

クイックスタート

本書について

- 本書では、はじめて Quick MONITOR をお使いになる方に向けて、初期設定ウィザードを利用した初期設定方法についてご説明しています。
- 監視設定の詳細や仕様等については、別冊のリファレンスガイドやサービス仕様書をご参照ください。

本ガイドに従って進めると、次の条件に沿った設定を完了できます。

- おすすめの警告・障害条件設定
- 自動復旧設定は無効
- 通知方法は「メール」

自動復旧設定を有効にしたい場合や通知方法に Teams を選択したい場合は、本書に記載している以外の事前準備が必要です。それらの事前準備の内容については [リファレンスガイド] に記載しています。

目次

- 1. Quick MONITOR アカウントと URL の確認
- 2. Azure API 認証情報の用意
 - 1. Azure にアプリを登録
 - 2. サブスクリプションIDの確認と権限設定
- 3. その他の事前準備
 - 1. データベース認証情報の用意
 - 2. MySQL へのアクセス許可設定
 - 3. MariaDB へのアクセス許可設定
- 4. 初期設定ウィザード
 - 0. ログイン
 - 1. 初期設定ウィザード Step1: Azure API アクセスの設定
 - 2. 初期設定ウィザード Step2: メトリック収集設定
 - 1. メトリック収集設定 (Virtual Machines)
 - 2. メトリック収集設定 (Database)
 - 3. メトリック収集設定 (URL)
 - 3. 初期設定ウィザード Step3: 警告と障害条件設定
 - 4. 初期設定ウィザード Step4: 自動復旧設定
 - 5. 初期設定ウィザード Step5: 通知設定
 - 6. 初期設定ウィザード Step6: 完了
- 初期設定ウィザードを終えたあとの設定変更について

1. Quick MONITOR アカウントと URL の確認

お客様の契約内容にあわせてお知らせしている、次の情報をご用意ください。

- ユーザーアカウント
- サービス提供URL

2. Azure API 認証情報の用意

Microsoft Azure に接続して情報を得るために、以下の Azure API 認証情報をQuick MONITOR に登録します。

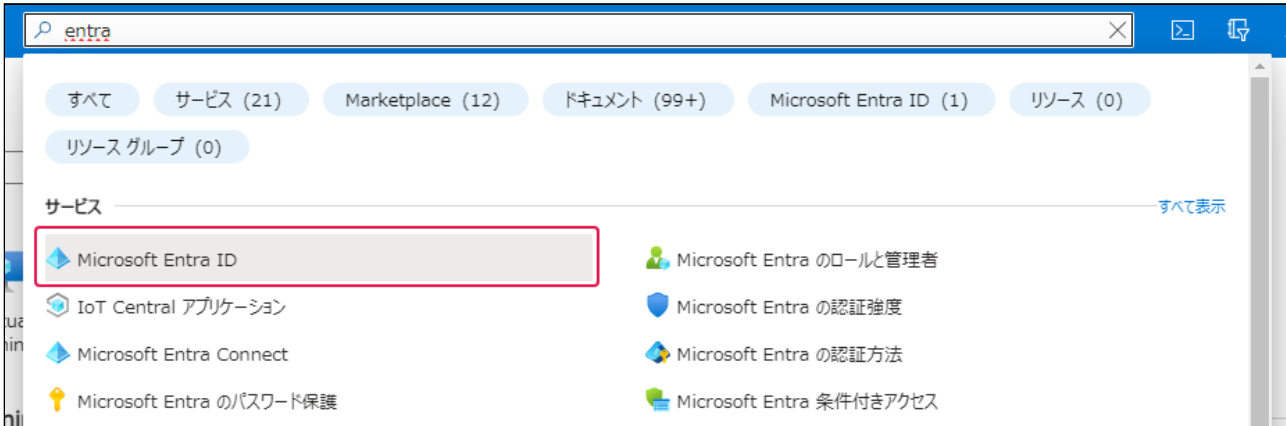
- (A)クライアントID
- (B) アプリケーションシークレット
- (C) テナントまたはドメイン名
- (D) サブスクリプションID

