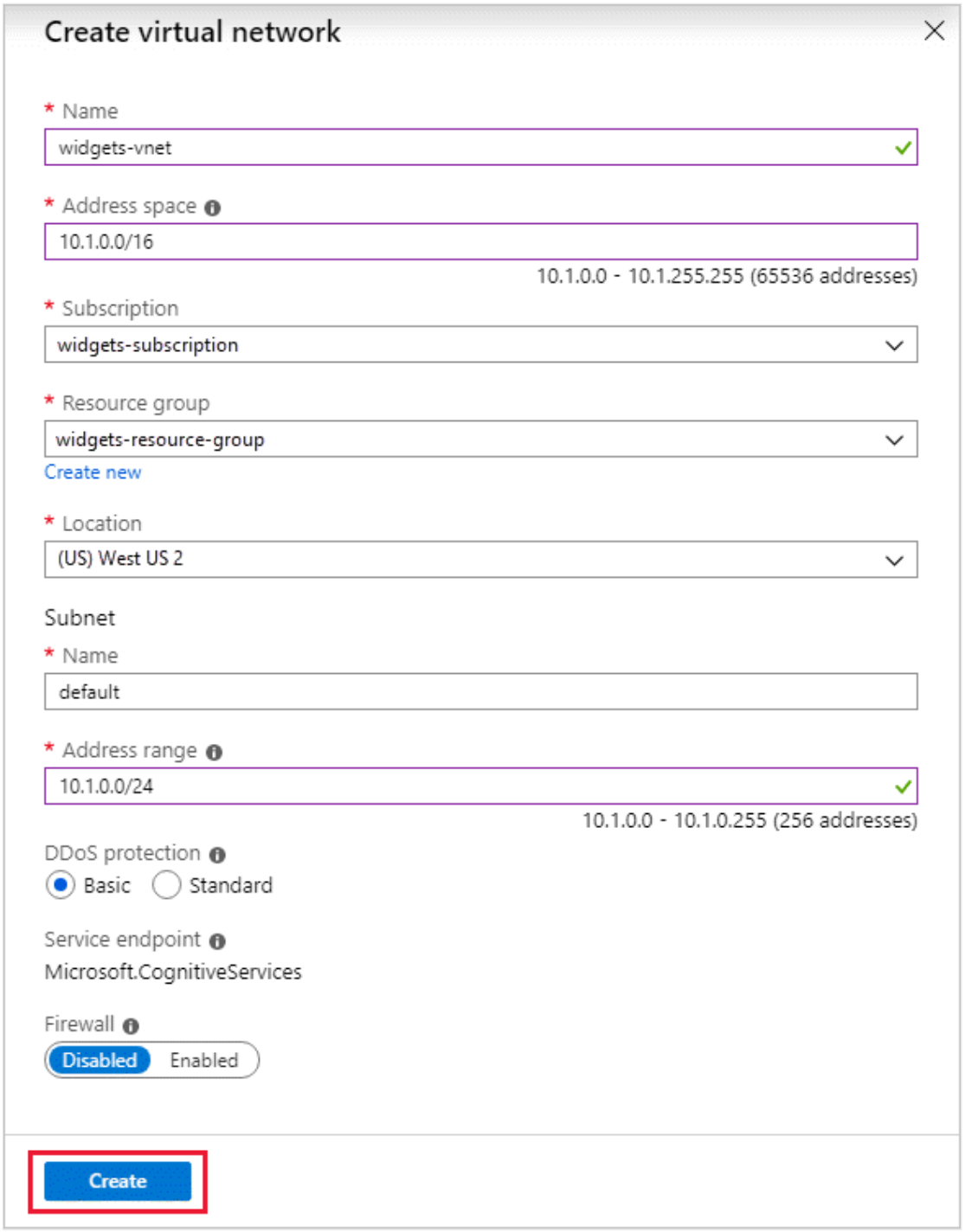
6. **[保存]** を選択して変更を保存します。

新しい仮想ネットワークを作成してアクセスを許可するには、次のようにします。

1. 前の手順と同じページで、**[新しい仮想ネットワークを追加]** を選択します。



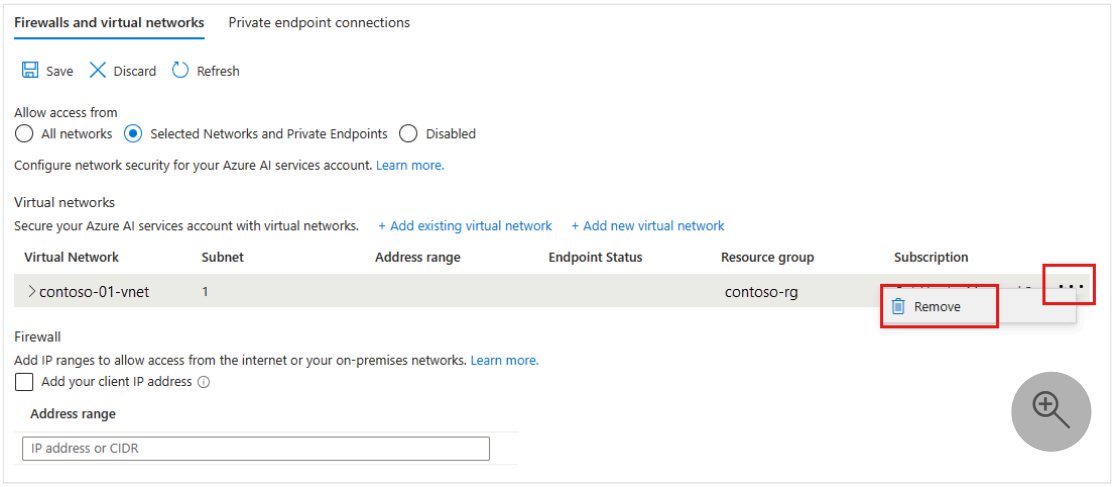
2. 新しい仮想ネットワークの作成に必要な情報を指定して、 **[作成]** を選択します。



3. **[保存]** を選択して変更を保存します。

仮想ネットワークまたはサブネット規則を削除するには、次のようにします。

1. 前の手順と同じページで、**...(その他のオプション)** を選択し、仮想ネットワークまたはサブネットのコンテキスト メニューを開いて、**[削除]** を選択します。



2. **[保存]** を選択して変更を保存します。

> **重要**
>
> 拒否するように**既定のルールを設定**します。そうしないと、ネットワーク ルールは効力を発揮しません。

インターネットの IP 範囲からのアクセスを許可する

パブリック インターネットの特定の IP アドレス範囲からのアクセスを許可するように、Azure AI サービス リソースを構成できます。 この構成では、一般的なインターネット トラフィックを効率的にブロックする特定のサービスとオンプレミスのネットワークにアクセスを許可します。

許可するインターネット アドレスの範囲は、CIDR 表記法 (RFC 4632) を使って `192.168.0.0/16` の形式で、または `192.168.0.1` のように個々の IP アドレスとして指定できます。

> **ヒント**
>
> `/31` や `/32` のプレフィックス サイズを使用する小さいアドレス範囲はサポートされていません。 これらの範囲を構成するには、個別の IP アドレス規則を使用します。

IP ネットワーク ルールは、パブリック インターネットの IP アドレスに対してのみ許可されます。 プライベート ネットワーク用に予約されている IP アドレス範囲は、IP 規則では許可されません。 プライベート ネットワークには、`10.*`、`172.16.*` -

`172.31.*`、および `192.168.*` で始まるアドレスが含まれます。 詳細については、「プライベート アドレス空間 (RFC 1918)」を参照してください。

現在サポートされているのは、IPv4 アドレスのみです。 各 Azure AI サービス リソースでは最大 100 個の IP ネットワーク規則がサポートされ、それを IP ネットワーク規則と組み合わせることができます。

オンプレミスのネットワークからのアクセスの構成

IP ネットワーク ルールでオンプレミスのネットワークから Azure AI サービス リソースへのアクセスを許可するには、ネットワークで使用するインターネット接続 IP アドレスを特定します。 サポートが必要な場合は、ネットワーク管理者にお問い合わせください。

パブリック ピアリングまたは Microsoft ピアリングのためにオンプレミスで Azure ExpressRoute を使用している場合、NAT の IP アドレスを識別する必要があります。 詳細については、「Azure ExpressRoute とは」を参照してください。

パブリック ピアリングの場合、各 ExpressRoute 回線は既定で 2 つの NAT IP アドレスを使用します。 それぞれの NAT IP アドレスは、トラフィックが Microsoft Azure ネットワーク バックボーンに入ったときに Azure サービス トラフィックに適用されます。 Microsoft ピアリングの場合、使用される NAT の IP アドレスは、ユーザーが指定するか、サービス プロバイダーが指定します。 サービス リソースへのアクセスを許可するには、リソースの IP ファイアウォール設定でこれらのパブリック IP アドレスを許可する必要があります。

パブリック ピアリングの ExpressRoute 回線の IP アドレスを確認するには、Azure portal を使用して ExpressRoute のサポート チケットを開いてください。 詳細については、「Azure パブリック ピアリングの NAT 要件」を参照してください。

IP ネットワーク ルールの管理

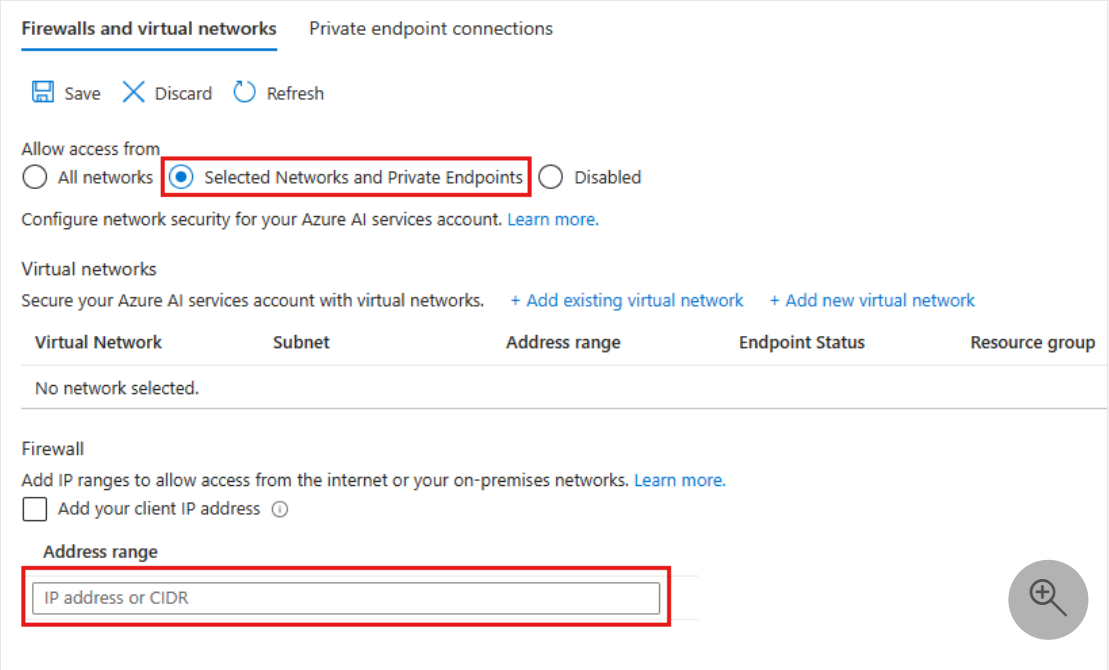
Azure AI サービス リソースの IP ネットワーク ルールは、Azure portal、PowerShell、または Azure CLI で管理できます。

Azure Portal

1. セキュリティで保護する Azure AI サービス リソースにアクセスします。
2. **[リソース管理]** を選択して展開し、**[ネットワーク]** を選択します。

3. 選択した **[選択されたネットワークとプライベート エンドポイント]** を確認します。

4. **[ファイアウォールと仮想ネットワーク]** で、**[アドレス範囲]** オプションを見つけます。 インターネット IP 範囲へのアクセスを許可するには、IP アドレスまたはアドレス範囲 (CIDR 形式) を入力します。 有効なパブリック IP (予約されない) アドレスのみが受け入れられます。



IP ネットワーク ルールを削除するには、アドレス範囲の横にあるごみ箱 🗑 のアイコンを選択します。

5. **[保存]** を選択して変更を保存します。

> **ⓘ 重要**
>
> 拒否するように**既定のルールを設定**します。そうしないと、ネットワーク ルールは効力を発揮しません。

プライベート エンドポイントを使用する

お使いの Azure AI サービス リソースのプライベート エンドポイントを使用すると、仮想ネットワーク上のクライアントは Azure Private Link を介してデータに安全にアクセスできるようになります。 プライベート エンドポイントでは、対象の Azure AI サービス リソースのために仮想ネットワークのアドレス空間の IP アドレスを使用します。 仮想ネットワーク上のクライアントとリソース間のネットワーク トラフィックは、仮想

ネットワークおよび Microsoft Azure バックボーン ネットワーク上のプライベート リンクを経由することで、パブリック インターネットにさらされないようにします。

Azure AI サービス リソースのプライベート エンドポイントを使用すると、次のことができます。

- Azure AI サービスのパブリック エンドポイント上のすべての接続をブロックするようにファイアウォールを構成して、Azure AI サービス リソースをセキュリティで保護します。
- 仮想ネットワークからのデータの流出をブロックし、仮想ネットワークのセキュリティを強化します。
- Azure VPN Gateway または ExpressRoute プライベート ピアリングを使用することで、仮想ネットワークに接続するオンプレミス ネットワークから Azure AI サービス リソースに安全に接続します。

プライベート エンドポイントの概要

プライベート エンドポイントは、仮想ネットワーク内の Azure リソース用の特別なネットワーク インターフェイスです。 Azure AI サービス リソースのプライベート エンドポイントを作成すると、対象の仮想ネットワーク上のクライアントと対象のリソース間のセキュリティで保護された接続が提供されます。 プライベート エンドポイントには、仮想ネットワークの IP アドレス範囲から IP アドレスが割り当てられます。 プライベート エンドポイントと Azure AI サービス間の接続には、セキュリティで保護されたプライベート リンクを使用します。

仮想ネットワーク内のアプリケーションは、プライベート エンドポイント経由でサービスにシームレスに接続できます。 接続には、それ以外の接続で使用するものと同じ接続文字列と承認メカニズムが使用されます。 例外は Speech Service で、これには別のエンドポイントが必要です。 詳細については、この記事の「プライベート エンドポイントと Speech Service」を参照してください。 プライベート エンドポイントは、Azure AI サービス リソースでサポートされているすべてのプロトコル (REST を含む) で使用できます。

プライベート エンドポイントは、サービス エンドポイントを使用するサブネットに作成できます。 サブネット内のクライアントは、プライベート エンドポイントを使用して 1 つの Azure AI サービス リソースに接続する一方で、サービス エンドポイントを使用して他のリソースにアクセスできます。 詳細については、「仮想ネットワーク サービス エンドポイント」を参照してください。

お使いの仮想ネットワークで Azure AI サービス リソース向けのプライベート エンドポイントを作成すると、承認を得るための同意要求が Azure から Azure AI サービス リソ

ースの所有者に送信されます。 プライベート エンドポイントの作成を要求しているユーザーがリソースの所有者でもある場合、この同意要求は自動的に承認されます。

Azure AI サービス リソースの所有者は、Azure portal で Azure AI サービス リソースの [**プライベート エンドポイント接続**] タブを使用して、同意要求とプライベート エンドポイントを管理できます。

プライベート エンドポイントを指定する

プライベート エンドポイントを作成する場合は、接続先の Azure AI サービス リソースを指定します。 プライベート エンドポイントを作成する方法の詳細については、次の記事を参照してください。

- Azure portal を使用してプライベート エンドポイントを作成する
- Azure PowerShell を使用してプライベート エンドポイントを作成する
- Azure CLI を使用してプライベート エンドポイントを作成する

プライベート エンドポイントに接続する

> **注意**
>
> Azure OpenAI Service では、他の Azure AI サービスとは異なるプライベート DNS ゾーンおよびパブリック DNS ゾーン フォワーダーが使用されます。 正しいゾーンとフォワーダーの名前については、「**Azure サービス DNS ゾーンの構成**」に関する記事を参照してください。

プライベート エンドポイントを使用する仮想ネットワーク上のクライアントは、パブリック エンドポイントに接続するクライアントと同じ接続文字列を Azure AI サービス リソースに対して使用します。 例外は Speech サービスで、これには別のエンドポイントが必要です。 詳細については、この記事の「Speech サービスでプライベート エンドポイントを使用する」を参照してください。 DNS 解決は、プライベート リンク経由の仮想ネットワークから Azure AI サービス リソースへの接続を自動的にルーティングします。

既定では、Azure によって、仮想ネットワークに接続されているプライベート DNS ゾーンが作成され、プライベート エンドポイントに必要な更新も行われます。 独自の DNS サーバーを使用している場合は、DNS 構成に追加の変更が必要になることがあります。 プライベート エンドポイントに必要な更新プログラムについては、この記事の「プライベート エンドポイントに DNS の変更を適用する」を参照してください。

Speech サービスでプライベート エンドポイントを使用する

「プライベート エンドポイント経由で Speech サービスを使用する」を参照してください。

プライベート エンドポイントに DNS の変更を適用する

プライベート エンドポイントを作成すると、Azure AI サービス リソースの DNS `CNAME` リソース レコードは、プレフィックス `privatelink` を持つサブドメイン内のエイリアスに更新されます。 既定で、Azure で `privatelink` サブドメインに対応するプライベート DNS ゾーンも作成されます。これには、プライベート エンドポイントの DNS A リソース レコードが含まれます。 詳細については、「Azure Private DNS とは」を参照してください。

プライベート エンドポイントがある仮想ネットワークの外部からエンドポイントの URL を解決すると、Azure AI サービス リソースのパブリック エンドポイントに解決されます。 プライベート エンドポイントをホストしている仮想ネットワークから解決されると、エンドポイント URL はプライベート エンドポイントの IP アドレスに解決されます。

この方法を使用すると、プライベート エンドポイントをホストしている仮想ネットワーク上のクライアントと、仮想ネットワークの外部のクライアントから同じ接続文字列を使用して Azure AI サービス リソースにアクセスできます。

ネットワーク上でカスタム DNS サーバーを使用している場合、クライアントで、Azure AI サービス リソースのエンドポイントの完全修飾ドメイン名 (FQDN) をプライベート エンドポイントの IP アドレスに解決できる必要があります。 Private Link サブドメインを仮想ネットワークのプライベート DNS ゾーンに委任するように、DNS サーバーを構成します。

> **ヒント**
>
> カスタムまたはオンプレミスの DNS サーバーを使用している場合は、`privatelink` サブドメインの Azure AI サービス リソース名をプライベート エンドポイントの IP アドレスに解決するように、DNS サーバーを構成する必要があります。 `privatelink` サブドメインを仮想ネットワークのプライベート DNS ゾーンに委任します。 または、DNS サーバーで DNS ゾーンを構成し、DNS A レコードを追加します。

プライベート エンドポイントをサポートするように独自の DNS サーバーを構成する方法の詳細については、次のリソースを参照してください。

- 独自の DNS サーバーを使用する名前解決
- DNS の構成

Azure OpenAI の信頼された Azure サービスへのアクセス権を付与する

他のアプリのネットワーク規則を維持しながら、信頼された Azure サービスのサブセットに Azure OpenAI へのアクセス権を付与することができます。 その後、これらの信頼されたこれらのサービスでは、マネージド ID を使用して、Azure OpenAI サービスの認証が行われます。 次の表は、これらのサービスのマネージド ID に適切なロールが割り当てられている場合に Azure OpenAI にアクセスできるサービスを示しています。