それぞれの認証情報の取得方法を以下にご案内いたします。Quick MONITOR の初期設定開始前に、これらの情報をご用意ください。

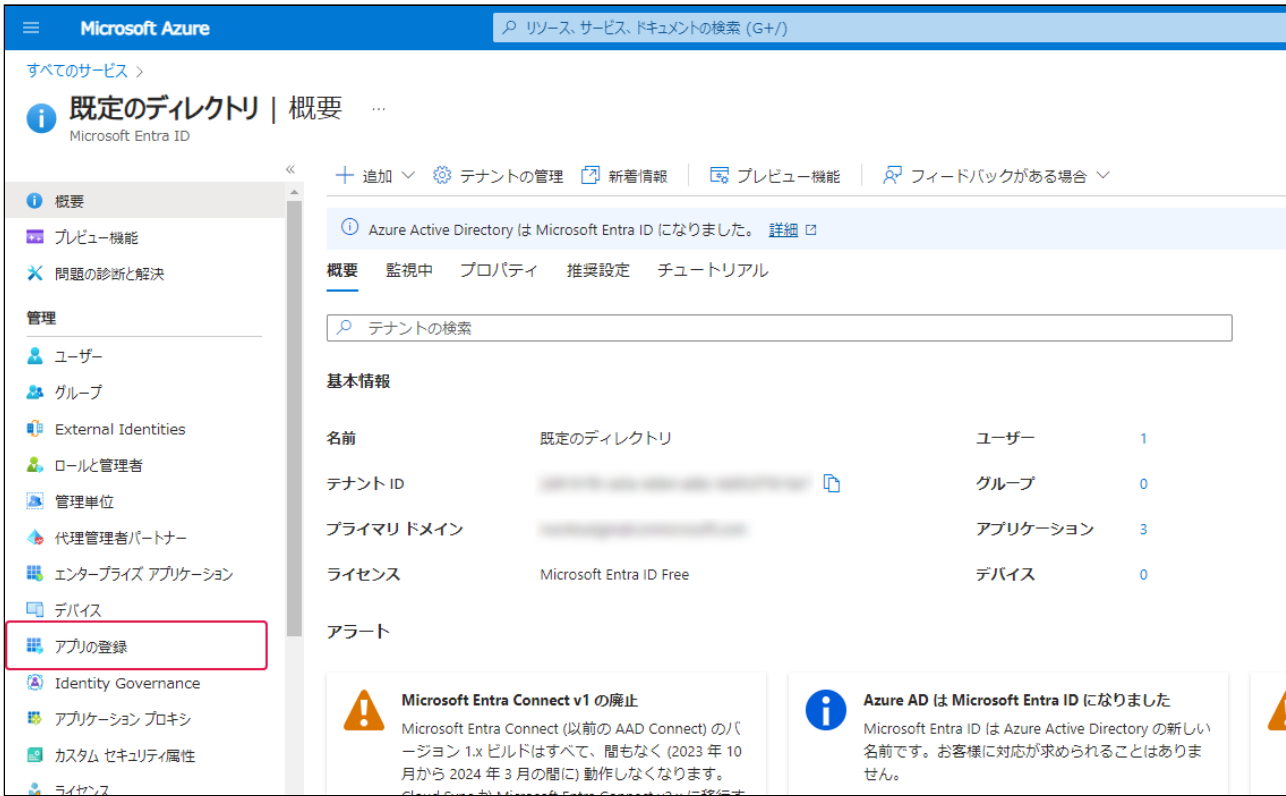
1. Azure にアプリを登録

この操作により、 クライアントID および アプリケーションシークレット、 テナントまたはドメイン名 を用意します。

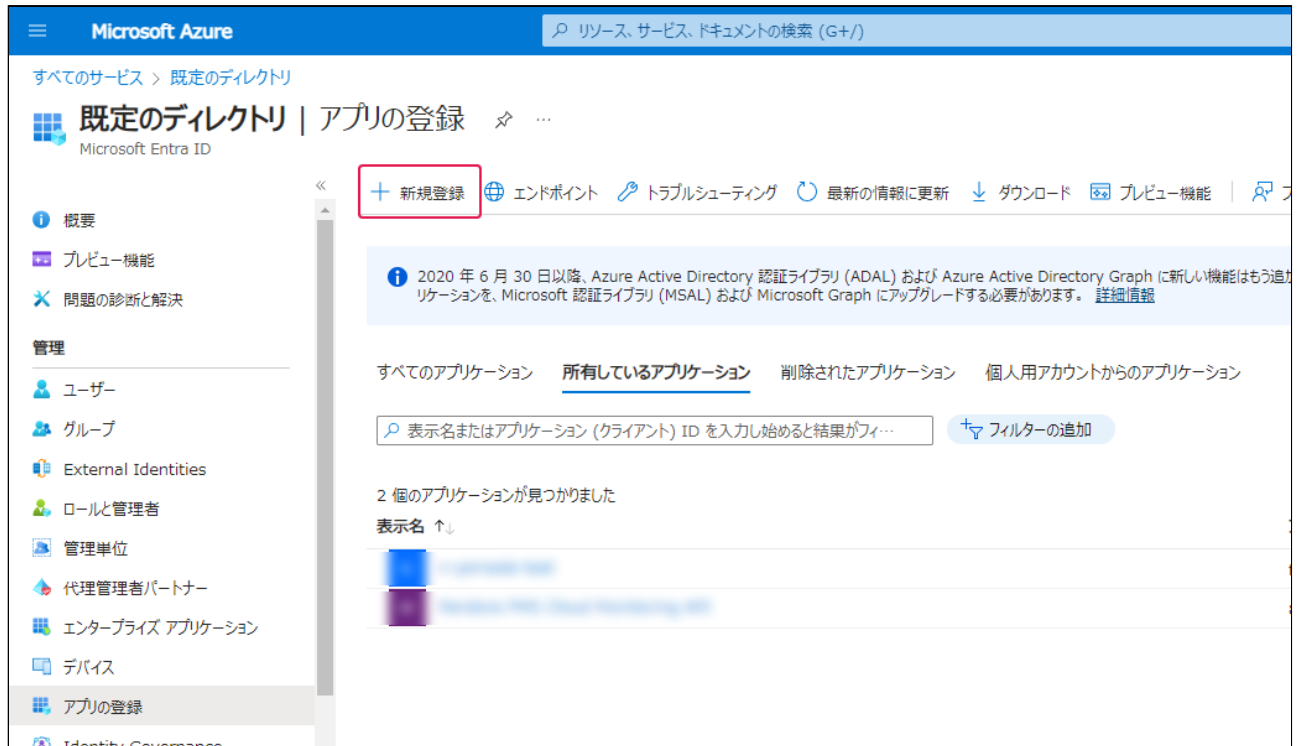
- 1. Azure Portalにサインインします。
- 2. Microsoft Entra ID サービスを開きます。



- 3. [アプリの登録] を開きます。



4. [新規登録] をクリックします。



5. 画面に従って入力後 [登録] ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

すべてのサービス > 既定のディレクトリ | アプリの登録 >

アプリケーションの登録

* 名前

このアプリケーションのユーザー向け表示名 (後で変更できます)。

1 任意の名前を入力 (例: Quick MONITOR)

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

☒ この組織ディレクトリのみに含まれるアカウント (既定のディレクトリ のみ - シングル テナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント) と個人用の Microsoft アカウント (Skype、Xbox など)

☐ 個人用 Microsoft アカウントのみ

[選択に関する詳細...](#)

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

プラットフォームの選択

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加して統合します。

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります [🔗](#)

登録 **2 クリック**

6. 登録したアプリの基本欄に表示されている次のパラメータを控えます。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > 既定のディレクトリ | アプリの登録 >

↑ ここには先程入力したアプリの名前が表示されます。(例: Quick MONITOR)

検索

概要

クイック スタート

統合アシスタント

管理

ブランド化とプロパティ

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

基本

表示名 :

アプリケーション (クライアントID) : **A クライアントID**

オブジェクト ID :

ディレクトリ (テナント) ID : **C テナントまたはドメイン名**

サポートされているアカウント : [すべての Microsoft アカウント ユーザー](#)

2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および Azure Active Directory Graph に新しい機能。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft Graph にアップグレードする必要があります。 [詳細情報](#)

7. [証明書とシークレット] を開きます。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > 既定のディレクトリ | アプリの登録 >

↑ ここには先程入力したアプリの名前が表示されます。(例: Quick MONITOR)

検索

概要

クイック スタート

統合アシスタント

管理

ブランド化とプロパティ

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

基本

表示名 :

アプリケーション (クライアントID) :

オブジェクト ID :

ディレクトリ (テナント) ID :

サポートされているアカウント : [すべての Microsoft アカウント ユーザー](#)

2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および Azure Active Directory Graph に新しい機能。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft Graph にアップグレードする必要があります。 [詳細情報](#)