テーブルを展開する

サービス	リソース プロバイダー名
Azure AI Services	`Microsoft.CognitiveServices`
Azure Machine Learning	`Microsoft.MachineLearningServices`
Azure AI Search	`Microsoft.Search`

信頼された Azure サービスへのネットワーク アクセス権は、REST API を使用してネットワーク規則の例外を作成すると付与できます。

Bash

```
accessToken=$(az account get-access-token --resource
https://management.azure.com --query "accessToken" --output tsv)
rid="/subscriptions/<your subscription id>/resourceGroups/<your resource
group>/providers/Microsoft.CognitiveServices/accounts/<your Azure AI
resource name>"

curl -i -X PATCH https://management.azure.com$rid?api-version=2023-10-01-
preview \
-H "Content-Type: application/json" \
-H "Authorization: Bearer $accessToken" \
-d \
'
{
    "properties":
    {
        "networkAcls": {
```

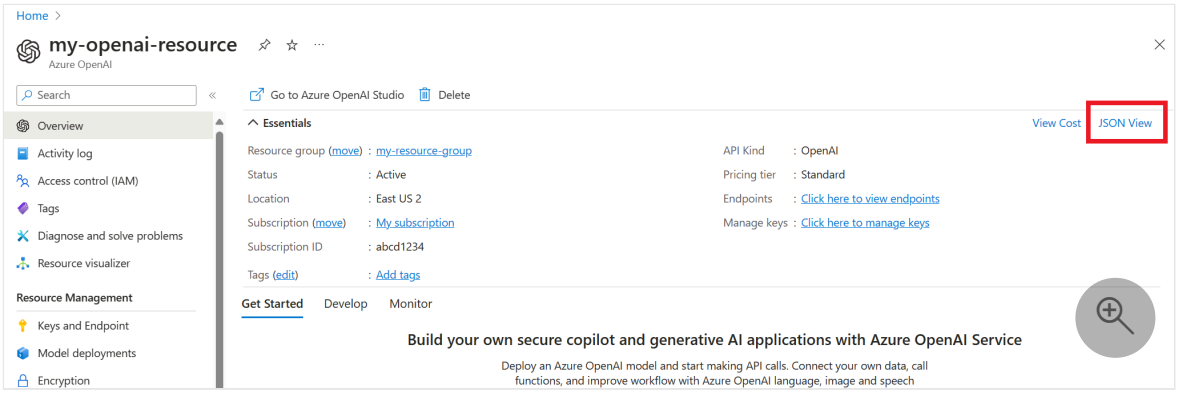
```
            "bypass": "AzureServices"
        }
    }
}
'
```

> **注意**
>
> 信頼されたサービス機能は、上記のコマンド ラインを使用してのみ使用でき、Azure portal を使用して実行することはできません。

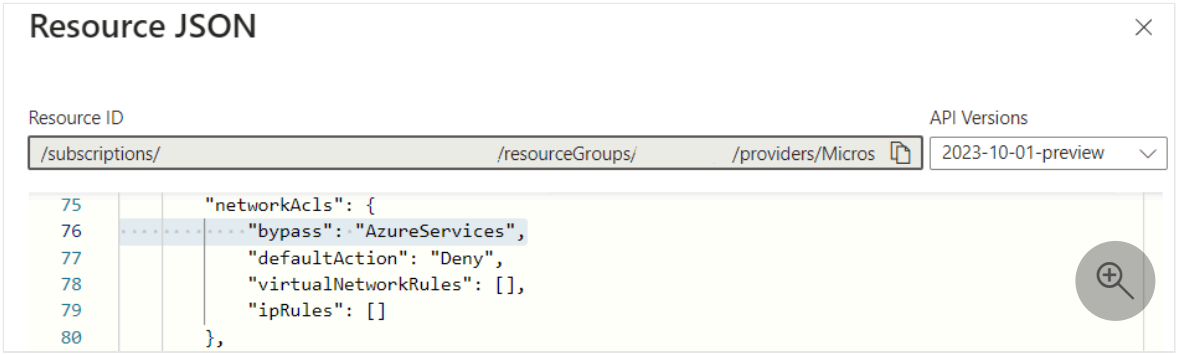
例外を取り消すには、`networkAcls.bypass` を `None` に設定します。

Azure portal から信頼できるサービスが有効になっているかどうかを確認するには、

1. Azure OpenAI リソースの概要ページから **[JSON ビュー]** を使用します。



2. **[API バージョン]** で最新の API バージョンを選択します。 最新の API バージョン (`2023-10-01-preview`) のみサポートされています。



価格

料金の詳細については、「Azure Private Link の料金」をご覧ください。

次のステップ

- さまざまな Azure AI サービスを探索する
- 仮想ネットワーク サービス エンドポイントの詳細

Key Vault を使用して Azure AI サービス アプリケーションを開発する

[アーティクル] • 2024/02/14

Azure Key Vault を使用して Azure AI サービス アプリケーションを安全に開発する方法について説明します。

Key Vault を使うと、アプリケーションにセキュリティ情報を格納せずにすむため、シークレットが誤って漏洩するリスクが軽減されます。

前提条件

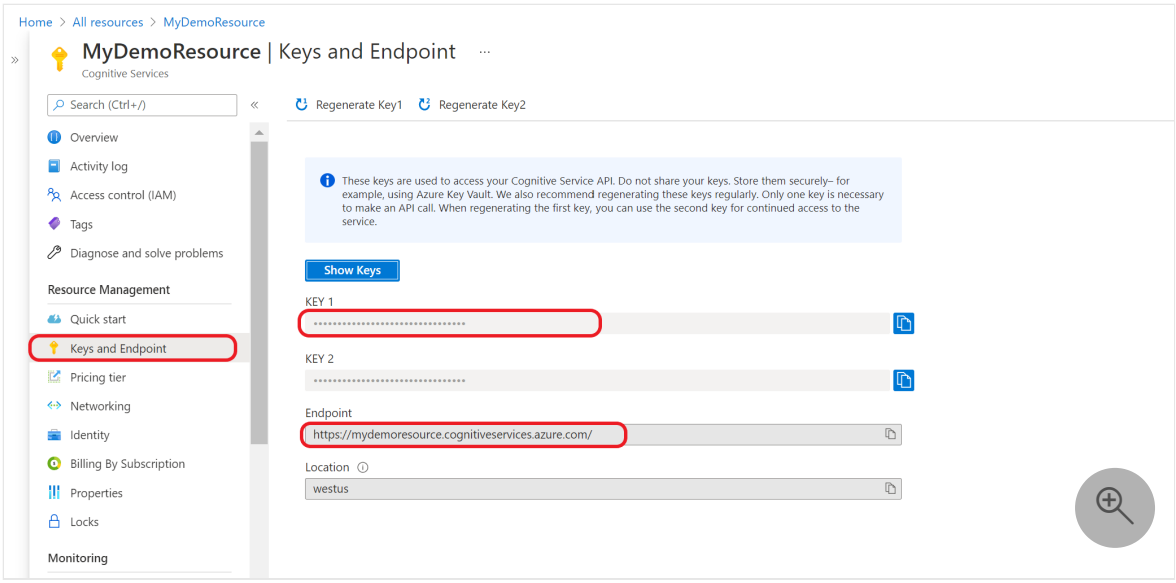
- 有効な Azure サブスクリプション - 無料アカウントを作成する
- Visual Studio IDE
- Azure Key Vault
- マルチサービス リソースまたは特定のサービスのリソース

> **注意**
>
> お使いの Azure AI サービスのドキュメントとクイックスタート記事を確認して、以下の内容を理解してください。
>
> - API 呼び出しを送信するために必要な資格情報と他の情報。
> - アプリケーションを実行するために必要なパッケージとコード。

Azure AI サービス リソースから資格情報を取得する

資格情報を Azure キー コンテナーに追加する前に、Azure AI サービス リソースから資格情報を取得する必要があります。 たとえば、お使いのサービスでキーとエンドポイントが必要な場合は、次の手順のようにして確認します。

1. Azure portal で Azure リソースに移動します。
2. 左側の折りたたみ可能なメニューから、**[キーとエンドポイント]** を選びます。



一部の Azure AI サービスでは、キーやリージョンなど、API 呼び出しの認証に必要な情報が異なります。 続ける前に、必ずこの情報を取得してください。

資格情報をキー コンテナーに追加する

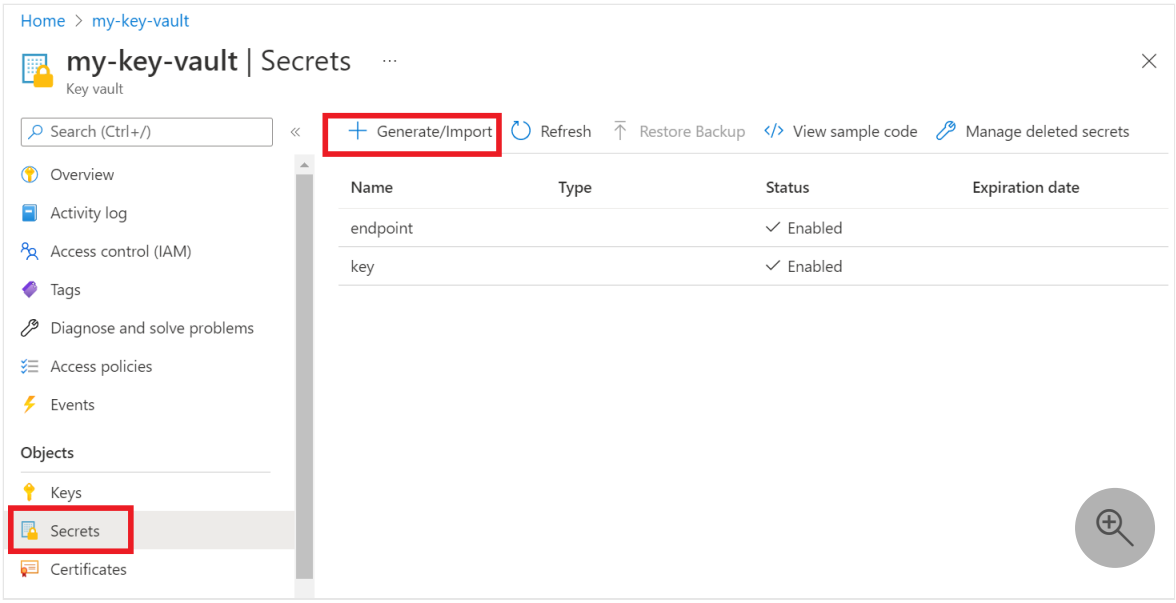
アプリケーションで資格情報を取得し、それを使って API 呼び出しの認証を行うには、キー コンテナーのシークレットにそれを追加する必要があります。

次の手順を繰り返して、必要なリソース資格情報ごとにシークレットを生成します。 たとえば、キーとエンドポイントなどです。 これらのシークレット名は、後でアプリケーションの認証に使われます。

1. ブラウザーの新しいタブまたはウィンドウを開きます。 Azure portal で、キー コンテナーに移動します。

2. 左側の折りたたみ可能なメニューから、**[オブジェクト]**>**[シークレット]** を選びます。

3. **[Generate/Import](生成/インポート)** を選択します。



4. **[シークレットの作成]** 画面で、次の値を入力します。

テーブルを展開する

名前	値
Upload options	手動
名前	キーまたはエンドポイントのシークレット名。 例: "CognitiveServicesKey" または "CognitiveServicesEndpoint"
値	Azure AI サービス リソースのキーまたはエンドポイント。

後で、アプリケーションでシークレットの "名前" を使って "値" に安全にアクセスします。

5. 他の値は既定値のままにしておきます。 **［作成］** を選択します

> **ヒント**
>
> 後でアプリケーションで使うので、シークレットに設定した名前を必ず覚えておいてください。

これで、リソース情報用のシークレットに名前を付けました。

キー コンテナーの名前用の環境変数を作成する

お使いの Azure キー コンテナーの名前用に環境変数を作ることをお勧めします。 アプリケーションで実行時にこの環境変数を読み取って、キーとエンドポイントの情報を取

得します。

環境変数を設定するには、次のいずれかのコマンドを使います。 `KEY_VAULT_NAME` は環境変数の名前で、`Your-Key-Vault-Name` はキー コンテナーの名前に置き換えます。これが環境変数に格納されます。

Azure CLI

永続化された環境変数を作成して割り当て、値を指定します。

CMD

```
setx KEY_VAULT_NAME "Your-Key-Vault-Name"
```

コマンド プロンプトの新しいインスタンスで、環境変数を読み取ります。

CMD

```
echo %KEY_VAULT_NAME%
```

Visual Studio を使用して Azure に対する認証を行う

Visual Studio 2017 以降を使っている開発者は、Visual Studio で Microsoft Entra アカウントの認証を行うことができます。 これにより、IDE 内から Azure サブスクリプションにサインインすることで、キー コンテナー内のシークレットにアクセスできます。

Visual Studio で認証を行うには、上部のナビゲーション メニューから **[ツール]** を選んで、**[オプション]** を選びます。 **[Azure サービス認証]** オプションに移動し、ユーザー名とパスワードでサインインします。

コマンド ラインを使用して認証を行う

キー コンテナーへのアクセスを許可する前に、Microsoft Entra のユーザー名とパスワードで認証を行う必要があります。

Azure CLI

Azure CLI で認証を行うには、`az login` コマンドを実行します。

Azure CLI

```
az login
```

既定の Web ブラウザーを使っているシステムでは、Azure CLI によって認証のためにブラウザーが起動されます。 既定の Web ブラウザーがないシステムの場合は、`az login` コマンドでデバイス コード認証フローを使用します。 `--use-device-code` 引数を指定してブラウザーを起動するのではなく、デバイス コード フローを使うよう Azure CLI に強制することもできます。

複数のサブスクリプションがある場合は、必ずキー コンテナーが含まれる Azure サブスクリプションを選択してください。

キー コンテナーへのアクセス許可を付与する

自分のユーザー アカウントにシークレットのアクセス許可を付与するアクセス ポリシーをキー コンテナーに対して作成します。

Azure CLI

アクセス ポリシーを設定するには、az keyvault set-policy コマンドを実行します。 `Your-Key-Vault-Name` は、実際のキー コンテナーの名前に置き換えます。 `user@domain.com` をお使いの Microsoft Entra ユーザー名に置き換えます。

Azure CLI

```
az keyvault set-policy --name Your-Key-Vault-Name --upn user@domain.com
--secret-permissions delete get list set purge
```

新しい C# アプリケーションを作成する

Visual Studio IDE を使用して新しい .NET Core コンソール アプリを作成します。 1 つの C# ソース ファイル (`program.cs`) を含んだ "Hello World" プロジェクトが作成されます。

ソリューション エクスプローラーでソリューションを右クリックし、**[NuGet パッケージの管理]** を選んで、次のクライアント ライブラリをインストールします。 開いたパッケージ マネージャーで **[参照]** を選び、次のライブラリを検索して、**[インストール]** を選びます。

- `Azure.Security.KeyVault.Secrets`
- `Azure.Identity`

コード例をインポートする

`program.cs` ファイルに次のコード例をコピーします。 `Your-Key-Secret-Name` と `Your-Endpoint-Secret-Name` は、自分のキー コンテナーに設定したシークレット名に置き換えます。

C#

```
using System;
using System.Threading.Tasks;
using Azure;
using Azure.Identity;
using Azure.Security.KeyVault.Secrets;
using System.Net;

namespace key_vault_console_app
{
    class Program
    {
        static async Task Main(string[] args)
        {
            //Name of your key vault
            var keyVaultName =
Environment.GetEnvironmentVariable("KEY_VAULT_NAME");

            //variables for retrieving the key and endpoint from your key
vault.
            //Set these variables to the names you created for your secrets
            const string keySecretName = "Your-Key-Secret-Name";
            const string endpointSecretName = "Your-Endpoint-Secret-Name";

            //Endpoint for accessing your key vault
            var kvUri = $"https://{keyVaultName}.vault.azure.net";

            var keyVaultClient = new SecretClient(new Uri(kvUri), new
DefaultAzureCredential());

            Console.WriteLine($"Retrieving your secrets from
{keyVaultName}.");

            //Key and endpoint secrets retrieved from your key vault
            var keySecret = await
keyVaultClient.GetSecretAsync(keySecretName);
            var endpointSecret = await
keyVaultClient.GetSecretAsync(endpointSecretName);
            Console.WriteLine($"Your key secret value is:
{keySecret.Value.Value}");
            Console.WriteLine($"Your endpoint secret value is:
```

```
{endpointSecret.Value.Value}");
            Console.WriteLine("Secrets retrieved successfully");

        }
    }
}
```

アプリケーションの実行

Visual studio の上部にある [**デバッグ**] ボタンを選んで、アプリケーションを実行します。 キーとエンドポイントのシークレットが、キー コンテナーから取得されます。

言語サービスのテスト呼び出しを送信する (省略可能)

マルチサービス リソースまたは言語リソースを使っている場合は、次の手順のようにして、キー コンテナーからキーとエンドポイントを取得することで固有表現認識の呼び出し例を送信するように、アプリケーションを更新できます。

1. **ソリューション エクスプローラー**でソリューションを右クリックし、[**NuGet パッケージの管理**] を選んで、`Azure.AI.TextAnalytics` ライブラリをインストールします。 開いたパッケージ マネージャーで [**参照**] を選び、次のライブラリを検索して、[**インストール**] を選びます。

2. 次のディレクティブを自分の `program.cs` ファイルの先頭に追加します。

   C#

   ```
   using Azure.AI.TextAnalytics;
   ```

3. 次のコード サンプルをアプリケーションに追加します。

   C#

   ```
   // Example method for extracting named entities from text
   private static void EntityRecognitionExample(string keySecret, string
   endpointSecret)
   {
       //String to be sent for Named Entity Recognition
       var exampleString = "I had a wonderful trip to Seattle last week.";

       AzureKeyCredential azureKeyCredential = new
   AzureKeyCredential(keySecret);
       Uri endpoint = new Uri(endpointSecret);
   ```

```
    var languageServiceClient = new TextAnalyticsClient(endpoint,
azureKeyCredential);

    Console.WriteLine($"Sending a Named Entity Recognition (NER)
request");
    var response =
languageServiceClient.RecognizeEntities(exampleString);
    Console.WriteLine("Named Entities:");
    foreach (var entity in response.Value)
    {
        Console.WriteLine($"\tText: {entity.Text},\tCategory:
{entity.Category},\tSub-Category: {entity.SubCategory}");
        Console.WriteLine($"\t\tScore:
{entity.ConfidenceScore:F2},\tLength: {entity.Length},\tOffset:
{entity.Offset}\n");
    }
}
```

4. キーとエンドポイントの値を使って、main メソッドから `EntityRecognitionExample()` を呼び出す次のコードを追加します。

```
C#

EntityRecognitionExample(keySecret.Value.Value,
endpointSecret.Value.Value);
```

5. アプリケーションを実行します。

次のステップ

- Azure Key Vault と共に開発できる使用可能な機能については、「Azure AI サービスとは」をご覧ください。
- セキュリティで保護されたアプリケーション開発について詳しくは、以下をご覧ください。
  - Azure Key Vault を使用するためのベスト プラクティス
  - Azure AI サービスのセキュリティ
  - Azure AI サービス用の Azure セキュリティ ベースライン