8. [新しいクライアントシークレット] をクリックします。



9. 画面に従って入力後 [追加] ボタンをクリックします。

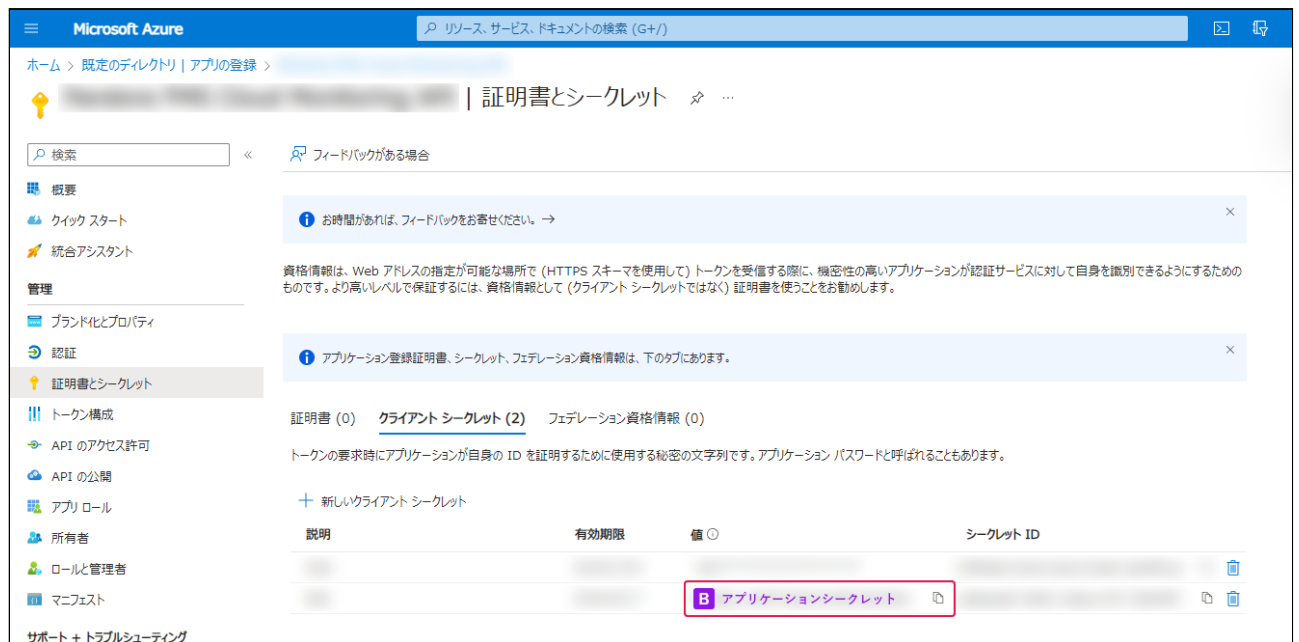
クライアント シークレットの追加

説明 **1 任意の説明を入力**

有効期限 **2 任意の期限を入力**

3 クリック

10. 作成したクライアントシークレットの値を控えます。

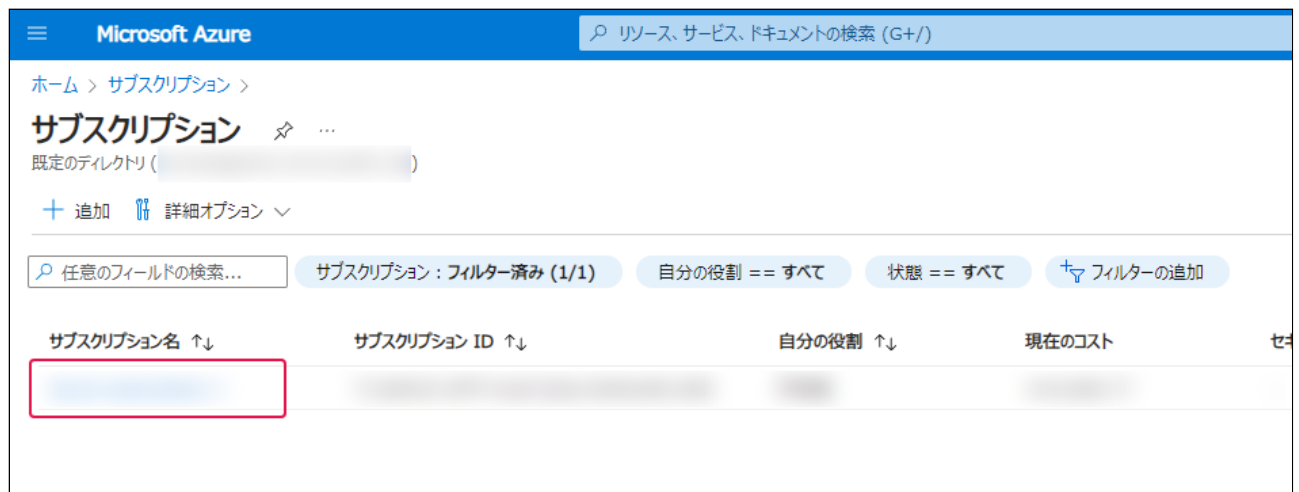


2. サブスクリプションIDの確認と権限設定

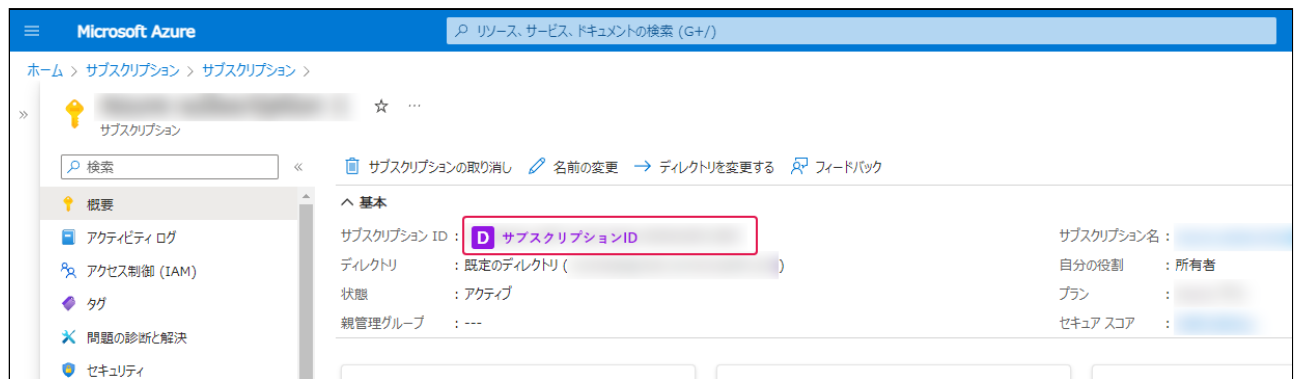
1. Azure portalにサインインします。
2. サブスクリプション サービスを開きます。



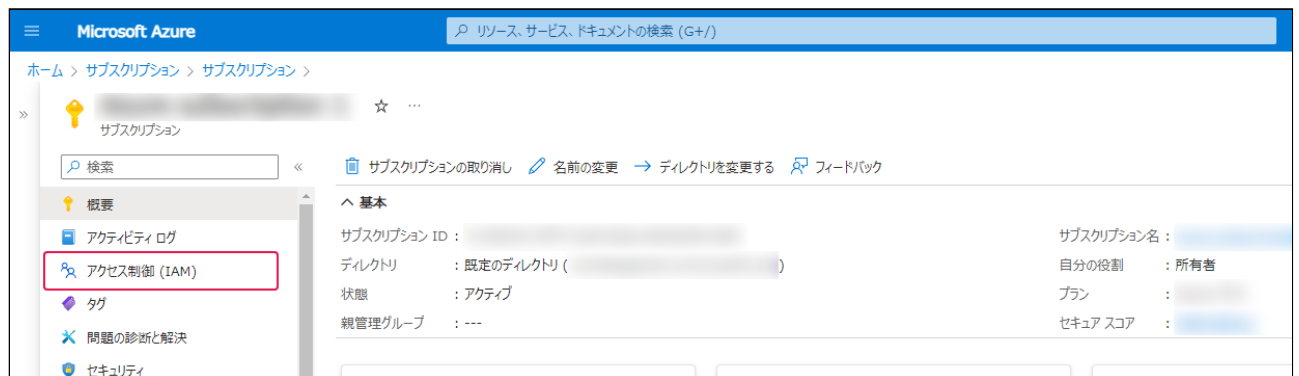
3. 任意のサブスクリプションを選びます。



4. サブスクリプションIDを控えておきます。



5. [アクセス制御 (IAM)] を開きます。



6. [追加] のメニューから [ロールの割り当ての追加] を選びます。



7. 閲覧者 のロールを選択し、[次へ] ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > サブスクリプション > サブスクリプション > | アクセス制御 (IAM) >

ロールの割り当ての追加

ロール

メンバー

レビューと割り当て

ロールの定義は、アクセス許可のコレクションです。組み込みロールを使用するか、カスタム ロールを作成することができます。 [詳細情報を見る](#)

割り当ての種類

職務ロール

特権管理者ロール

仮想マシンを作成する権限など、職務に基づいた Azure リソースへのアクセス権を付与します。

🔍

ロール名、説明、または ID で検索してください

種類: すべて

カテゴリ: すべて

名前 ↑↓	説明 ↑↓
閲覧者	すべてのリソースを表示しますが、変更することはできません。
AcrDelete	acr delete
AcrImageSigner	ACR イメージ署名者
AcrPull	acr のプル
AcrPush	acr のプッシュ
AcrQuarantineReader	ACR 検査データ閲覧者
AcrQuarantineWriter	ACR 検査データ作成者
Advisor Reviews Contributor	View reviews for a workload and triage recommendations linked to them.
Advisor Reviews Reader	View reviews for a workload and recommendations linked to them.
AgFood Platform Dataset Admin	Provides access to Dataset APIs
AgFood Platform Sensor Partner Contributor	Provides contribute access to manage sensor related entities in AgFood Platform Service
AgFood プラットフォーム サービス閲覧者	AgFood プラットフォーム サービスへの読み取りアクセスを提供します