Azure AI サービスのデータ損失防止を構成する

[アーティクル] • 2024/01/09

お客様は、Azure AI サービスのデータ損失防止機能を使用して、自分の Azure AI サービス リソースがアクセスを許可されている送信 URL の一覧を構成できます。 これにより、お客様がデータ損失を防止するための別のレベルのコントロールが作成されます。 この記事では、Azure AI サービス リソースに対してデータ損失防止機能を有効にするために必要な手順について説明します。

前提条件

要求を行うには、Azure アカウントと Azure AI サービス サブスクリプションが必要になります。 既にアカウントをお持ちの場合は、次のセクションまでスキップして進んでください。 アカウントをお持ちでない場合は、数分で設定を行えるガイドをご覧ください。「マルチサービス リソースの作成」を参照してください。

アカウントの作成 後に、Azure portal からサブスクリプション キーを取得できます。

データ損失防止の有効化

データ損失防止の有効化には 2 つの部分があります。 最初に、プロパティ restrictOutboundNetworkAccess を true に設定する必要があります。 これを true に設定するときは、承認済み URL の一覧も指定する必要があります。 その URL の一覧が、allowedFqdnList プロパティに追加されます。 allowedFqdnList プロパティには、コンマ区切りの URL の配列が格納されます。

> **注意**
>
> - `allowedFqdnList` プロパティ値では最大 1000 個の URL がサポートされます。
> - このプロパティでは、IP アドレスと完全修飾ドメイン名 (例: `www.microsoft.com` 値) の両方がサポートされます。
> - 更新が有効になるまで、最大で 15 分かかる可能性があります。

Azure CLI

1. Azure CLI をインストールしてサインインするか、 **[使ってみる]** を選択します。

2. Azure AI サービス リソースの詳細を表示します。

   Azure CLI

   ```
   az cognitiveservices account show \
       -g "myresourcegroup" -n "myaccount" \
   ```

3. Azure AI サービス リソースの現在のプロパティを表示します。

   Azure CLI

   ```
   az rest -m get \
       -u /subscriptions/{subscription ID}}/resourceGroups/{resource
   group}/providers/Microsoft.CognitiveServices/accounts/{account
   name}}?api-version=2021-04-30 \
   ```

4. restrictOutboundNetworkAccess プロパティを構成し、許可されている FqdnList を承認済み URL で更新します。

   Azure CLI

   ```
   az rest -m patch \
       -u /subscriptions/{subscription ID}}/resourceGroups/{resource
   group}/providers/Microsoft.CognitiveServices/accounts/{account
   name}}?api-version=2021-04-30 \
       -b '{"properties": { "restrictOutboundNetworkAccess": true,
   "allowedFqdnList": [ "microsoft.com" ] }}'
   ```

サポートされているサービス

データ損失防止の構成は次のサービスでサポートされています。

- Azure OpenAI
- Azure AI Vision
- Content Moderator
- Custom Vision
- Face
- Document Intelligence
- Speech Service

- QnA Maker

制限事項

独自のデータに基づく Azure OpenAI - テキスト機能では、データ損失防止はまだサポートされていません。 `restrictOutboundNetworkAccess` が true に設定されている場合、次の API に対するすべての要求は、データ損失の可能性を防ぐために直ちに失敗します。

- /extensions/chat/completions (テキスト モデルを使用)
- /extensions/on-your-data/ingestion-jobs

次のステップ

- 仮想ネットワークを構成する

Cognitive Services の Azure セキュリティ ベースライン

[アーティクル] • 2023/12/12

このセキュリティ ベースラインは、 Microsoft クラウド セキュリティ ベンチマーク バージョン 1.0 のガイダンスを Cognitive Services に適用します。 Microsoft クラウド セキュリティ ベンチマークでは、Azure 上のクラウド ソリューションをセキュリティで保護する方法に関する推奨事項が提供されます。 コンテンツは、Microsoft クラウド セキュリティ ベンチマークと Cognitive Services に適用される関連ガイダンスによって定義されたセキュリティコントロールによってグループ化されます。

このセキュリティ ベースラインとその推奨事項は、Microsoft Defender for Cloud を使用して監視できます。 Azure Policy定義は、[クラウド ポータルのMicrosoft Defender] ページの [規制コンプライアンス] セクションに一覧表示されます。

機能に関連するAzure Policy定義がある場合は、Microsoft クラウド セキュリティ ベンチマークの制御と推奨事項への準拠を測定するのに役立つ、このベースラインに一覧表示されます。 一部の推奨事項では、特定のセキュリティ シナリオを有効にするために有料Microsoft Defenderプランが必要になる場合があります。

> **注意**
>
> Cognitive Services に適用されない**機能**は除外されています。 Cognitive Services が Microsoft クラウド セキュリティ ベンチマークに完全にマップされる方法については、 **完全な Cognitive Services セキュリティ ベースライン マッピング ファイル** を参照してください。

セキュリティ プロファイル

セキュリティ プロファイルは、Cognitive Services の影響が大きい動作をまとめたものです。これにより、セキュリティに関する考慮事項が高まる可能性があります。

テーブルを展開する

サービス動作属性	値
製品カテゴリ	AI + ML
お客様は HOST/OS にアクセスできます	アクセス権なし

サービス動作属性	値
サービスは顧客の仮想ネットワークにデプロイできます	False
顧客のコンテンツを保存する	True

ネットワークのセキュリティ

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: ネットワーク セキュリティ」を参照してください。

NS-1: ネットワーク セグメント化の境界を確立する

機能

Virtual Network 統合

説明: サービスは、顧客のプライベート Virtual Network (VNet) へのデプロイをサポートします。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

ネットワーク セキュリティ グループのサポート

説明: サービス ネットワーク トラフィックは、サブネット上のネットワーク セキュリティ グループルールの割り当てを尊重します。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

機能ノート: このサービスのネットワーク セキュリティ グループはサポートされていませんが、サービス レベルのファイアウォールを構成できます。 詳細については、「IP ネットワーク規則の管理」を参照してください。

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

NS-2: ネットワーク制御を使用してクラウド サービスをセキュリティで保護する

機能

Azure Private Link

説明: ネットワーク トラフィックをフィルター処理するためのサービス ネイティブ IP フィルタリング機能 (NSG やAzure Firewallと混同しないように)。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Private Link機能をサポートするすべての Azure リソースのプライベート エンドポイントをデプロイして、リソースのプライベート アクセス ポイントを確立します。

リファレンス: プライベート エンドポイントを使用する

パブリック ネットワーク アクセスの無効化

説明: サービスでは、サービス レベルの IP ACL フィルター規則 (NSG またはAzure Firewallではなく) または [パブリック ネットワーク アクセスの無効化] トグル スイッチを使用して、パブリック ネットワーク アクセスを無効にできます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: サービス レベルの IP ACL フィルタリング規則またはパブリック ネットワーク アクセス用の切り替えスイッチを使用して、パブリック ネットワーク アクセスを無効にします。

リファレンス: 既定のネットワーク アクセス規則を変更する

Microsoft Defender for Cloud による監視

Azure Policy組み込み定義 - Microsoft.CognitiveServices:

テーブルを展開する

名前 (Azure portal)	説明	効果	Version (GitHub)
Cognitive Services アカウントでパブリック ネットワーク アクセスを無効にする必要がある	Cognitive Services アカウントのセキュリティを強化するには、パブリック インターネットに公開されないようにして、プライベート エンドポイントからのみアクセスできるようにします。 https://go.microsoft.com/fwlink/?linkid=2129800 の説明に従って、公衆ネットワーク アクセス プロパティを無効にします。 このオプションにより、Azure IP 範囲外のパブリック アドレス空間からのアクセスが無効になり、IP または仮想ネットワークベースのファイアウォール規則に一致するすべてのログインが拒否されます。 これにより、データ漏洩のリスクが軽減されます。	Audit、Deny、Disabled	3.0.1
Cognitive Services アカウントでネットワーク アクセスを制限する必要がある	Cognitive Services アカウントに対するネットワーク アクセスは、制限する必要があります。 許可されているネットワークのアプリケーションのみが Cognitive Services アカウントにアクセスできるように、ネットワーク ルールを構成します。 特定のインターネットまたはオンプレミスのクライアントからの接続を許可するため、特定の Azure 仮想ネットワークからのトラフィックまたはパブリック インターネット IP アドレス範囲に、アクセス権を付与できます。	Audit、Deny、Disabled	3.0.0
Cognitive Services ではプライベート リンクを使用する必要がある	Azure Private Link を使用すると、接続元または接続先にパブリック IP アドレスを使用せずに、仮想ネットワークを Azure サービスに接続できます。 Private Link プラットフォームでは、Azure のバックボーン ネットワークを介してコンシューマーとサービスの間の接続が処理されます。 プライベート エンドポイントを Cognitive Services にマッピングすることにより、データ漏えいの可能性を減らすことができます。 プライベート リンクの詳細については、https://go.microsoft.com/fwlink/?linkid=2129800 を参照してください。	Audit、Disabled	3.0.0

ID 管理

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: *ID* 管理」を参照してください。

IM-1: 一元的な ID および認証システムを使用する

機能

データ プレーン アクセスに必要な Azure AD Authentication

説明: サービスでは、データ プレーン アクセスに Azure AD 認証を使用できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: 既定の認証方法として Azure Active Directory (Azure AD) を使用して、データ プレーンへのアクセスを制御します。

リファレンス: Azure Active Directory で認証する

データ プレーン アクセスのローカル認証方法

説明: ローカルユーザー名やパスワードなど、データ プレーンアクセスでサポートされるローカル認証方法。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

機能ノート: 単一サービスまたはマルチサービスのサブスクリプション キーを使用して Azure Cognitive Services に対して認証を行ったり、これらのキーを使用してアクセス トークンで認証したりできますが、これらの認証方法は、Azure ロールベースのアクセス制御 (Azure RBAC) を必要とするより複雑なシナリオでは不足しています。 ローカル認証方法またはアカウントの使用は避けてください。これらは可能な限り無効にする必要があります。 代わりに、Azure AD を使用して、可能な限り認証を行います。

構成ガイダンス: データ プレーン へのアクセスに対するローカル認証方法の使用を制限します。 代わりに、データ プレーン アクセスを制御するための既定の認証方法として、Azure Active Directory (Azure AD) を使います。

リファレンス: アクセス トークンを使用して認証する

Microsoft Defender for Cloud による監視

Azure Policy組み込み定義 - Microsoft.CognitiveServices:

テーブルを展開する

名前 (Azure portal)	説明	効果	Version (GitHub)
Cognitive Services アカウントでは、ローカル認証方法を無効にする必要がある	ローカル認証方法を無効にすると、Cognitive Services アカウントで Azure Active Directory ID を認証専用で求めることにより、セキュリティが向上します。 詳細については、https://aka.ms/cs/auth を参照してください。	Audit、Deny、Disabled	1.0.0

IM-3: アプリケーション ID を安全かつ自動的に管理する

機能

マネージド ID

説明: データ プレーン アクションは、マネージド ID を使用した認証をサポートします。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: 可能な場合は、サービス プリンシパルではなく Azure マネージド ID を使用します。これは、Azure Active Directory (Azure AD) 認証をサポートする Azure サービスとリソースに対して認証できます。 マネージド ID の資格情報は、プラットフォームによって完全に管理、ローテーション、保護されており、ソース コードまたは構成ファイル内でハードコーディングされた資格情報を使用せずに済みます。

リファレンス: マネージド ID へのアクセスを承認する

サービス プリンシパル

説明: データ プレーンでは、サービス プリンシパルを使用した認証がサポートされています。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: この機能の構成に関する現在の Microsoft ガイダンスはありません。organizationがこのセキュリティ機能を構成する必要があるかどうかを確認して判断してください。

リファレンス: Azure Cognitive Services への要求を認証する

IM-7: 条件に基づいてリソースへのアクセスを制限する

機能

データ プレーンへの条件付きアクセス

説明: データ プレーンアクセスは、Azure AD 条件付きアクセス ポリシーを使用して制御できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: ワークロード内の Azure Active Directory (Azure AD) 条件付きアクセスに適用できる条件と条件を定義します。 特定の場所からのアクセスのブロックや許可、危険なサインイン動作のブロック、特定のアプリケーションに対するorganizationマネージド デバイスの要求など、一般的なユース ケースを検討してください。

IM-8: 資格情報とシークレットの公開を制限する

機能

Azure Key Vault での、サービス資格情報とシークレットの統合とストレージのサポート

説明: データ プレーンでは、資格情報とシークレット ストアに対する Azure Key Vault のネイティブな使用がサポートされています。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: シークレットと資格情報は、コードファイルや構成ファイルに埋め込むのではなく、Azure Key Vault などのセキュリティで保護された場所に格納されていることを確認します。

リファレンス: Key Vaultを使用して Azure Cognitive Services アプリケーションを開発する

特権アクセス

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: 特権アクセス」を参照してください。

PA-1: 高い特権を持つ/管理者ユーザーを分離して制限する

機能

ローカル 管理 アカウント

説明: サービスには、ローカル管理アカウントの概念があります。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

PA-7: Just Enough Administration (最小限の特権の原則) に従う

機能

Azure RBAC for Data Plane

説明: Azure Role-Based Access Control (Azure RBAC) を使用して、サービスのデータ プレーン アクションへのアクセスを管理できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: 組み込みのロールの割り当てを使用して Azure リソース アクセスを管理するには、Azure ロールベースのアクセス制御 (Azure RBAC) を使用します。 Azure RBAC ロールは、ユーザー、グループ、サービス プリンシパル、マネージド ID に割り当てることができます。

リファレンス: Azure Active Directory で認証する

PA-8: クラウド プロバイダー サポートのアクセス プロセスを決定する

機能

カスタマー ロックボックス

説明: カスタマー ロックボックスは、Microsoft サポート へのアクセスに使用できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Microsoft がデータにアクセスする必要があるサポート シナリオでは、カスタマー ロックボックスを使用して確認し、Microsoft の各データ アクセス要求を承認または拒否します。

データの保護

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: データ保護」を参照してください。

DP-1:機密データを検出、分類、ラベル付けする

機能

機密データの検出と分類

説明: ツール (Azure Purview や Azure Information Protection など) は、サービスでのデータの検出と分類に使用できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

DP-2: 機密データをターゲットにした異常と脅威を監視する

機能

データ漏えい/損失防止

説明: サービスでは、機密データの移動 (顧客のコンテンツ内) を監視するための DLP ソリューションがサポートされています。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Cognitive Services データ損失防止機能を使用すると、Cognitive Services リソースがアクセスできる送信 URL の一覧を構成できます。 これにより、お客様がデータ損失を防止するための別のレベルのコントロールが作成されます。

リファレンス: Azure Cognitive Services のデータ損失防止を構成する

DP-3: 転送中の機密データの暗号化

機能

転送中データの暗号化

説明: サービスでは、データ プレーンの転送中のデータ暗号化がサポートされています。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	True	Microsoft

構成ガイダンス: 既定のデプロイでこれが有効になっているので、追加の構成は必要ありません。

リファレンス: Azure Cognitive Services のセキュリティ

DP-4: 保存データ暗号化を既定で有効にする

機能

プラットフォーム キーを使用した保存データの暗号化

説明: プラットフォーム キーを使用した保存データの暗号化がサポートされています。保存中の顧客コンテンツは、これらの Microsoft マネージド キーで暗号化されます。詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	True	Microsoft

構成ガイダンス: 既定のデプロイでこれが有効になっているので、追加の構成は必要ありません。

リファレンス: Cognitive Services 用の Azure Key Vaultを使用してカスタマー マネージド キーを構成する

DP-5: 必要に応じて保存データ暗号化でカスタマー マネージド キー オプションを使用する

機能

CMK を使用した保存データの暗号化

説明: カスタマー マネージド キーを使用した保存データの暗号化は、サービスによって格納される顧客コンテンツでサポートされています。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: 規制コンプライアンスに必要な場合は、カスタマー マネージド キーを使用した暗号化が必要なユース ケースとサービス スコープを定義します。 それらのサービスでカスタマー マネージド キーを使って、保存データ暗号化を有効にして実装します。

リファレンス: Cognitive Services 用の Azure Key Vaultを使用してカスタマー マネージド キーを構成する

Microsoft Defender for Cloud による監視

Azure Policy組み込み定義 - Microsoft.CognitiveServices:

テーブルを展開する

名前 (Azure portal)	説明	効果	Version (GitHub)
Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	規制コンプライアンス標準を満たすには、一般にカスタマー マネージド キーが必要です。 カスタマー マネージド キーを使用すると、自分が作成して所有する Azure Key Vault キーを使用して、Cognitive Services に格納されているデータを暗号化できます。 ローテーションや管理など、キーのライフサイクルを完全に制御し、責任を負うことになります。 カスタマー マネージド キーの詳細については、https://go.microsoft.com/fwlink/?linkid=2121321 をご覧ください。	Audit、Deny、Disabled	2.1.0

DP-6: セキュア キー管理プロセスの使用

機能

Azure Key Vault でのキー管理

説明: このサービスでは、カスタマー キー、シークレット、または証明書に対する Azure Key Vault統合がサポートされています。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Azure Key Vaultを使用して、キーの生成、配布、ストレージなど、暗号化キーのライフ サイクルを作成および制御します。 定義されたスケジュールに基づいて、またはキーの廃止や侵害が発生した場合に、Azure Key Vault とサービスのキーをローテーションして取り消します。 ワークロード、サービス、またはアプリケーション レベルでカスタマー マネージド キー (CMK) を使用する必要がある場合は、キー管理のベスト プラクティスに従ってください。キー階層を使用して、キー コンテナーにキー暗号化キー (KEK) を使用して別のデータ暗号化キー (DEK) を生成します。 キーが Azure Key Vaultに登録され、サービスまたはアプリケーションのキー ID を介して参照されていることを確認します。 独自のキー (BYOK) をサービスに持ち込む必要がある場合 (オンプレミスの HSM から Azure Key Vaultに HSM で保護されたキーをインポートする場合など)、初期キーの生成とキー転送を実行するための推奨ガイドラインに従ってください。

リファレンス: Cognitive Services 用の Azure Key Vaultを使用してカスタマー マネージド キーを構成する

DP-7: セキュリティで保護された証明書管理プロセスを使用する

機能

Azure Key Vault での証明書管理

説明: このサービスでは、顧客証明書に対する Azure Key Vault統合がサポートされます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

アセット管理

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: 資産管理」を参照してください。

AM-2: 承認済みのサービスのみを使用する

機能

Azure Policy のサポート

説明: サービス構成は、Azure Policy経由で監視および適用できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Microsoft Defender for Cloud を使用して、Azure リソースの構成を監査および適用するAzure Policyを構成します。 Azure Monitor を使用し、リソースで構成の逸脱が検出されたときにアラートを作成します。 [deny] と [deploy if not exists] 効果Azure Policy使用して、Azure リソース全体でセキュリティで保護された構成を適用します。

リファレンス: Azure Cognitive Services の組み込みポリシー定義をAzure Policyする

ログと脅威検出

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: ログ記録と脅威検出」を参照してください。

LT-1: 脅威検出機能を有効にする

機能

サービス/製品のオファリングのための Microsoft Defender

説明: サービスには、セキュリティの問題を監視およびアラートするためのオファリング固有のMicrosoft Defender ソリューションがあります。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

LT-4: セキュリティ調査のためのログを有効にする

機能

Azure リソース ログ

説明: サービスは、サービス固有のメトリックとログ記録を強化できるリソース ログを生成します。 お客様はこれらのリソース ログを構成し、ストレージ アカウントやログ分析ワークスペースなどの独自のデータ シンクに送信できます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: サービスのリソース ログを有効にします。 たとえば、Key Vaultでは、キー コンテナーからシークレットを取得するアクションや、データベースへの要求を追跡するリソース ログがAzure SQLされるアクションに対して、追加のリソース ログがサポートされます。 リソース ログの内容は、Azure サービスとリソースの種類によって異なります。

リファレンス: Azure Cognitive Services の診断ログを有効にする

バックアップと回復

詳細については、「*Microsoft* クラウド セキュリティ ベンチマーク: バックアップと回復」を参照してください。

BR-1:定期的な自動バックアップを保証する

機能

Azure Backup

説明: サービスは、Azure Backup サービスによってバックアップできます。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

サービス ネイティブ バックアップ機能

説明: サービスでは、独自のネイティブ バックアップ機能がサポートされます (Azure Backupを使用していない場合)。 詳細については、こちらを参照してください。

テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

次の手順

- Microsoft クラウド セキュリティ ベンチマークの概要を参照してください
- Azure セキュリティ ベースラインの詳細について学習する

Azure AI サービス用の Azure Policy 規制コンプライアンス コントロール

[アーティクル] • 2024/04/13

Azure Policy の規制コンプライアンスにより、さまざまなコンプライアンス基準に関連する**コンプライアンス ドメイン**および**セキュリティ コントロール**に対して、"組み込み" と呼ばれる、Microsoft が作成および管理するイニシアチブ定義が提供されます。 このページでは、Azure AI サービス用の**コンプライアンス ドメイン**と**セキュリティ コントロール**の一覧を示します。 **セキュリティ コントロール**の組み込みを個別に割り当てることで、Azure リソースを特定の基準に準拠させることができます。

各組み込みポリシー定義のタイトルは、Azure portal のポリシー定義にリンクしています。 **[ポリシーのバージョン]** 列のリンクを使用すると、Azure Policy GitHub リポジトリのソースを表示できます。

> **重要**
>
> 各コントロールは、1 つ以上の **Azure Policy** 定義に関連付けられています。 これらのポリシーは、コントロールの**コンプライアンスの評価**に役立つ場合があります。 ただし、多くの場合、コントロールと 1 つ以上のポリシーとの間には、一対一、または完全な一致はありません。 そのため、Azure Policy での**準拠**は、ポリシー自体のみを指しています。 これによって、コントロールのすべての要件に完全に準拠していることが保証されるわけではありません。 また、コンプライアンス標準には、現時点でどの Azure Policy 定義でも対応されていないコントロールが含まれています。 したがって、Azure Policy でのコンプライアンスは、全体のコンプライアンス状態の部分的ビューでしかありません。 これらのコンプライアンス標準に対するコントロールと Azure Policy 規制コンプライアンス定義の間の関連付けは、時間の経過と共に変わることがあります。

CMMC レベル 3

すべての Azure サービスで使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy の規制コンプライアンス - CMMC レベル 3 に関する記事をご覧ください。 このコンプライアンス標準の詳細については、サイバーセキュリティ成熟度モデル認定 (CMMC) に関するドキュメントをご覧ください。

テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC.1.001	情報システムへのアクセスを、許可されているユーザー、許可されているユーザーの代わりに動作するプロセス、およびデバイス (他の情報システムを含む) に制限する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
アクセス制御	AC.1.002	情報システムへのアクセスを、許可されているユーザーが実行を許可されているトランザクションおよび機能の種類に制限する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
アクセス制御	AC.2.016	承認された認可に従って CUI のフローを制御する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
構成管理	CM.3.068	不要なプログラム、関数、ポート、プロトコル、およびサービスの使用を制限、無効化、または禁止する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC.1.175	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織システムによって送受信される情報) を監視、制御、および保護する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC.3.177	CUI の機密性を保護するために使用する場合は、FIPS 検証済みの暗号化を採用する。	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0
システムと通信の保護	SC.3.183	ネットワーク通信トラフィックを既定で拒否し、ネットワーク通信トラフィックを例外的に許可する (つまり、すべて拒否し、例外的に許可する)。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0

FedRAMP High

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy の規制コンプライアンス - FedRAMP High に関するページを参照してください。 このコンプライアンス標準の詳細については、FedRAMP High に関するページを参照してください。

テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (7)	ロールベースのスキーム	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
アクセス制御	AC-4	情報フローの適用	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17	リモート アクセス	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17 (1)	監視または制御の自動化	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
識別と認証	IA-2	識別と認証 (組織のユーザー)	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
システムと通信の保護	SC-7	境界保護	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-12	暗号化キーの確立と管理	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

FedRAMP Moderate

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy の規制コンプライアンス - FedRAMP Moderate に関するページを参照してください。 このコンプライアンス標準の詳細については、FedRAMP Moderate に関するページを参照してください。

テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (7)	ロールベースのスキーム	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
アクセス制御	AC-4	情報フローの適用	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17	リモート アクセス	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17 (1)	監視または制御の自動化	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
識別と認証	IA-2	識別と認証 (組織のユーザー)	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7	境界保護	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-12	暗号化キーの確立と管理	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

Microsoft クラウド セキュリティ ベンチマーク

Microsoft クラウド セキュリティ ベンチマークでは、Azure 上のクラウド ソリューションをセキュリティで保護する方法に関する推奨事項が提供されます。 このサービスを完全に Microsoft クラウド セキュリティ ベンチマークにマップする方法については、「Azure Security Benchmark mapping files」 (Azure セキュリティ ベンチマークのマッピング ファイル) を参照してください。

すべての Azure サービスに対して使用可能な Azure Policy 組み込みを、このコンプライアンス基準に対応させる方法については、Azure Policy の規制コンプライアンス - Microsoft クラウド セキュリティ ベンチマークに関するページを参照してください。

テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
ネットワークのセキュリティ	NS-2	ネットワーク制御を使用してクラウド サービスをセキュリティで保護します	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
ネットワークのセキュリティ	NS-2	ネットワーク制御を使用してクラウド サービスをセキュリティで保護します	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
ID 管理	IM-1	一元的な ID および認証システムを使用する	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
データ保護	DP-5	必要に応じて保存データ暗号化でカスタマー マネージド キー オプションを使用する	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

NIST SP 800-171 R2

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy の規制コンプライアンス - NIST SP 800-171 R2 に関するページを参照してください。 このコンプライアンス標準の詳細については、NIST SP 800-171 R2 に関するページを参照してください。

テーブルを展開する

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	3.1.1	承認されているユーザー、承認されているユーザーの代わりに動作するプロセス、およびデバイス (他のシステムを含む) へのシステム アクセスを制限する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	3.1.1	承認されているユーザー、承認されているユーザーの代わりに動作するプロセス、およびデバイス (他のシステムを含む) へのシステム アクセスを制限する。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	3.1.12	リモート アクセス セッションの監視および制御を行う。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	3.1.13	リモート アクセス セッションの機密性を保護するため暗号化メカニズムを採用する。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	3.1.14	管理対象のアクセス制御ポイントを介してリモート アクセスをルーティングする。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	3.1.2	システム アクセスを、許可されたユーザーが実行を許可されているトランザクションおよび機能の種類に限定する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	3.1.3	承認された認可に従って CUI のフローを制御する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
アクセス制御	3.1.3	承認された認可に従って CUI のフローを制御する。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	3.13.1	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織システムによって送受信される情報) を監視、制御、および保護する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システム	3.13.1	組織システムの外部境界と主要な内部境界で、通信 (つまり、組	Cognitive Services ではプライベート リンクを使用する	3.0.0

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
と通信の保護		織システムによって送受信される情報) を監視、制御、および保護する。	必要がある	
システムと通信の保護	3.13.10	組織のシステムで採用されている暗号化の暗号化キーを確立し、管理する。	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0
システムと通信の保護	3.13.2	組織のシステム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発手法、システム エンジニアリングの原則を採用する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	3.13.2	組織のシステム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発手法、システム エンジニアリングの原則を採用する。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	3.13.5	内部ネットワークから物理的または論理的に分離されている、公的にアクセス可能なシステム コンポーネントのサブネットワークを実装する。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	3.13.5	内部ネットワークから物理的または論理的に分離されている、公的にアクセス可能なシステム コンポーネントのサブネットワークを実装する。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	3.13.6	ネットワーク通信トラフィックを既定で拒否し、ネットワーク通信トラフィックを例外的に許可する (つまり、すべて拒否し、例外的に許可する)。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
識別と認証	3.5.1	システム ユーザー、ユーザーの代わりに動作するプロセス、およびデバイスを特定する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
識別と認証	3.5.2	組織システムへのアクセスを許可するための前提条件として、ユーザー、プロセス、またはデバイスの ID を認証 (または検証) する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	3.5.5	定義された期間、識別子の再利用を防止する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	3.5.6	定義された非アクティブな期間の経過後に識別子を無効にする。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0

NIST SP 800-53 Rev. 4

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy の規制コンプライアンス - NIST SP 800-53 Rev. 4 に関するページを参照してください。 このコンプライアンス標準の詳細については、NIST SP 800-53 Rev. 4 に関するページを参照してください。

テーブルを展開する

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (7)	ロールベースのスキーム	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ロー	1.1.0

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
			カル認証を無効にする)	
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.2.0
アクセス制御	AC-4	情報フローの適用	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17	リモート アクセス	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17 (1)	監視または制御の自動化	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
識別と認証	IA-2	識別と認証 (組織のユーザー)	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7	境界保護	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-12	暗号化キーの確立と管理	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

NIST SP 800-53 Rev. 5

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy の規制コンプライアンス - NIST SP 800-53 Rev. 5 に関するページを参照してください。 このコンプライアンス標準の詳細については、NIST SP 800-53 Rev. 5 に関するページを参照してください。

テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-2 (7)	特権ユーザー アカウント	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
アクセス制御	AC-4	情報フローの適用	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17	リモート アクセス	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
アクセス制御	AC-17 (1)	監視および制御	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
識別と認証	IA-2	識別と認証 (組織のユーザー)	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7	境界保護	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
システムと通信の保護	SC-12	暗号化キーの確立と管理	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

NL BIO Cloud Theme

すべての Azure サービスで使用可能な Azure Policy の組み込みがこのコンプライアンス標準にどのように対応しているのかを確認するには、「NL BIO Cloud Theme に関する Azure Policy の規制コンプライアンスの詳細」を参照してください。 このコンプライアンス標準の詳細については、「ベースライン情報セキュリティ政府サイバーセキュリティ - デジタル政府 (digitaleoverheid.nl)」を参照してください。

テーブルを展開する

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
U.05.2 データ保護 - 暗号化対策	U.05.2	クラウド サービスに格納されているデータは、最先端の技術で保護されます。	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0
U.07.1 データの分離 - 分離	U.07.1	データの永続的な分離は、マルチテナント アーキテクチャの 1 つです。 パッチは制御された方法で実現されます。	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
U.07.1 データの分離 - 分離	U.07.1	データの永続的な分離は、マルチテナント アーキテクチャの 1 つです。 パッチは制御された方法で実現されます。	Cognitive Services ではプライベート リンクを使用する必要がある	3.0.0
U.07.3 データの分離 - 管理機能	U.07.3	U.07.3 - CSC データおよび/または暗号化キーを表示あるいは変更する権限は、制御された方法で付与され、使用状況がログに記録されます。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
U.10.2 IT サービスとデータへのアクセス - ユーザー	U.10.2	CSP の責任の下、アクセス権が管理者に付与されます。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
U.10.3 IT サービスとデータへのアクセス - ユーザー	U.10.3	IT サービスとデータにアクセスできるのは、認証された機器を持つユーザーだけです。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
U.10.5 IT サービスとデータへのアクセス - 適格性	U.10.5	IT サービスとデータへのアクセスは技術的な手段によって制限され、実装されています。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
U.11.3 暗号化サービス - 暗号化	U.11.3	機密データは、CSC によって管理される秘密キーを使用して常に暗号化されます。	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

インド準備銀行の銀行向けの IT フレームワーク v2016

すべての Azure サービスで使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、Azure Policy 規制コンプライアンス -

RBI ITF Banks v2016 に関する記事を参照してください。 このコンプライアンス標準の詳細については、RBI ITF Banks v2016 (PDF) を参照してください。

テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
フィッシング詐欺対策		フィッシング詐欺対策-14.1	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.2.0
メトリック		メトリック-21.1	Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	2.1.0

次のステップ

- Azure Policy の規制コンプライアンスの詳細を確認します。
- Azure Policy GitHub リポジトリのビルトインを参照します。

Azure AI サービスにおける AI の責任ある使用

[アーティクル] • 2024/01/20

Azure AI サービスは、アプリケーションで人工知能を責任ある方法で使用するための情報とガイドラインを提供します。 Azure AI サービス スイート内のさまざまなサービスについて、このガイダンスを提供する記事へのリンクを下に示します。

Anomaly Detector

- 透過性に関するメモとユースケース
- データ、プライバシー、セキュリティ

Azure AI Vision - OCR

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

Azure AI Vision - 画像分析

- わかりやすさに関するメモ
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ
- 制限付きアクセス機能

Azure AI Vision - Face

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ
- 制限付きアクセス機能

Azure AI Vision - 空間分析

- 透過性に関するメモとユースケース
- AI デプロイでの責任ある使用
- 開示設計のガイドライン
- リサーチの分析情報
- データ、プライバシー、セキュリティ

Custom Vision

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語サービス

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - カスタム テキスト分類

- わかりやすさに関するメモ
- 統合と責任ある使用
- 特性と制限
- データ、プライバシー、セキュリティ

言語 - 名前付きエンティティの認識

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - カスタム固有表現認識

- わかりやすさに関するメモ
- 統合と責任ある使用
- 特性と制限
- データ、プライバシー、セキュリティ

言語 - エンティティ リンク

- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - 言語検出

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - キー フレーズ抽出

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - 個人を特定できる情報 (PII) の検出

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - 質問応答

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - 感情分析とオピニオン マイニング

- わかりやすさに関するメモ
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - Text Analytics for Health

- わかりやすさに関するメモ

- 統合と責任ある使用
- データ、プライバシー、セキュリティ

言語 - 概要作成

- わかりやすさに関するメモ
- 統合と責任ある使用
- 特性と制限
- データ、プライバシー、セキュリティ

Language Understanding

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

Azure OpenAI Service

- わかりやすさに関するメモ
- 制限付きアクセス
- 倫理規定
- データ、プライバシー、セキュリティ

Personalizer

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データとプライバシー

QnA Maker

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

Speech - 発音評価を使用する

- 透過性に関するメモとユースケース
- 特性と制限

Speech - Speaker Recognition

- 透過性に関するメモとユースケース
- 特性と制限
- 制限付きアクセス
- 一般的なガイドライン
- データ、プライバシー、セキュリティ

Speech - カスタム ニューラル音声

- 透過性に関するメモとユースケース
- 特性と制限
- 制限付きアクセス
- 合成音声の責任あるデプロイ
- ボイス タレントの開示
- ガイドライン設計の開示
- 設計パターンの開示
- 倫理規定
- データ、プライバシー、セキュリティ

Speech - テキスト読み上げ

- 透過性に関するメモとユースケース

Speech - 音声テキスト変換

- 透過性に関するメモとユースケース
- 特性と制限
- 統合と責任ある使用
- データ、プライバシー、セキュリティ

Azure AI サービスの制限付きアクセス機能

[アーティクル] • 2024/02/27

Microsoft が目指しているのは、AI を利用して社会を良い方向に変革する開発者や組織の力になることです。 個人の権利や安全を守るために、私たちは責任ある AI のプラクティスを奨励しています。 その実現に向け Microsoft は、Azure サービスの責任あるデプロイを支援するための、AI の原則 に基づく制限付きアクセス ポリシーを導入しました。

制限付きアクセスとは

制限付きアクセス サービスには登録が必要です。Microsoft の管理下にある (つまり Microsoft アカウント チームと直接連携する) お客様だけに利用資格が与えられます。 これらのサービスの使用は、登録時点で選択されたユース ケースに限定されます。 お客様には、サービス使用条件に目を通したこと、またそれらに同意することへの確認が必要となります。 Microsoft では、お客様にこの情報の再確認を求める場合があります。

制限付きアクセス サービスは、Microsoft Azure サービスのサブスクリプションを規定する条項 (including the サービス固有の条件 を含む) の下でお客様に提供されます。 制限付きアクセス サービスの使用に関する重要な条件と義務が含まれているので、これらの条項をよくお読みください。

制限付きアクセス サービスの一覧

アクセスが制限されているサービスは次のとおりです。

- カスタム ニューラル音声: Pro の機能
- カスタム テキスト読み上げアバター: すべての機能
- 話者認識: すべての機能
- Face API: 識別および検証の機能、顔 ID プロパティ
- Azure AI Vision: 著名人認識機能
- Azure AI Video Indexer: 著名人認識と顔識別の機能
- Azure OpenAI: Azure OpenAI Service、変更された不正使用の監視、および変更されたコンテンツ フィルター

これらのサービスのうち上に記載されていない機能は、登録なしでご利用いただけます。

制限付きアクセスに関する FAQ

アクセスの登録方法を教えてください。

使用を希望する制限付きアクセス サービスごとに登録フォームを送信してください。

- カスタム ニューラル音声: Pro の機能
- カスタム テキスト読み上げアバター: すべての機能
- 話者認識: すべての機能
- Face API: 識別および検証の機能
- Azure AI Vision: 著名人認識機能
- Azure AI Video Indexer: 著名人認識と顔識別の機能
- Azure OpenAI: Azure OpenAI Service、変更された不正使用の監視、および変更されたコンテンツ フィルター

登録プロセスにはどのくらいの時間がかかりますか?

お申し込み後、5 から 10 営業日以内に審査に関するご連絡を差し上げます。 場合によっては、確認に時間がかかることがあります。 申請が審査されるとすぐにメールが届きます。

制限付きアクセスのサービスを使用する資格があるのはだれですか?

制限付きアクセス サービスは、Microsoft の管理下にあるお客様にのみ提供されます。 加えて、制限付きアクセスのサービスは特定のユース ケースに限定して提供され、お客様は登録フォームで、意図するユース ケースを選ぶ必要があります。

登録フォームには、組織に関連付けられているメール アドレスを使用してください。 個人のメール アドレスで提出された登録フォームは拒否されます。

Microsoft の管理下にないお客様については、同じフォームを使用して申請をご提出いただければ、こちらから適格プログラムへの参加機会について連絡差し上げます。

管理下の顧客とは? 管理下の顧客に該当するかどうかがわからない場合はどうすればよいですか?

管理下のお客様は、Microsoft アカウント チームと連携します。 使用を希望する機能の登録フォームをご提出ください。お客様の利用資格を確認させていただきます。 現時点では、管理下のお客様になる要求を受け入れることができません。

既に利用していて登録しなかった場合はどうなりますか?

既存のお客様は、2023 年 6 月 30 日までに登録フォームを提出し、2023 年 6 月 30 日以降、制限付きアクセス サービスの使用を継続することについての承認を得る必要があります。 審査には 10 営業日見込むことをお勧めします。 申請が認められなかった場合、2023 年 6 月 30 日を過ぎるとアクセスが拒否されます。

既にカスタム ニューラル音声や話者認識の利用申請を行って使用しているユーザーも、これらのサービスの使用を継続するためには登録が必要なのですか?

Microsoft は責任ある AI プログラムの改善を絶えず追求しており、制限付きアクセスは、Microsoft の新たなサービス制限プロセスです。 過去にカスタム ニューラル音声または話者認識の利用を申請し、許可が下りた場合でも、2023 年 6 月 30 日以降、これらのサービスの使用を継続するためには新しい登録フォームの提出をお願いいたします。

既に 2022 年 6 月 21 日の時点でカスタム ニューラル音声または話者認識を使用しているお客様が、2023 年 6 月 30 日以降も引き続きこれらのサービスを使用するためには、2023 年 6 月 30 日までに、ユース ケースを選択して登録フォームを提出し、承認される必要があります。 申請プロセスには 10 日間見込むことをお勧めします。 既存のお客様は 2023 年 6 月 30 日までは引き続きサービスをご利用いただけますが、その後は、利用申請の承認を受ける必要があります。 登録フォームは、こちらから入手できます。

- カスタム ニューラル音声: Pro の機能
- 話者認識: すべての機能

ユース ケースが登録フォームにない場合はどうなりますか?

制限付きアクセス機能は、登録フォームに記載のユース ケースに限って提供されます。 目的のユース ケースが記載されていない場合は、サービス内容改善のため、こちらのフィードバック フォームでお知らせください。

制限付きアクセス サービスはどこで使用できますか?

こちらで制限付きアクセス サービスを検索して、その提供リージョンをご確認ください。 ブラジル南部とアラブ首長国連邦北部のデータセンター リージョンでは、Microsoft が管理する法人のお客様の利用を優先しております。

カスタム ニューラル音声と話者認識の操作がサポートされているリージョンについては、こちらで詳しい情報をご覧いただけます。

申請が拒否された場合、私のデータはどうなりますか?

既存のお客様の利用申請が拒否された場合、2023 年 6 月 30 日を過ぎると、制限付きアクセスの機能は使用できなくなります。 お客様のデータには、Microsoft のデータ保有ポリシー が適用されます。

ヘルプとサポート

制限付きアクセス サービスの乱用については、こちら からご報告ください。

Azure AI SDK リファレンス

[アーティクル] • 2024/03/20

この記事では、利用可能な Azure AI クライアント ライブラリとパッケージの概要と、サービス レベルと機能レベルのリファレンス ドキュメントへのリンクについて説明します。

利用可能な Azure AI サービス

表からサービスを選択し、Azure AI が開発目標の達成にどのように役立つかを学習します。

サポートされているサービス

テーブルを展開する

サービス	説明	リファレンス ドキュメント
Azure AI Search	AI を利用したクラウド検索をモバイルおよび Web アプリで実現できます。	• Azure AI Search SDK for .NET • Azure AI Search NuGet パッケージ
Azure OpenAI	さまざまな自然言語タスクを実行します。	• Azure OpenAI SDK for .NET • Azure OpenAI NuGet パッケージ
Bot Service	ボットを作成し、それらをチャネル間で接続します。	• Bot Service SDK for .NET • Bot Builder (NuGet パッケージ)
Content Safety	アプリケーションやサービスの有害なコンテンツを検出します。	• コンテンツ セーフty SDK for .NET • コンテンツ セーフty NuGet パッケージ
Custom Vision	アプリケーションとモデルの画像認識をカスタマイズします。	• Custom Vision SDK for .NET

サービス	説明	リファレンス ドキュメン
		• Custom Vision NuGet パッケージ (予測)
		• Custom Vision NuGet パッケージ (トレーニング)
Document Intelligence	ドキュメントをインテリジェントなデータ ドリブン ソリューションに変換します。	• ドキュメント インテリジェンス SDK for .NET • ドキュメント インテリジェンス NuGet パッケージ
Face	画像内の人間の顔を検出、認識、識別します。	• Face SDK for .NET • Face NuGet パッケージ
Immersive Reader	テキストの読みやすさと理解力をユーザーに提供します。	• イマーシブ リーダー C# クイック スタート
Language	自然言語理解機能を使用してアプリケーションを構築します。	• .NET 用言語 SDK (テキスト分析) • 言語 NuGet パッケージ (テキスト分析) • Language SDK for .NET (質問への回答) • 言語 NuGet パッケージ (質問への回答)
Speech	音声テキスト変換、テキスト読み上げ、翻訳、話者認識機能をアプリケーションに追加します。	• Speech SDK for .NET • Speech NuGet パッケージ (Speech CLI)
Translator	AI を利用した翻訳テクノロジを使用して、100 を超える使用中、危険な言語、危険にさらされている言語や方言を翻訳します。	• 翻訳 SDK for .NET (テキスト) • 翻訳 NuGet パッケージ (テキスト) • 翻訳 SDK for .NET (バッチ) • 翻訳 NuGet パッケージ (バッチ)

サービス	説明	リファレンス ドキュメント
Video Indexer	ご利用のビデオからアクションにつながる分析情報を抽出します。	Video Indexer C# のコード サンプル
Vision	デジタル画像やリッチ メディア資産のコンテンツを分析します。	• Vision SDK for .NET • Vision NuGet パッケージ

非推奨のサービス

テーブルを展開する

サービス	説明	リファレンス ドキュメント
Anomaly Detector (2023 年非推奨)	時系列データの異常を監視して検出します。	• Anomaly Detector SDK for .NET • Anomaly Detector NuGet パッケージ
Content Moderator (2024 年非推奨)	攻撃的で望ましくない可能性のあるコンテンツを監視して検出します。	• Content Moderator SDK for .NET • Content Moderator NuGet パッケージ
Language Understanding (LUIS) (2023 年非推奨)	アプリケーションで自然言語の理解を使用します。	• LUIS SDK for .NET (オーサリング) • LUIS NuGet パッケージ (オーサリング) • LUIS SDK for .NET (予測) • LUIS NuGet パッケージ (予測)
Metrics Advisor (2023 年非推奨)	アプリケーションやサービスの有害なコンテンツを検出します。	• Metrics Advisor SDK for .NET • Metrics Advisor NuGet パッケージ

サービス	説明	リファレンス ドキュメント
Personalizer (2023 年非推奨)	豊富でパーソナライズされたコンテンツとエクスペリエンスをユーザーに提示します。	• Personalizer SDK for .NET • Personalizer NuGet パッケージ
QnA maker (非推奨 2022)	簡単にナビゲートできる質問と回答のアプリケーションに情報を蒸留します。	• QnA maker SDK for .NET • QnA maker NuGet パッケージ

次のステップ

- Azure AI REST API リファレンスを表示する

Azure AI REST API リファレンス

[アーティクル] • 2024/03/20

この記事では、利用可能な Azure AI REST API の概要と、サービス レベルと機能レベルのリファレンス ドキュメントへのリンクについて説明します。

利用可能な Azure AI サービス

表からサービスを選択して、開発目標の達成にどのように役立つかを確認します。

サポートされているサービス

テーブルを展開する

サービスのドキュメント	説明	リファレンス ドキュメント
Azure AI Search	AI を利用したクラウド検索をモバイル アプリと Web アプリで使用できるようにします	Azure AI Search API
Azure OpenAI	さまざまな自然言語タスクを実行する	Azure OpenAI API • リソースの作成とデプロイ • 完了と埋め込み • 微調整
Bot Service	ボットを作成して複数のチャネルにわたって接続します	Bot Service API
Content Safety	望ましくないコンテンツを検出する AI サービス	Content セーフty API
Custom Vision	ビジネス アプリケーションの画像認識をカスタマイズします。	Custom Vision API • 予測 • トレーニング
Document Intelligence	ドキュメントをインテリジェントなデータドリブン ソリューションに変換する	ドキュメント インテリジェンス API
Face	画像内の人や感情を検出および識別する	Face API
Language	業界をリードする自然言語理解機能を備えたアプリを構築する	REST API
Speech	音声テキスト変換、テキスト読み上げ、翻訳、話者認識	Speech API • 音声テキスト変換

サービスのドキュメント	説明	リファレンス ドキュメント
		• テキスト読み上げ
Translator	100以上の使用中、危険、絶滅危惧言語や方言を翻訳する	**翻訳 API** • テキスト翻訳 • バッチ翻訳 • 同期変換
Video Indexer	ご利用のビデオからアクションにつながる分析情報を抽出します	Video Indexer API
Vision	画像と動画のコンテンツを分析する	Vision API

非推奨のサービス

テーブルを展開する

サービスのドキュメント	説明	リファレンス ドキュメント
Anomaly Detector (2023 年非推奨)	潜在的な問題を早期に特定する	Anomaly Detector API
Content Moderator (2024 年非推奨)	不快感を与える可能性がある、または望ましくないコンテンツを検出する	Content Moderator API
Language Understanding (LUIS) (2023 年非推奨)	アプリで自然な言語を理解する	LUIS API
Metrics Advisor (2023 年非推奨)	望ましくないコンテンツを検出する AI サービス	Metrics Advisor API
Personalizer (2023 年非推奨)	ユーザーごとに豊富でパーソナライズされたエクスペリエンスを作成する	Personalizer API
QnA maker (2022 年非推奨)	情報を、よりナビゲートしやすい質問と回答に変換する	QnA Maker API

次のステップ

- Azure AI SDK リファレンスを表示する

Accounts

リファレンス

Service: Azure AI Services

API Version: 2023-05-01

Operations

テーブルを展開する

Create	Cognitive Services アカウントを作成します。 アカウントは、リソース グループ全体のリソースの種類です。 開発者がインテリジェント API にアクセスするためのキーが保持されます。 また、re...
Delete	リソース グループから Cognitive Services アカウントを削除します。
Get	パラメーターで指定された Cognitive Services アカウントを返します。
List	サブスクリプションに属する特定の種類のすべてのリソースを返します。
List By Resource Group	リソース グループに属する特定の種類のすべてのリソースを返します
List Keys	指定した Cognitive Services アカウントのアカウント キーをListsします。
List Models	要求された Cognitive Services アカウントで使用可能なモデルを一覧表示する
List Skus	要求された Cognitive Services アカウントで使用可能な SKU を一覧表示する
List Usages	要求された Cognitive Services アカウントの使用状況を取得する
Regenerate Key	指定した Cognitive Services アカウントの指定したアカウント キーを再生成します。
Update	Cognitive Services アカウントを更新する

.NET 用 Microsoft Azure Cognitive Services 管理クライアント ライブラリ

[アーティクル] • 2023/06/27

Microsoft Azure Cognitive Services は、すべての開発者とデータ サイエンティストの手の届く範囲に AI をもたらします。 主要なモデルでは、さまざまなユース ケースをロック解除できます。 必要なのは、高度な意思決定をアプリに表示、読み上げ、読み上げ、検索、理解、高速化する機能を埋め込む API 呼び出しです。 すべてのスキル レベルの開発者とデータ サイエンティストが、アプリに AI 機能を簡単に追加できるようにします。

このライブラリでは、Microsoft Azure Cognitive Services リソースの管理がサポートされています。

このライブラリは 、新しい Azure SDK ガイドライン に従い、多くのコア機能を提供します。

```
- Support MSAL.NET, Azure.Identity is out of box for supporting MSAL.NET.
- Support [OpenTelemetry](https://opentelemetry.io/) for distributed
tracing.
- HTTP pipeline with custom policies.
- Better error-handling.
- Support uniform telemetry across all languages.
```

作業の開始

パッケージをインストールする

NuGet を使用して .NET 用の Microsoft Azure Cognitive Services 管理ライブラリをインストールします。

.NET CLI

```
dotnet add package Azure.ResourceManager.CognitiveServices
```

前提条件

- Microsoft Azure サブスクリプション が必要です。

クライアントの認証

認証されたクライアントを作成し、Microsoft Azure リソースとの対話を開始するには、 こちらのクイックスタート ガイドを参照してください。

主要な概念

Microsoft Azure SDK for .NETの主な概念については、こちらを参照してください。

ドキュメント

ドキュメントは、このパッケージの使用方法を学習するのに役立ちます。

- クイック スタート。
- API 参照。
- [認証] :

例

.NET 用管理ライブラリを使用するためのコード サンプルは、次の場所にあります。

- .NET 管理ライブラリのコード サンプル

トラブルシューティング

- GitHub の問題を使用して 問題を報告します。
- 以前の質問を確認するか、Azure タグと .NET タグを使用して Stack Overflow で新しい質問をします。

次のステップ

Microsoft Azure SDK の詳細については、 こちらの Web サイトを参照してください。

共同作成

このリポジトリへの投稿の詳細については、 投稿ガイドを参照してください。

このプロジェクトでは、共同作成と提案を歓迎しています。 ほとんどの共同作成では、共同作成者使用許諾契約書 (CLA) にご同意いただき、ご自身の共同作成内容を使用

する権利を Microsoft に供与する権利をお持ちであり、かつ実際に供与することを宣言していただく必要があります。 詳細については、 https://cla.microsoft.com を参照してください。

pull request を送信すると、CLA を提供して PR (ラベルやコメントなど) を適宜装飾する必要があるかどうかを CLA ボットが自動的に決定します。 ボットによって提供される手順に従ってください。 このアクションは、CLA を使用してすべてのリポジトリで 1 回だけ実行する必要があります。

このプロジェクトは、「Microsoft のオープン ソースの倫理規定」を採用しています。 詳しくは、倫理規定についてよくある質問 に関する記事を参照するか、opencode@microsoft.com 宛てに質問またはコメントをお送りください。

フィードバック

このページはお役に立ちましたか? Yes いいえ

製品フィードバックの提供

@azure/arm-cognitiveservices package

リファレンス

クラス

テーブルを展開する

CognitiveServicesManagementClient	

インターフェイス

テーブルを展開する

AbusePenalty	虐待の罰則。
Account	Cognitive Services アカウントは、プロビジョニングされたアカウントを表す Azure リソースであり、種類、場所、SKU です。
AccountListResult	Cognitive Services アカウント操作応答の一覧。
AccountModel	Cognitive Services アカウント モデル。
AccountModelListResult	Cognitive Services アカウント操作応答の一覧。
AccountProperties	Cognitive Services アカウントのプロパティ。
AccountSku	Cognitive Services リソースの種類と SKU。
AccountSkuListResult	Cognitive Services アカウント操作応答の一覧。
Accounts	アカウントを表すインターフェイス。
AccountsCreateOptionalParams	省略可能なパラメーター。
AccountsDeleteOptionalParams	省略可能なパラメーター。
AccountsGetOptionalParams	省略可能なパラメーター。
AccountsListByResourceGroupNextOptionalParams	省略可能なパラメーター。
AccountsListByResource	省略可能なパラメーター。

GroupOptionalParams	
AccountsListKeysOptionalParams	省略可能なパラメーター。
AccountsListModelsNextOptionalParams	省略可能なパラメーター。
AccountsListModelsOptionalParams	省略可能なパラメーター。
AccountsListNextOptionalParams	省略可能なパラメーター。
AccountsListOptionalParams	省略可能なパラメーター。
AccountsListSkusOptionalParams	省略可能なパラメーター。
AccountsListUsagesOptionalParams	省略可能なパラメーター。
AccountsRegenerateKeyOptionalParams	省略可能なパラメーター。
AccountsUpdateOptionalParams	省略可能なパラメーター。
ApiKeys	コグニティブ サービス アカウントのアクセス キー。
ApiProperties	特殊な API の API プロパティ。
AzureEntityResource	etag を含む Azure Resource Manager リソースのリソース モデル定義。
CallRateLimit	呼び出しレート制限 Cognitive Services アカウント。
CapacityConfig	容量の構成。
CheckDomainAvailabilityOptionalParams	省略可能なパラメーター。
CheckDomainAvailabilityParameter	[ドメインの可用性パラメーター] を確認します。
CheckSkuAvailabilityOptionalParams	省略可能なパラメーター。
CheckSkuAvailabilityParameter	SKU 可用性パラメーターを確認します。

CognitiveServices ManagementClient OptionalParams	省略可能なパラメーター。
CommitmentCost	Cognitive Services アカウントコミットメント コスト。
CommitmentPeriod	Cognitive Services アカウントのコミットメント期間。
CommitmentPlan	Cognitive Services アカウントコミットメント プラン。
CommitmentPlanAccount Association	コミットメント 計画の関連付け。
CommitmentPlanAccount AssociationListResult	Cognitive Services コミットメント プラン アカウントの関連付け操作応答の一覧。
CommitmentPlan Association	コミットメント 計画の関連付け。
CommitmentPlanListResult	Cognitive Services アカウント操作応答の一覧。
CommitmentPlanProperties	Cognitive Services アカウントコミットメント プランのプロパティ。
CommitmentPlans	CommitmentPlans を表すインターフェイス。
CommitmentPlansCreate OrUpdateAssociation OptionalParams	省略可能なパラメーター。
CommitmentPlansCreate OrUpdateOptionalParams	省略可能なパラメーター。
CommitmentPlansCreate OrUpdatePlanOptional Params	省略可能なパラメーター。
CommitmentPlansDelete AssociationHeaders	CommitmentPlans_deleteAssociation操作のヘッダーを定義します。
CommitmentPlansDelete AssociationOptionalParams	省略可能なパラメーター。
CommitmentPlansDelete OptionalParams	省略可能なパラメーター。
CommitmentPlansDelete PlanHeaders	CommitmentPlans_deletePlan操作のヘッダーを定義します。
CommitmentPlansDelete PlanOptionalParams	省略可能なパラメーター。

CommitmentPlansGetAssociationOptionalParams	省略可能なパラメーター。
CommitmentPlansGetOptionalParams	省略可能なパラメーター。
CommitmentPlansGetPlanOptionalParams	省略可能なパラメーター。
CommitmentPlansListAssociationsNextOptionalParams	省略可能なパラメーター。
CommitmentPlansListAssociationsOptionalParams	省略可能なパラメーター。
CommitmentPlansListNextOptionalParams	省略可能なパラメーター。
CommitmentPlansListOptionalParams	省略可能なパラメーター。
CommitmentPlansListPlansByResourceGroupNextOptionalParams	省略可能なパラメーター。
CommitmentPlansListPlansByResourceGroupOptionalParams	省略可能なパラメーター。
CommitmentPlansListPlansBySubscriptionNextOptionalParams	省略可能なパラメーター。
CommitmentPlansListPlansBySubscriptionOptionalParams	省略可能なパラメーター。
CommitmentPlansUpdatePlanHeaders	CommitmentPlans_updatePlan操作のヘッダーを定義します。
CommitmentPlansUpdatePlanOptionalParams	省略可能なパラメーター。
CommitmentQuota	Cognitive Services アカウントのコミットメント クォータ。
CommitmentTier	Cognitive Services アカウント コミットメント レベル。
CommitmentTierListResult	Cognitive Services アカウント操作応答の一覧。
CommitmentTiers	CommitmentTiers を表すインターフェイス。

CommitmentTiersListNextOptionalParams	省略可能なパラメーター。
CommitmentTiersListOptionalParams	省略可能なパラメーター。
DeletedAccounts	DeletedAccounts を表すインターフェイス。
DeletedAccountsGetOptionalParams	省略可能なパラメーター。
DeletedAccountsListNextOptionalParams	省略可能なパラメーター。
DeletedAccountsListOptionalParams	省略可能なパラメーター。
DeletedAccountsPurgeOptionalParams	省略可能なパラメーター。
Deployment	Cognitive Services アカウントのデプロイ。
DeploymentListResult	Cognitive Services アカウント操作応答の一覧。
DeploymentModel	Cognitive Services アカウントデプロイ モデルのプロパティ。
DeploymentProperties	Cognitive Services アカウントの展開のプロパティ。
DeploymentScaleSettings	Cognitive Services アカウントデプロイ モデルのプロパティ。
Deployments	デプロイを表すインターフェイス。
DeploymentsCreateOrUpdateOptionalParams	省略可能なパラメーター。
DeploymentsDeleteOptionalParams	省略可能なパラメーター。
DeploymentsGetOptionalParams	省略可能なパラメーター。
DeploymentsListNextOptionalParams	省略可能なパラメーター。
DeploymentsListOptionalParams	省略可能なパラメーター。
DomainAvailability	ドメインの可用性。
Encryption	暗号化を構成するプロパティ
ErrorAdditionalInfo	リソース管理エラーの追加情報。

ErrorDetail	エラーの詳細。
ErrorResponse	失敗した操作のエラーの詳細を返す、すべての Azure Resource Manager API に対する一般的なエラー応答。 (これは、OData エラー応答形式にも従います)。
Identity	リソースの ID。
IpRule	特定の IP アドレスまたは IP 範囲からのアクセシビリティを制御する規則。
KeyVaultProperties	keyVault プロパティを構成するプロパティ
MetricName	メトリック名。
Model	Cognitive Services モデル。
ModelDeprecationInfo	Cognitive Services アカウント ModelDeprecationInfo。
ModelListResult	コグニティブ サービス モデルの一覧。
ModelSku	使用可能な Cognitive Services モデル SKU について説明します。
Models	モデルを表すインターフェイス。
ModelsListNextOptionalParams	省略可能なパラメーター。
ModelsListOptionalParams	省略可能なパラメーター。
MultiRegionSettings	マルチリージョン設定 Cognitive Services アカウント。
NetworkRuleSet	ネットワーク アクセシビリティを管理する一連の規則。
Operation	リソース プロバイダー操作 API から返される REST API 操作の詳細
OperationDisplay	この特定の操作のローカライズされた表示情報。
OperationListResult	Azure リソース プロバイダーでサポートされている REST API 操作の一覧。 これには、次の結果セットを取得するための URL リンクが含まれています。
Operations	操作を表すインターフェイス。
OperationsListNextOptionalParams	省略可能なパラメーター。
OperationsListOptionalParams	省略可能なパラメーター。
PatchResourceTags	リソースのタグの更新に使用されるオブジェクト。一般に PATCH 操作に使用されます。

PatchResourceTagsAndSku	リソースのタグと SKU の更新に使用されるオブジェクト。一般に PATCH 操作に使用されます。
PrivateEndpoint	プライベート エンドポイント リソース。
PrivateEndpointConnection	プライベート エンドポイント接続リソース。
PrivateEndpointConnectionListResult	プライベート エンドポイント接続の一覧
PrivateEndpointConnectionProperties	PrivateEndpointConnectProperties のプロパティ。
PrivateEndpointConnections	PrivateEndpointConnections を表すインターフェイス。
PrivateEndpointConnectionsCreateOrUpdateOptionalParams	省略可能なパラメーター。
PrivateEndpointConnectionsDeleteOptionalParams	省略可能なパラメーター。
PrivateEndpointConnectionsGetOptionalParams	省略可能なパラメーター。
PrivateEndpointConnectionsListOptionalParams	省略可能なパラメーター。
PrivateLinkResource	プライベート リンク リソース
PrivateLinkResourceListResult	プライベート リンク リソースの一覧
PrivateLinkResourceProperties	プライベート リンク リソースのプロパティ。
PrivateLinkResources	PrivateLinkResources を表すインターフェイス。
PrivateLinkResourcesListOptionalParams	省略可能なパラメーター。
PrivateLinkServiceConnectionState	サービス コンシューマーとプロバイダー間の接続の状態に関する情報のコレクション。
ProxyResource	Azure Resource Manager プロキシ リソースのリソース モデル定義。 タグと場所は含まれません
QuotaLimit	

RegenerateKeyParameters	キー パラメーターを再生成します。
RegionSetting	呼び出しレート制限 Cognitive Services アカウント。
RequestMatchPattern	
Resource	すべての Azure Resource Manager リソースの応答で返される一般的なフィールド
ResourceSku	使用可能な Cognitive Services SKU について説明します。
ResourceSkuListResult	Get Skus 操作の応答。
ResourceSkuRestrictionInfo	
ResourceSkuRestrictions	SKU の制限について説明します。
ResourceSkus	ResourceSkus を表すインターフェイス。
ResourceSkusListNextOptionalParams	省略可能なパラメーター。
ResourceSkusListOptionalParams	省略可能なパラメーター。
Sku	SKU を表すリソース モデル定義
SkuAvailability	SKU の可用性。
SkuAvailabilityListResult	SKU の可用性の結果の一覧を確認します。
SkuCapability	SkuCapability は、特定の機能の機能を示します。
SkuChangeInfo	アカウントの SKU 変更情報。
SystemData	リソースの作成と最後の変更に関連するメタデータ。
ThrottlingRule	
Usage	使用状況要求の使用状況データ。
UsageListResult	リストの使用要求に対する応答。
Usages	使用法を表すインターフェイス。
UsagesListNextOptionalParams	省略可能なパラメーター。
UsagesListOptionalParams	省略可能なパラメーター。
UserAssignedIdentity	ユーザー割り当てマネージド ID。
UserOwnedStorage	Cognitive Services アカウントのユーザー所有ストレージ。

VirtualNetworkRule	特定の仮想ネットワークからのアクセシビリティを制御するルール。

型エイリアス

テーブルを展開する

AbusePenaltyAction	AbusePenaltyAction の値を定義します。 KnownAbusePenaltyAction は AbusePenaltyAction と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **スロットル** **ブロック**
AccountsCreateResponse	作成操作の応答データが含まれます。
AccountsGetResponse	get 操作の応答データが含まれます。
AccountsListByResourceGroupNextResponse	listByResourceGroupNext 操作の応答データを格納します。
AccountsListByResourceGroupResponse	listByResourceGroup 操作の応答データを格納します。
AccountsListKeysResponse	listKeys 操作の応答データを格納します。
AccountsListModelsNextResponse	listModelsNext 操作の応答データを格納します。
AccountsListModelsResponse	listModels 操作の応答データを格納します。
AccountsListNextResponse	listNext 操作の応答データを格納します。
AccountsListResponse	リスト操作の応答データが含まれます。
AccountsListSkusResponse	listSkus 操作の応答データを格納します。

AccountsListUsages Response	listUsages 操作の応答データを格納します。
AccountsRegenerate KeyResponse	regenerateKey 操作の応答データを格納します。
AccountsUpdate Response	更新操作の応答データが含まれます。
ActionType	ActionType の値を定義します。 KnownActionType は ActionType と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **内部**
CheckDomain AvailabilityResponse	checkDomainAvailability 操作の応答データを格納します。
CheckSkuAvailability Response	checkSkuAvailability 操作の応答データを格納します。
CommitmentPlan ProvisioningState	CommitmentPlanProvisioningState の値を定義します。 KnownCommitmentPlanProvisioningState は CommitmentPlanProvisioningState と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **同意** **作成** **削除中** **移動** **Failed** **Succeeded** **Canceled**
CommitmentPlans CreateOrUpdate AssociationResponse	createOrUpdateAssociation 操作の応答データを格納します。
CommitmentPlans CreateOrUpdatePlan Response	createOrUpdatePlan 操作の応答データを格納します。
CommitmentPlans CreateOrUpdate Response	createOrUpdate 操作の応答データを格納します。

CommitmentPlans GetAssociation Response	getAssociation 操作の応答データを格納します。
CommitmentPlans GetPlanResponse	getPlan 操作の応答データが含まれます。
CommitmentPlans GetResponse	get 操作の応答データが含まれます。
CommitmentPlans ListAssociationsNext Response	listAssociationsNext 操作の応答データを格納します。
CommitmentPlans ListAssociations Response	listAssociations 操作の応答データを格納します。
CommitmentPlans ListNextResponse	listNext 操作の応答データを格納します。
CommitmentPlans ListPlansByResource GroupNextResponse	listPlansByResourceGroupNext 操作の応答データが含まれます。
CommitmentPlans ListPlansByResource GroupResponse	listPlansByResourceGroup 操作の応答データを格納します。
CommitmentPlans ListPlans BySubscriptionNext Response	listPlansBySubscriptionNext 操作の応答データを格納します。
CommitmentPlans ListPlans BySubscription Response	listPlansBySubscription 操作の応答データが含まれます。
CommitmentPlans ListResponse	リスト操作の応答データが含まれます。
CommitmentPlans UpdatePlanResponse	updatePlan 操作の応答データが含まれます。
CommitmentTiersList NextResponse	listNext 操作の応答データが含まれます。
CommitmentTiersList Response	リスト操作の応答データが含まれます。

CreatedByType	CreatedByType の値を定義します。 KnownCreatedByType は CreatedByType と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 ## サービスでサポートされている既知の値 **User** **Application** **ManagedIdentity** **キー**
DeletedAccountsGetResponse	get 操作の応答データが含まれます。
DeletedAccountsListNextResponse	listNext 操作の応答データが含まれます。
DeletedAccountsListResponse	リスト操作の応答データが含まれます。
DeploymentModelVersionUpgradeOption	DeploymentModelVersionUpgradeOption の値を定義します。 KnownDeploymentModelVersionUpgradeOption は DeploymentModelVersionUpgradeOption と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 ## サービスでサポートされている既知の値 **OnceNewDefaultVersionAvailable** **OnceCurrentVersionExpired** **NoAutoUpgrade**
DeploymentProvisioningState	DeploymentProvisioningState の値を定義します。 KnownDeploymentProvisioningState は DeploymentProvisioningState と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 ## サービスでサポートされている既知の値 **同意** **作成** **削除中** **移動** **Failed** **Succeeded** **Disabled** **Canceled**

DeploymentScaleType	DeploymentScaleType の値を定義します。 KnownDeploymentScaleType は DeploymentScaleType と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **Standard** **手動**
DeploymentsCreateOrUpdateResponse	createOrUpdate 操作の応答データが含まれます。
DeploymentsGetResponse	get 操作の応答データが含まれます。
DeploymentsListNextResponse	listNext 操作の応答データが含まれます。
DeploymentsListResponse	リスト操作の応答データが含まれます。
HostingModel	HostingModel の値を定義します。 KnownHostingModel は HostingModel と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **Web** **ConnectedContainer** **DisconnectedContainer** **ProvisionedWeb**
KeyName	KeyName の値を定義します。
KeySource	KeySource の値を定義します。 KnownKeySource は KeySource と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **Microsoft.CognitiveServices** **Microsoft.KeyVault**
ModelLifecycleStatus	ModelLifecycleStatus の値を定義します。 KnownModelLifecycleStatus は ModelLifecycleStatus と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。

	サービスでサポートされている既知の値 **GenerallyAvailable** **プレビュー**
ModelsListNext Response	listNext 操作の応答データを格納します。
ModelsListResponse	リスト操作の応答データが含まれます。
NetworkRuleAction	NetworkRuleAction の値を定義します。 KnownNetworkRuleAction は NetworkRuleAction と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **許可** **Deny**
OperationsListNext Response	listNext 操作の応答データを格納します。
OperationsList Response	リスト操作の応答データが含まれます。
Origin	Origin の値を定義します。 KnownOrigin は Origin と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **user** **システム** **user,system**
PrivateEndpoint Connection ProvisioningState	PrivateEndpointConnectionProvisioningState の値を定義します。 KnownPrivateEndpointConnectionProvisioningState は PrivateEndpointConnectionProvisioningState と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **Succeeded** **作成**

	削除中 **失敗**
PrivateEndpointConnectionsCreateOrUpdateResponse	createOrUpdate 操作の応答データを格納します。
PrivateEndpointConnectionsGetResponse	get 操作の応答データが含まれます。
PrivateEndpointConnectionsListResponse	リスト操作の応答データが含まれます。
PrivateEndpointServiceConnectionStatus	PrivateEndpointServiceConnectionStatus の値を定義します。 KnownPrivateEndpointServiceConnectionStatus は PrivateEndpointServiceConnectionStatus と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **保留中** **Approved** **拒否**
PrivateLinkResourcesListResponse	リスト操作の応答データが含まれます。
ProvisioningState	ProvisioningState の値を定義します。 KnownProvisioningState は ProvisioningState と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **同意** **作成** **削除中** **移動** **Failed** **Succeeded** **DNS の解決**
PublicNetworkAccess	PublicNetworkAccess の値を定義します。 KnownPublicNetworkAccess は PublicNetworkAccess と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。

	サービスでサポートされている既知の値 **有効** **Disabled**
QuotaUsageStatus	QuotaUsageStatus の値を定義します。 KnownQuotaUsageStatus は QuotaUsageStatus と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **含まれる** **ブロック** **InOverage** **Unknown**
ResourceIdentityType	ResourceIdentityType の値を定義します。
ResourceSku RestrictionsReason Code	ResourceSkuRestrictionsReasonCode の値を定義します。 KnownResourceSkuRestrictionsReasonCode は ResourceSkuRestrictionsReasonCode と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **QuotaId** **NotAvailableForSubscription**
ResourceSku RestrictionsType	ResourceSkuRestrictionsType の値を定義します。
ResourceSkusList NextResponse	listNext 操作の応答データを格納します。
ResourceSkusList Response	リスト操作の応答データが含まれます。
RoutingMethods	RoutingMethods の値を定義します。 KnownRoutingMethods は RoutingMethods と同じ意味で使用できます。この列挙型には、サービスがサポートする既知の値が含まれています。 **サービスでサポートされている既知の値** **優先順位** **重み付け** **パフォーマンス**

SkuTier	SkuTier の値を定義します。 KnownSkuTier は SkuTier と同じ意味で使用できます。この列挙型には、サービスでサポートされている既知の値が含まれています。 **サービスでサポートされている既知の値** **Free** **Basic** **Standard** **Premium** **エンタープライズ**
UnitType	UnitType の値を定義します。 KnownUnitType は UnitType と同じ意味で使用できます。この列挙型には、サービスでサポートされている既知の値が含まれています。 **サービスでサポートされている既知の値** **Count** **[サイズ]** **Seconds** **パーセント** **CountPerSecond** **BytesPerSecond** **ミリ秒**
UsagesListNext Response	listNext 操作の応答データを格納します。
UsagesListResponse	リスト操作の応答データが含まれます。

列挙型

テーブルを展開する

KnownAbusePenaltyAction	サービスが受け入れる AbusePenaltyAction の既知の値。
KnownActionType	サービスが受け入れる ActionType の既知の値。
KnownCommitmentPlan ProvisioningState	サービスが受け入れる CommitmentPlanProvisioningState の既知の値。
KnownCreatedByType	サービスが受け入れる CreatedByType の既知の値。
KnownDeploymentModel VersionUpgradeOption	サービスが受け入れる DeploymentModelVersionUpgradeOption の既知の値。

KnownDeploymentProvisioningState	サービスが受け入れる DeploymentProvisioningState の既知の値。
KnownDeploymentScaleType	サービスが受け入れる DeploymentScaleType の既知の値。
KnownHostingModel	サービスが受け入れる HostingModel の既知の値。
KnownKeySource	サービスが受け入れる KeySource の既知の値。
KnownModelLifecycleStatus	サービスが受け入れる ModelLifecycleStatus の既知の値。
KnownNetworkRuleAction	サービスが受け入れる NetworkRuleAction の既知の値。
KnownOrigin	サービスが受け入れる Origin の既知の値。
KnownPrivateEndpointConnectionProvisioningState	サービスが受け入れる PrivateEndpointConnectionProvisioningState の既知の値。
KnownPrivateEndpointServiceConnectionStatus	サービスが受け入れる PrivateEndpointServiceConnectionStatus の既知の値。
KnownProvisioningState	サービスが受け入れる ProvisioningState の既知の値。
KnownPublicNetworkAccess	サービスが受け入れる PublicNetworkAccess の既知の値。
KnownQuotaUsageStatus	サービスが受け入れる QuotaUsageStatus の既知の値。
KnownResourceSkuRestrictionsReasonCode	サービスが受け入れる ResourceSkuRestrictionsReasonCode の既知の値。
KnownRoutingMethods	サービスが受け入れる RoutingMethods の既知の値。
KnownSkuTier	サービスが受け入れる SkuTier の既知の値。
KnownUnitType	サービスが受け入れる UnitType の既知の値。

機能

テーブルを展開する

getContinuationToken(unknown)	反復子によって `byPage` 最後 `.value` に生成された を指定すると、後でそのポイントからページングを開始するために使用できる継続トークンが返されます。

関数の詳細

getContinuationToken(unknown)

反復子によって`byPage`最後`.value`に生成された を指定すると、後でそのポイントからページングを開始するために使用できる継続トークンが返されます。

TypeScript

```
function getContinuationToken(page: unknown): string | undefined
```

パラメーター

page unknown

反復子から IteratorResult にアクセス `value` する `byPage` オブジェクト。

戻り値

string | undefined

今後の呼び出し中に byPage() に渡すことができる継続トークン。

cognitiveservices パッケージ

リファレンス

パッケージ

テーブルを展開する

aio
models
operations

クラス

テーブルを展開する

CognitiveServicesManagementClient	Cognitive Services 管理クライアント。

GitHub で Microsoft と共同作業する

このコンテンツのソースは GitHub にあります。そこで、issue や pull request を作成および確認することもできます。 詳細については、共同作成者ガイドを参照してください。

Azure SDK for Python に関するフィードバック

Azure SDK for Python はオープンソース プロジェクトです。 フィードバックを提供するにはリンクを選択します。

ドキュメントの問題を開く

製品フィードバックの提供

com.microsoft.azure.management.cognitiveservices

Reference

Package: com.microsoft.azure.management.cognitiveservices

Maven Artifact: com.microsoft.azure:azure-mgmt-cognitiveservices:1.10.0-beta

This package contains the classes for CognitiveServicesManagementClient. Cognitive Services Management Client.

Classes

Expand table

CheckSkuAvailabilityParameter	Check SKU availability parameter.
CheckSkuAvailabilityResult	Check SKU availability result.
CognitiveServicesAccountUpdateParameters	The parameters to provide for the account.
CognitiveServicesResourceAndSku	Cognitive Services resource type and SKU.
Error	Cognitive Services error object.
ErrorBody	Cognitive Services error body.
ErrorException	Exception thrown for an invalid response with Error information.
Kind	Defines values for Kind.
MetricName	A metric name.
OperationDisplayInfo	The operation supported by Cognitive Services.
ProvisioningState	Defines values for ProvisioningState.
QuotaUsageStatus	Defines values for QuotaUsageStatus.
RegenerateKeyParameters	Regenerate key parameters.
SkuName	Defines values for SkuName.
UnitType	Defines values for UnitType.
Usage	The usage data for a usage request.

Enums

Expand table

KeyName	Defines values for KeyName.
SkuTier	Defines values for SkuTier.

Collaborate with us on GitHub

The source for this content can be found on GitHub, where you can also create and review issues and pull requests. For more information, see our contributor guide.

Azure SDK for Java feedback

Azure SDK for Java is an open source project. Select a link to provide feedback:

Open a documentation issue

Provide product feedback

az cognitiveservices

リファレンス

Azure Cognitive Services アカウントを管理します。

この記事では、Azure Cognitive Services アカウントとサブスクリプション管理専用の Azure CLI コマンドの一覧を示します。 API とサポートされている SDK の使用方法については、個々のサービスのドキュメント https://docs.microsoft.com/azure/cognitive-services/ を参照してください。

コマンド

テーブルを展開する

名前	説明	型	Status
az cognitiveservices account	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account commitment-plan	Azure Cognitive Services アカウントのコミットメント 計画を管理します。	コア	GA
az cognitiveservices account commitment-plan create	Azure Cognitive Services アカウントのコミットメント 計画を作成します。	コア	GA
az cognitiveservices account commitment-plan delete	Azure Cognitive Services アカウントからコミットメント プランを削除します。	コア	GA
az cognitiveservices account commitment-plan list	Azure Cognitive Services アカウントからのすべてのコミットメント プランを表示します。	コア	GA
az cognitiveservices account commitment-plan show	Azure Cognitive Services アカウントからのコミットメント プランを表示します。	コア	GA
az cognitiveservices account create	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account delete	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account deployment	Azure Cognitive Services アカウントのデプロイを管理します。	コア	GA
az cognitiveservices account deployment create	Azure Cognitive Services アカウントのデプロイを作成します。	コア	GA

名前	説明	型	Status
az cognitiveservices account deployment delete	Azure Cognitive Services アカウントからデプロイを削除します。	コア	GA
az cognitiveservices account deployment list	Azure Cognitive Services アカウントのすべてのデプロイを表示します。	コア	GA
az cognitiveservices account deployment show	Azure Cognitive Services アカウントのデプロイを表示します。	コア	GA
az cognitiveservices account identity	Cognitive Services アカウントの ID を管理します。	コア	GA
az cognitiveservices account identity assign	Cognitive Services アカウントの ID を割り当てます。	コア	GA
az cognitiveservices account identity remove	Cognitive Services アカウントから ID を削除します。	コア	GA
az cognitiveservices account identity show	Cognitive Services アカウントの ID を表示します。	コア	GA
az cognitiveservices account keys	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account keys list	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account keys regenerate	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account list	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account list-deleted	論理的に削除された Azure Cognitive Services アカウントを一覧表示します。	コア	GA
az cognitiveservices account list-kinds	Azure Cognitive Services アカウントのすべての有効な種類を一覧表示します。	コア	GA
az cognitiveservices account list-models	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account list-skus	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account list-usage	Azure Cognitive Services アカウントの使用状況を一覧表示します。	コア	GA
az cognitiveservices account network-rule	ネットワーク規則を管理します。	コア	GA

名前	説明	型	Status
az cognitiveservices account network-rule add	ネットワーク ルールを追加します。	コア	GA
az cognitiveservices account network-rule list	ネットワーク ルールを一覧表示します。	コア	GA
az cognitiveservices account network-rule remove	ネットワーク規則を削除します。	コア	GA
az cognitiveservices account purge	論理的に削除された Azure Cognitive Services アカウントを消去します。	コア	GA
az cognitiveservices account recover	論理的に削除された Azure Cognitive Services アカウントを復旧します。	コア	GA
az cognitiveservices account show	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices account show-deleted	論理的に削除された Azure Cognitive Services アカウントを表示します。	コア	GA
az cognitiveservices account update	Azure Cognitive Services アカウントを管理します。	コア	GA
az cognitiveservices commitment-tier	Azure Cognitive Services のコミットメント レベルを管理します。	コア	GA
az cognitiveservices commitment-tier list	Azure Cognitive Services のすべてのコミットメント レベルを表示します。	コア	GA
az cognitiveservices list	Azure Cognitive Services アカウントを管理します。	コア	非推奨
az cognitiveservices model	Azure Cognitive Services のモデルを管理します。	コア	GA
az cognitiveservices model list	Azure Cognitive Services のすべてのモデルを表示します。	コア	GA
az cognitiveservices usage	Azure Cognitive Services の使用状況を管理します。	コア	GA
az cognitiveservices usage list	Azure Cognitive Services のすべての使用状況を表示します。	コア	GA

az cognitiveservices list

編集

非推奨

> このコマンドは非推奨となり、今後のリリースで削除される予定です。 代わりに 'az cognitiveservices account list' を使用してください。

Azure Cognitive Services アカウントを管理します。

この記事では、Azure Cognitive Services アカウントとサブスクリプション管理専用の Azure CLI コマンドの一覧を示します。 API とサポートされている SDK の使用方法については、個々のサービスのドキュメント https://docs.microsoft.com/azure/cognitive-services/ を参照してください。

Azure CLI

```
az cognitiveservices list [--resource-group]
```

例

リソース グループ内のすべての Cognitive Services アカウントを一覧表示します。

Azure CLI

```
az cognitiveservices list -g MyResourceGroup
```

省略可能のパラメーター

`--resource-group -g`

リソース グループの名前。 `az configure --defaults group=<name>` を使用して、既定のグループを構成できます。

▼ グローバル パラメーター

`--debug`

すべてのデバッグ ログを表示するようにログの詳細レベルを上げます。

`--help -h`

このヘルプ メッセージを表示して終了します。

`--only-show-errors`

エラーのみを表示し、警告は抑制します。

`--output -o`

出力形式。

承認された値: json, jsonc, none, table, tsv, yaml, yamlc

既定値: json

`--query`

JMESPath クエリ文字列。 詳細と例については、http://jmespath.org/ をご覧ください。

`--subscription`

サブスクリプションの名前または ID。 `az account set -s NAME_OR_ID` を使用して、既定のサブスクリプションを構成できます。

`--verbose`

ログの詳細レベルを上げます。 詳細なデバッグ ログを表示するには --debug を使います。

AzureRM.CognitiveServices

リファレンス

このトピックでは、Azure Cognitive Services コマンドレットのヘルプ トピックが表示されます。

Cognitive Services

テーブルを展開する

Get-AzureRmCognitiveServicesAccount	Gets an account. **⚠ 警告** The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
Get-AzureRmCognitiveServicesAccountKey	Gets the API keys for an account. **⚠ 警告** The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates.

	Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
Get-AzureRmCognitiveServicesAccountSkus	Gets the available SKUs for an account. ⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
Get-AzureRmCognitiveServicesAccountType	Gets the available Cognitive Services Account Types. ⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for

	guidance on transitioning to the Az module.
Get-AzureRmCognitiveServicesAccountUsage	Get current usages for a Cognitive Services account. ⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
New-AzureRmCognitiveServicesAccount	Creates a Cognitive Services account. ⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
New-AzureRmCognitiveServicesAccountKey	Regenerates an account key.

	⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
Remove-AzureRmCognitiveServicesAccount	Deletes a Cognitive Services account. ⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate from AzureRM to the Az PowerShell module to ensure continued support and updates. Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our migration resources for guidance on transitioning to the Az module.
Set-AzureRmCognitiveServicesAccount	Modifies an account. ⚠ 警告 The AzureRM PowerShell module has been officially deprecated as of February 29, 2024. Users are advised to migrate

from AzureRM to the Az PowerShell module to ensure continued support and updates.

Although the AzureRM module may still function, it's no longer maintained or supported, placing any continued use at the user's discretion and risk. Please refer to our **migration resources** for guidance on transitioning to the Az module.

Azure AI サービスの Azure Policy 組み込みポリシー定義

[アーティクル] • 2024/04/13

このページは、Azure AI サービス用の Azure Policy 組み込みポリシー定義のインデックスです。 他のサービス用の Azure Policy 組み込みについては、Azure Policy 組み込み定義に関するページをご覧ください。

各組み込みポリシー定義の名前は、Azure portal のポリシー定義にリンクしています。 **[バージョン]** 列のリンクを使用すると、Azure Policy GitHub リポジトリ のソースを表示できます。

Azure AI サービス

テーブルを展開する

名前 (Azure portal)	説明	効果	Version (GitHub)
Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	セキュリティのため、キー アクセス (ローカル認証) を無効にしておくことをお勧めします。 開発/テストで通常使用される Azure OpenAI Studio にはキー アクセスが必要であり、キー アクセスが無効になっている場合は機能しません。 無効にすると、Microsoft Entra ID が唯一のアクセス方法になるため、最小特権の原則と詳細な制御を維持できます。 詳細については、https://aka.ms/AI/auth を参照してください	Audit、Deny、Disabled	1.1.0
Azure AI Services リソースでネットワーク アクセスを制限する必要がある	ネットワーク アクセスを制限すると、許可されたネットワークのみがサービスにアクセスできるようになります。 これを実現するには、許可されたネットワークからのアプリケーションのみが Azure AI サービスにアクセスできるようにネットワーク規則を構成します。	Audit、Deny、Disabled	3.2.0
Cognitive Services アカウントでカスタマー マネージド キーによるデータ暗号化を有効にする必要がある	規制コンプライアンス標準を満たすには、一般にカスタマー マネージド キーが必要です。 カスタマー マネージド キーを使用すると、自分が作成して所有する Azure Key Vault キーを使用して、Cognitive Services に格納	Audit、Deny、Disabled	2.1.0

名前 (Azure portal)	説明	効果	Version (GitHub)
	されているデータを暗号化できます。 ローテーションや管理など、キーのライフサイクルを完全に制御し、責任を負うことになります。 カスタマー マネージド キーの詳細については、https://go.microsoft.com/fwlink/?linkid=2121321 をご覧ください。		
Cognitive Services アカウントではマネージド ID を使用する必要がある	マネージド ID を Cognitive Service アカウントに割り当てると、安全な認証を確実に行うことができます。 この ID は、この Cognitive Service アカウントが、資格情報を管理しなくても、安全な方法で Azure Key Vault などの他の Azure サービスと通信するために使用されます。	Audit、Deny、Disabled	1.0.0
Cognitive Services アカウントで顧客所有のストレージを使用する必要がある	Cognitive Services の保存データは、顧客所有のストレージを使用して制御します。 顧客所有のストレージの詳細については、https://aka.ms/cogsvc-cmk を参照してください。	Audit、Deny、Disabled	2.0.0
Cognitive Services ではプライベート リンクを使用する必要がある	Azure Private Link を使用すると、接続元または接続先にパブリック IP アドレスを使用せずに、仮想ネットワークを Azure サービスに接続できます。 Private Link プラットフォームでは、Azure のバックボーン ネットワークを介してコンシューマーとサービスの間の接続が処理されます。 プライベート エンドポイントを Cognitive Services にマッピングすることにより、データ漏えいの可能性を減らすことができます。 プライベート リンクの詳細については、https://go.microsoft.com/fwlink/?linkid=2129800 を参照してください。	Audit、Disabled	3.0.0
ローカル認証方法を無効にするように Cognitive Services アカウントを構成する	ローカル認証方法を無効にして、Cognitive Services アカウントで Azure Active Directory ID を認証専用で要求するようにします。 詳細については、https://aka.ms/cs/auth を参照してください。	Modify、Disabled	1.0.0

名前 (Azure portal)	説明	効果	Version (GitHub)
公衆ネットワーク アクセスを無効にするように Cognitive Services アカウントを構成する	Cognitive Services リソースの公衆ネットワーク アクセスを無効にして、パブリック インターネット経由でアクセスできないようにします。 これにより、データ漏えいのリスクを軽減することができます。 詳細については、https://go.microsoft.com/fwlink/?linkid=2129800 を参照してください。	Disabled、Modify	3.0.0
プライベート エンドポイントを使用して Cognitive Services アカウントを構成する	プライベート エンドポイントを使用すると、接続元または接続先にパブリック IP アドレスを使用せずに、仮想ネットワークを Azure サービスに接続できます。 プライベート エンドポイントを Cognitive Services にマッピングすることにより、データ漏えいの可能性を減らすことができます。 プライベート リンクの詳細については、https://go.microsoft.com/fwlink/?linkid=2129800 を参照してください。	DeployIfNotExists、Disabled	3.0.0
Azure AI サービス リソースの診断ログを有効にする必要がある	Azure AI サービス リソースのログを有効にします。 これで、セキュリティ インシデントが発生した場合やネットワークが侵害された場合に、調査目的でアクティビティ証跡を再作成できます	AuditIfNotExists、Disabled	1.0.0
Cognitive Services (microsoft.cognitiveservices/accounts) のカテゴリ グループごとのイベント ハブへのログを有効にする	リソース ログを有効にして、リソースで発生するアクティビティとイベントを追跡し、発生した変更を可視化し、分析情報を提供する必要があります。 このポリシーでは、カテゴリ グループを使用して診断設定をデプロイし、Cognitive Services (microsoft.cognitiveservices/accounts) 用のイベント ハブにログをルーティングします。	DeployIfNotExists、AuditIfNotExists、Disabled	1.1.0
Cognitive Services (microsoft.cognitiveservices/accounts) のカテゴリ グループごとの Log Analytics へのログを有効にする	リソース ログを有効にして、リソースで発生するアクティビティとイベントを追跡し、発生した変更を可視化し、分析情報を提供する必要があります。 このポリシーでは、カテゴリ グループを使用して診断設定をデ	DeployIfNotExists、AuditIfNotExists、Disabled	1.0.0

名前 (Azure portal)	説明	効果	Version (GitHub)
	プロイし、Cognitive Services (microsoft.cognitiveservices/accounts) 用の Log Analytics ワークスペースにログをルーティングします。		
Cognitive Services (microsoft.cognitiveservices/accounts) のカテゴリ グループごとのストレージへのログを有効にする	リソース ログを有効にして、リソースで発生するアクティビティとイベントを追跡し、発生した変更を可視化し、分析情報を提供する必要があります。 このポリシーでは、カテゴリ グループを使用して診断設定をデプロイし、Cognitive Services (microsoft.cognitiveservices/accounts) 用のストレージ アカウントにログをルーティングします。	DeployIfNotExists、AuditIfNotExists、Disabled	1.0.0

次のステップ

- Azure Policy GitHub リポジトリ のビルトインを参照します。
- 「Azure Policy の定義の構造」を確認します。
- 「Policy の効果について」を確認します。

Azure AI サービスのサポート オプションとヘルプ オプション

[アーティクル] • 2024/02/22

Azure AI サービスの機能を調べ始めたばかりですか。 今まさに、アプリケーションに新しい機能を実装中でしょうか。 あるいはもうすでにサービスを使用して、その改善方法についての提案をお持ちでしょうか。 ここでは、Azure AI サービスのサポートを受ける方法、最新の状態を維持する方法、フィードバックを提供する方法、バグを報告する方法に関するオプションを説明します。

Azure サポート要求を作成する

クラウドへの移行を始めたばかりの開発者の方も、ビジネスクリティカルで戦略的なアプリケーションの展開を行う大企業のお客様も、さまざな Azure サポート オプションをご確認し、最適なプランをお選びください。 Azure ユーザーは、Azure portal でサポート要求を作成し、管理できます。

- Azure Portal
- 米国政府機関向け Azure portal

Microsoft Q&A に質問を投稿する

製品に関する技術的な質問については、Azure に関するコミュニティ サポートの場である Microsoft Q&A をぜひご利用ください。Microsoft のエンジニアや Azure Most Valuable Professional (MVP)、エキスパート コミュニティからすばやく、信頼できる回答が得られます。

問題に対する回答が検索で見つからない場合は、Microsoft Q&A に新しい質問を送信してください。 質問するときは、次のタグのいずれかを使います。

- Azure AI サービス

Vision

- Azure AI Vision
- Custom Vision
- Face
- Document Intelligence
- Video Indexer

Language

- Immersive Reader
- Language Understanding (LUIS)
- QnA Maker
- 言語サービス
- Translator

Speech

- Speech サービス

Decision

- Anomaly Detector
- Content Moderator
- Metrics Advisor
- Personalizer

Azure OpenAI

- Azure OpenAI

Stack Overflow に質問を投稿する

開発に関する質問について、最大のコミュニティ開発者エコシステムから回答を得るには、Stack Overflow に質問を投稿してください。

Stack Overflow に新しい質問を送信する場合は、次のいずれかのタグを使用して質問を作成します。複数のタグを使用することもできます。

- Azure AI サービス

Vision

- Azure AI Vision
- Custom Vision
- Face
- Document Intelligence
- Video Indexer

Language

- Immersive Reader

- Language Understanding (LUIS)
- QnA Maker
- 言語サービス
- Translator

Speech

- Speech サービス

Decision

- Anomaly Detector
- Content Moderator
- Metrics Advisor
- Personalizer

Azure OpenAI

- Azure OpenAI

フィードバックを送信

新機能を要求するには、 https://feedback.azure.com に投稿します。 Azure AI サービスとその API が、開発しているアプリケーションにさらに役立つようにするアイデアを共有します。

- Azure AI サービス

Vision

- Azure AI Vision
- Custom Vision
- Face
- Document Intelligence
- Video Indexer

Language

- Immersive Reader
- Language Understanding (LUIS)
- QnA Maker
- 言語サービス
- Translator

Speech

- Speech サービス

Decision

- Anomaly Detector
- Content Moderator
- Metrics Advisor
- Personalizer

最新情報を入手

機能に関する新たなリリースやAzure ブログのニュースを常に把握しておくと、プログラミング エラー、サービス バグ、または Azure AI サービスではまだ利用できない機能についての役立つ情報を得ることができます。

- 製品の更新プログラム、ロードマップ、および発表の詳細については、「Azure の更新情報」で確認できます。
- Azure AI サービスに関するニュースは、Azure ブログで共有されています。
- Azure AI サービスに関して、Reddit で会話に参加します。

次のステップ

Azure AI サービスとは

Compare Azure Government and global Azure

Article • 10/12/2023

Microsoft Azure Government uses same underlying technologies as global Azure, which includes the core components of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Both Azure and Azure Government have the same comprehensive security controls in place and the same Microsoft commitment on the safeguarding of customer data. Whereas both cloud environments are assessed and authorized at the FedRAMP High impact level, Azure Government provides an extra layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to screened US persons. These commitments may be of interest to customers using the cloud to store or process data subject to US export control regulations.

> **Note**
>
> These lists and tables do not include feature or bundle availability in the Azure Government Secret or Azure Government Top Secret clouds. For more information about specific availability for air-gapped clouds, please contact your account team.

Export control implications

You're responsible for designing and deploying your applications to meet US export control requirements such as the requirements prescribed in the EAR, ITAR, and DoE 10 CFR Part 810. In doing so, you shouldn't include sensitive or restricted information in Azure resource names, as explained in Considerations for naming Azure resources.

Guidance for developers

Most of the currently available technical content assumes that applications are being developed on global Azure rather than on Azure Government. For this reason, it's important to be aware of two key differences in applications that you develop for hosting in Azure Government.

- Certain services and features that are in specific regions of global Azure might not be available in Azure Government.
- Feature configurations in Azure Government might differ from those in global Azure.

Therefore, it's important to review your sample code and configurations to ensure that you are building within the Azure Government cloud services environment.

For more information, see Azure Government developer guide.

> **Note**
>
> This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see **Introducing the new Azure PowerShell Az module**. For Az module installation instructions, see **Install the Azure Az PowerShell module**.

You can use AzureCLI or PowerShell to obtain Azure Government endpoints for services you provisioned:

- Use **Azure CLI** to run the az cloud show command and provide `AzureUSGovernment` as the name of the target cloud environment. For example,

Azure CLI

```
az cloud show --name AzureUSGovernment
```

should get you different endpoints for Azure Government.

- Use a **PowerShell** cmdlet such as Get-AzEnvironment to get endpoints and metadata for an instance of Azure service. For example,

  PowerShell

  ```
  Get-AzEnvironment -Name AzureUSGovernment
  ```

  should get you properties for Azure Government. This cmdlet gets environments from your subscription data file.

Table below lists API endpoints in Azure vs. Azure Government for accessing and managing some of the more common services. If you provisioned a service that isn't listed in the table below, see the Azure CLI and PowerShell examples above for suggestions on how to obtain the corresponding Azure Government endpoint.

Expand table

Service category	Service name	Azure Public	Azure Government	Notes
AI + machine learning	Azure Bot Service	botframework.com	botframework.azure.us	
	Azure AI Document Intelligence	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Azure OpenAI Service	openai.azure.com	openai.azure.us	
	Computer Vision	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Custom Vision	cognitiveservices.azure.com	cognitiveservices.azure.us Portal	
	Content Moderator	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Face API	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Language Understanding	cognitiveservices.azure.com	cognitiveservices.azure.us Portal	Part of Azure AI Language
	Personalizer	cognitiveservices.azure.com	cognitiveservices.azure.us	
	QnA Maker	cognitiveservices.azure.com	cognitiveservices.azure.us	Part of Azure AI Language
	Speech service	See STT API docs	Speech Studio See Speech service endpoints **Speech translation endpoints**	

Service category	Service name	Azure Public	Azure Government	Notes
			Virginia: `https://usgovvirginia.s2s.speech.azure.us` Arizona: `https://usgovarizona.s2s.speech.azure.us`	
	Text Analytics	cognitiveservices.azure.com	cognitiveservices.azure.us	Part of Azure AI Language
	Translator	See Translator API docs	cognitiveservices.azure.us	
Analytics	Azure HDInsight	azurehdinsight.net	azurehdinsight.us	
	Event Hubs	servicebus.windows.net	servicebus.usgovcloudapi.net	
	Power BI	app.powerbi.com	app.powerbigov.us	Power BI US Gov
Compute	Batch	batch.azure.com	batch.usgovcloudapi.net	
	Cloud Services	cloudapp.net	usgovcloudapp.net	
Containers	Azure Service Fabric	cloudapp.azure.com	cloudapp.usgovcloudapi.net	
	Container Registry	azurecr.io	azurecr.us	
Databases	Azure Cache for Redis	redis.cache.windows.net	redis.cache.usgovcloudapi.net	See How to connect to other clouds
	Azure Cosmos DB	documents.azure.com	documents.azure.us	
	Azure Database for MariaDB	mariadb.database.azure.com	mariadb.database.usgovcloudapi.net	
	Azure Database for MySQL	mysql.database.azure.com	mysql.database.usgovcloudapi.net	
	Azure Database for PostgreSQL	postgres.database.azure.com	postgres.database.usgovcloudapi.net	
	Azure SQL Database	database.windows.net	database.usgovcloudapi.net	
Identity	Microsoft Entra ID	login.microsoftonline.com	login.microsoftonline.us	
		certauth.login.microsoftonline.com	certauth.login.microsoftonline.us	
		passwordreset.microsoftonline.com	passwordreset.microsoftonline.us	
Integration	Service Bus	servicebus.windows.net	servicebus.usgovcloudapi.net	
Internet of Things	Azure IoT Hub	azure-devices.net	azure-devices.us	

Service category	Service name	Azure Public	Azure Government	Notes
	Azure Maps	atlas.microsoft.com	atlas.azure.us	
	Notification Hubs	servicebus.windows.net	servicebus.usgovcloudapi.net	
Management and governance	Azure Automation	azure-automation.net	azure-automation.us	
	Azure Monitor	mms.microsoft.com	oms.microsoft.us	Log Analytics workspace portal
		ods.opinsights.azure.com	ods.opinsights.azure.us	Data collector API
		oms.opinsights.azure.com	oms.opinsights.azure.us	
		portal.loganalytics.io	portal.loganalytics.us	
		api.loganalytics.io	api.loganalytics.us	
		docs.loganalytics.io	docs.loganalytics.us	
		adx.monitor.azure.com	adx.monitor.azure.us	Data Explorer queries
	Azure Resource Manager	management.azure.com	management.usgovcloudapi.net	
	Gallery URL	gallery.azure.com	gallery.azure.us	
	Microsoft Azure portal	portal.azure.com	portal.azure.us	
	Microsoft Intune	enterpriseregistration.windows.net	enterpriseregistration.microsoftonline.us	Enterprise registration
		manage.microsoft.com	manage.microsoft.us	Enterprise enrollment
Migration	Azure Site Recovery	hypervrecoverymanager.windowsazure.com	hypervrecoverymanager.windowsazure.us	Site Recovery service
		backup.windowsazure.com	backup.windowsazure.us	Protection service
		blob.core.windows.net	blob.core.usgovcloudapi.net	Storing VM snapshots
Networking	Traffic Manager	trafficmanager.net	usgovtrafficmanager.net	
Security	Key Vault	vault.azure.net	vault.usgovcloudapi.net	
Storage	Azure Backup	backup.windowsazure.com	backup.windowsazure.us	
	Blob	blob.core.windows.net	blob.core.usgovcloudapi.net	

Service category	Service name	Azure Public	Azure Government	Notes
	Queue	queue.core.windows.net	queue.core.usgovcloudapi.net	
	Table	table.core.windows.net	table.core.usgovcloudapi.net	
	File	file.core.windows.net	file.core.usgovcloudapi.net	
Virtual desktop infrastructure	Azure Virtual Desktop	See AVD docs	See AVD docs	
Web	API Management	management.azure.com	management.usgovcloudapi.net	
	API Management Gateway	azure-api.net	azure-api.us	
	API Management management	management.azure-api.net	management.azure-api.us	
	API Management Portal	portal.azure-api.net	portal.azure-api.us	
	App Configuration	azconfig.io	azconfig.azure.us	
	App Service	azurewebsites.net	azurewebsites.us	
	Azure AI Search	search.windows.net	search.windows.us	
	Azure Functions	azurewebsites.net	azurewebsites.us	

Service availability

Microsoft's goal for Azure Government is to match service availability in Azure. For service availability in Azure Government, see Products available by region. Services available in Azure Government are listed by category and whether they're Generally Available or available through Preview. If a service is available in Azure Government, that fact isn't reiterated in the rest of this article. Instead, you're encouraged to review Products available by region for the latest, up-to-date information on service availability.

In general, service availability in Azure Government implies that all corresponding service features are available to you. Variations to this approach and other applicable limitations are tracked and explained in this article based on the main service categories outlined in the online directory of Azure services. Other considerations for service deployment and usage in Azure Government are also provided.

AI + machine learning

This section outlines variations and considerations when using **Azure Bot Service**, **Azure Machine Learning**, and **Cognitive Services** in the Azure Government environment. For service availability, see Products available by region.

Azure Bot Service

The following Azure Bot Service **features aren't currently available** in Azure Government:

- Bot Framework Composer integration
- Channels (due to availability of dependent services)
  - Direct Line Speech Channel
  - Telephony Channel (Preview)
  - Microsoft Search Channel (Preview)
  - Kik Channel (deprecated)

For information on how to deploy Bot Framework and Azure Bot Service bots to Azure Government, see Configure Bot Framework bots for US Government customers.

Azure Machine Learning

For feature variations and limitations, see Azure Machine Learning feature availability across cloud regions.

Azure AI services: Content Moderator

The following Content Moderator **features aren't currently available** in Azure Government:

- Review UI and Review APIs.

Azure AI Language Understanding (LUIS)

The following Language Understanding **features aren't currently available** in Azure Government:

- Speech Requests
- Prebuilt Domains

Azure AI Language Understanding (LUIS) is part of Azure AI Language.

Azure AI Speech

For feature variations and limitations, including API endpoints, see Speech service in sovereign clouds.

Azure AI services: OpenAI Service

The following features of Azure OpenAI are available in Azure Government:

Expand table

Feature	Azure OpenAI
Models available	US Gov Arizona: GPT-4 (1106-Preview) GPT-3.5-Turbo (1106) GPT-3.5-Turbo (0125) text-embedding-ada-002 (version 2) US Gov Virginia: GPT-4 (1106-Preview) GPT-3.5-Turbo (0125) text-embedding-ada-002 (version 2) Learn more in Azure OpenAI Service models

Feature	Azure OpenAI
Virtual network support & private link support	Yes, unless using Azure OpenAI on your data
Managed Identity	Yes, via Microsoft Entra ID
UI experience	**Azure portal** for account & resource management **Azure OpenAI Studio** for model exploration

Next steps

- Get started by requesting access to Azure OpenAI Service in Azure Government at https://aka.ms/AOAIgovaccess
- Request quota increases for the pay-as-you-go consumption model, please fill out a separate form at https://aka.ms/AOAIGovQuota

Azure AI services: Translator

For feature variations and limitations, including API endpoints, see Translator in sovereign clouds.

Analytics

This section outlines variations and considerations when using Analytics services in the Azure Government environment. For service availability, see Products available by region.

Azure HDInsight

For secured virtual networks, you'll want to allow network security groups (NSGs) access to certain IP addresses and ports. For Azure Government, you should allow the following IP addresses (all with an Allowed port of 443):

Expand table

Region	Allowed IP addresses	Allowed port
US DoD Central	52.180.249.174 52.180.250.239	443
US DoD East	52.181.164.168 52.181.164.151	443
US Gov Texas	52.238.116.212 52.238.112.86	443
US Gov Virginia	13.72.49.126 13.72.55.55 13.72.184.124 13.72.190.110	443
US Gov Arizona	52.127.3.176 52.127.3.178	443

For a demo on how to build data-centric solutions on Azure Government using HDInsight, see Azure AI services, HDInsight, and Power BI on Azure Government.

Power BI

For usage guidance, feature variations, and limitations, see Power BI for US government customers. For a demo on how to build data-centric solutions on Azure Government using Power BI, see Azure AI services, HDInsight, and Power BI on Azure Government.

Power BI Embedded

To learn how to embed analytical content within your business process application, see Tutorial: Embed a Power BI content into your application for national clouds.

Databases

This section outlines variations and considerations when using Databases services in the Azure Government environment. For service availability, see Products available by region.

Azure Database for MySQL

The following Azure Database for MySQL **features aren't currently available** in Azure Government:

- Advanced Threat Protection

Azure Database for PostgreSQL

For Flexible Server availability in Azure Government regions, see Azure Database for PostgreSQL – Flexible Server.

The following Azure Database for PostgreSQL **features aren't currently available** in Azure Government:

- Azure Cosmos DB for PostgreSQL, formerly Azure Database for PostgreSQL – Hyperscale (Citus). For more information about supported regions, see Regional availability for Azure Cosmos DB for PostgreSQL.
- The following features of the Single Server deployment option
  - Advanced Threat Protection
  - Backup with long-term retention

Developer tools

This section outlines variations and considerations when using Developer tools in the Azure Government environment. For service availability, see Products available by region.

Enterprise Dev/Test subscription offer

- Enterprise Dev/Test subscription offer in existing or separate tenant is currently available only in Azure public as documented in Azure EA portal administration.

Identity

This section outlines variations and considerations when using Identity services in the Azure Government environment. For service availability, see Products available by region.

Microsoft Entra ID P1 and P2

For feature variations and limitations, see Cloud feature availability.

For information on how to use Power BI capabilities for collaboration between Azure and Azure Government, see Cross-cloud B2B.

The following features have known limitations in Azure Government:

- Limitations with B2B Collaboration in supported Azure US Government tenants:
  - For more information about B2B collaboration limitations in Azure Government and to find out if B2B collaboration is available in your Azure Government tenant, see Microsoft Entra B2B in government and national clouds.
- Limitations with multi-factor authentication:
  - Trusted IPs isn't supported in Azure Government. Instead, use Conditional Access policies with named locations to establish when multi-factor authentication should and shouldn't be required based off the user's current IP address.

Azure Active Directory B2C

Azure Active Directory B2C is **not available** in Azure Government.

Microsoft Authentication Library (MSAL)

The Microsoft Authentication Library (MSAL) enables developers to acquire security tokens from the Microsoft identity platform to authenticate users and access secured web APIs. For feature variations and limitations, see National clouds and MSAL.

Management and governance

This section outlines variations and considerations when using Management and Governance services in the Azure Government environment. For service availability, see Products available by region.

Automation

The following Automation **features aren't currently available** in Azure Government:

- Automation analytics solution

Azure Advisor

For feature variations and limitations, see Azure Advisor in sovereign clouds.

Azure Lighthouse

The following Azure Lighthouse **features aren't currently available** in Azure Government:

- Managed Service offers published to Azure Marketplace
- Delegation of subscriptions across a national cloud and the Azure public cloud, or across two separate national clouds, isn't supported
- Privileged Identity Management (PIM) feature isn't enabled, for example, just-in-time (JIT) / eligible authorization capability

Azure Monitor

Azure Monitor enables the same features in both Azure and Azure Government.

- System Center Operations Manager 2019 is supported equally well in both Azure and Azure Government.

The following options are available for previous versions of System Center Operations Manager:

- Integrating System Center Operations Manager 2016 with Azure Government requires an updated Advisor management pack that is included with Update Rollup 2 or later.
- System Center Operations Manager 2012 R2 requires an updated Advisor management pack included with Update Rollup 3 or later.

For more information, see Connect Operations Manager to Azure Monitor.

Frequently asked questions

- Can I migrate data from Azure Monitor logs in Azure to Azure Government?
  - No. It isn't possible to move data or your workspace from Azure to Azure Government.
- Can I switch between Azure and Azure Government workspaces from the Operations Management Suite portal?
  - No. The portals for Azure and Azure Government are separate and don't share information.

Application Insights

Application Insights (part of Azure Monitor) enables the same features in both Azure and Azure Government. This section describes the supplemental configuration that is required to use Application Insights in Azure Government.

Visual Studio – In Azure Government, you can enable monitoring on your ASP.NET, ASP.NET Core, Java, and Node.js based applications running on Azure App Service. For more information, see Application monitoring for Azure App Service overview. In Visual Studio, go to Tools|Options|Accounts|Registered Azure Clouds|Add New Azure Cloud and select Azure US Government as the Discovery endpoint. After that, adding an account in File|Account Settings will prompt you for which cloud you want to add from.

SDK endpoint modifications – In order to send data from Application Insights to an Azure Government region, you'll need to modify the default endpoint addresses that are used by the Application Insights SDKs. Each SDK requires slightly different modifications, as described in Application Insights overriding default endpoints.

Firewall exceptions – Application Insights uses several IP addresses. You might need to know these addresses if the app that you're monitoring is hosted behind a firewall. For more information, see IP addresses used by Azure Monitor from where you can download Azure Government IP addresses.

> **Note**
>
> Although these addresses are static, it's possible that we'll need to change them from time to time. All Application Insights traffic represents outbound traffic except for availability monitoring and webhooks, which require inbound firewall rules.

You need to open some **outgoing ports** in your server's firewall to allow the Application Insights SDK and/or Status Monitor to send data to the portal:

Expand table

Purpose	URL	IP address	Ports
Telemetry	dc.applicationinsights.us	23.97.4.113	443

Cost Management and Billing

The following Azure Cost Management + Billing **features aren't currently available** in Azure Government:

- Cost Management + Billing for cloud solution providers (CSPs)

Media

This section outlines variations and considerations when using Media services in the Azure Government environment. For service availability, see Products available by region.

Media Services

For Azure Media Services v3 feature variations in Azure Government, see Azure Media Services v3 clouds and regions availability.

Migration

This section outlines variations and considerations when using Migration services in the Azure Government environment. For service availability, see Products available by region.

Azure Migrate

The following Azure Migrate **features aren't currently available** in Azure Government:

- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on App Service.
- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on Azure Kubernetes Service (AKS).
- Containerizing ASP.NET apps and deploying them on Windows containers on AKS.
- Containerizing ASP.NET apps and deploying them on Windows containers on App Service.
- You can only create assessments for Azure Government as target regions and using Azure Government offers.

For more information, see Azure Migrate support matrix. For a list of Azure Government URLs needed by the Azure Migrate appliance when connecting to the internet, see Azure Migrate appliance URL access.

Networking

This section outlines variations and considerations when using Networking services in the Azure Government environment. For service availability, see Products available by region.

Azure ExpressRoute

For an overview of ExpressRoute, see What is Azure ExpressRoute?. For an overview of how **BGP communities** are used with ExpressRoute in Azure Government, see BGP community support in National Clouds.

Azure Front Door

Azure Front Door (AFD) Standard and Premium tiers are available in general availability in Azure Government regions US Gov Arizona and US Gov Texas. The following Azure Front Door feature **isn't supported** in Azure Government:

- Managed certificate for enabling HTTPS; instead use your own certificate.

Private Link

- For Private Link services availability, see Azure Private Link availability.
- For Private DNS zone names, see Azure Private Endpoint DNS configuration.

Traffic Manager

Traffic Manager health checks can originate from certain IP addresses for Azure Government. Review the IP addresses in the JSON file to ensure that incoming connections from these IP addresses are allowed at the endpoints to check its health status.

Security

This section outlines variations and considerations when using Security services in the Azure Government environment. For service availability, see Products available by region.

Microsoft Defender for Endpoint

For feature variations and limitations, see Microsoft Defender for Endpoint for US Government customers.

Microsoft Defender for IoT

For feature variations and limitations, see Cloud feature availability for US Government customers.

Azure Information Protection

Azure Information Protection Premium is part of the Enterprise Mobility + Security suite. For details on this service and how to use it, see Azure Information Protection Premium Government Service Description.

Microsoft Defender for Cloud

For feature variations and limitations, see Cloud feature availability for US Government customers.

Microsoft Sentinel

For feature variations and limitations, see Cloud feature availability for US Government customers.

Storage

This section outlines variations and considerations when using Storage services in the Azure Government environment. For service availability, see Products available by region.

Azure NetApp Files

For Azure NetApp Files feature availability in Azure Government and how to access the Azure NetApp Files service within Azure Government, see Azure NetApp Files for Azure Government.

Azure Import/Export

With Import/Export jobs for US Gov Arizona or US Gov Texas, the mailing address is for US Gov Virginia. The data is loaded into selected storage accounts from the US Gov Virginia region. For all jobs, we recommend that you rotate your storage account keys after the job is complete to remove any access granted during the process. For more information, see Manage storage account access keys.

Web

This section outlines variations and considerations when using Web services in the Azure Government environment. For service availability, see Products available by region.

API Management

The following API Management **features aren't currently available** in Azure Government:

- Azure AD B2C integration

App Service

The following App Service **resources aren't currently available** in Azure Government:

- App Service Certificate
- App Service Managed Certificate
- App Service Domain

The following App Service **features aren't currently available** in Azure Government:

- Deployment
  - Deployment options: only Local Git Repository and External Repository are available

Azure Functions

When connecting your Functions app to Application Insights in Azure Government, make sure you use APPLICATIONINSIGHTS_CONNECTION_STRING, which lets you customize the Application Insights endpoint.

Next steps

Learn more about Azure Government:

- Acquiring and accessing Azure Government
- Azure Government overview
- Azure support for export controls
- Azure Government compliance
- Azure Government security
- Azure guidance for secure isolation

Start using Azure Government:

- Guidance for developers
- Connect with the Azure Government portal