レビューと割り当て

前へ

次へ

1 クリック

2 クリック

8. [アクセスの割り当て先] を選択し、[メンバーを選択する] をクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > サブスクリプション > サブスクリプション > | アクセス制御 (IAM) >

ロールの割り当ての追加

ロール

メンバー

レビューと割り当て

選択されたロール

閲覧者

1 「閲覧者」が選択されていることを確認

アクセスの割り当て先

☒ ユーザー、グループ、またはサービス プリンシパル

☐ マネージド ID

2 選択

メンバー

+ メンバーを選択する

3 クリック

名前	オブジェクト ID	種類
メンバーが選択されていません		

Description

省略可能

レビューと割り当て

前へ

次へ

9. 登録したアプリを選び、[選択] ボタンをクリックします。

メンバーを選択する

1 アプリ登録のときにつけた名前を検索
(例: Quick MONITOR)

選択 



2 クリック

選択したメンバー:



削除

3 選択されていることを確認

4 クリック

選択

閉じる

10. 入力内容を確認後、[レビューと割り当て] ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > サブスクリプション > サブスクリプション > | アクセス制御 (IAM) >

ロールの割り当ての追加

ロール

メンバー

レビューと割り当て

選択されたロール

閲覧者

アクセスの割り当て先

☒ ユーザー、グループ、またはサービス プリンシパル

☐ マネージド ID

メンバー

+ メンバーを選択する

名前	オブジェクト ID	種類
		アプリ

Description

省略可能

1 選択したアプリが表示されていることを確認

2 クリック

レビューと割り当て

前へ

次へ

3. その他の事前準備

Database インスタンスを監視対象に含めない場合は「4. 初期設定ウィザード」に進んでください。

ここでは、Database インスタンスの監視を行うために必要な認証情報の用意と、アクセス許可設定を行います。

1. データベース認証用情報の用意

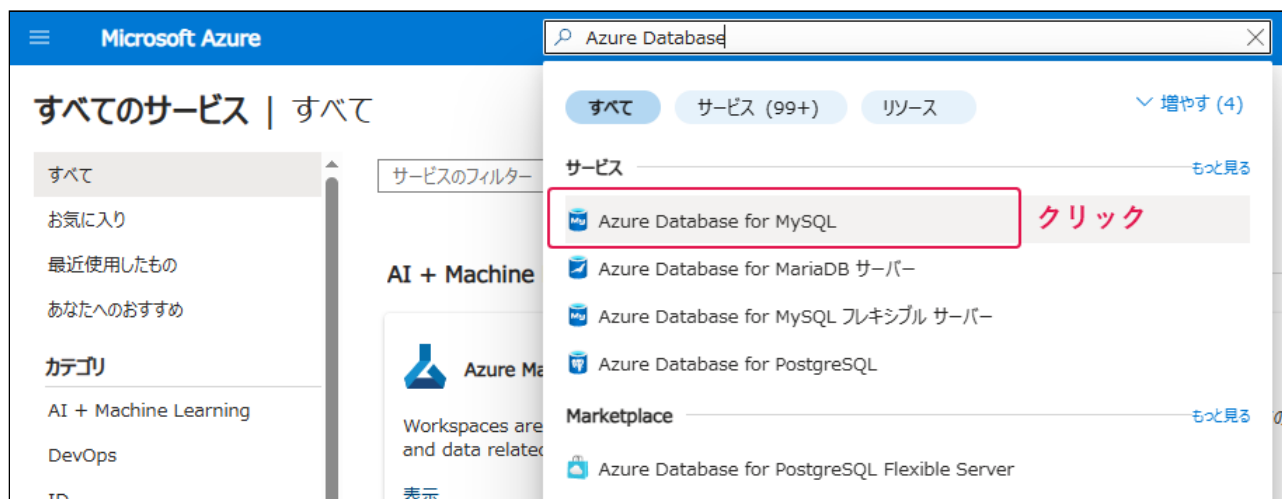
データベースの認証情報をご用意ください。

- MySQL ユーザー
- MySQL パスワード

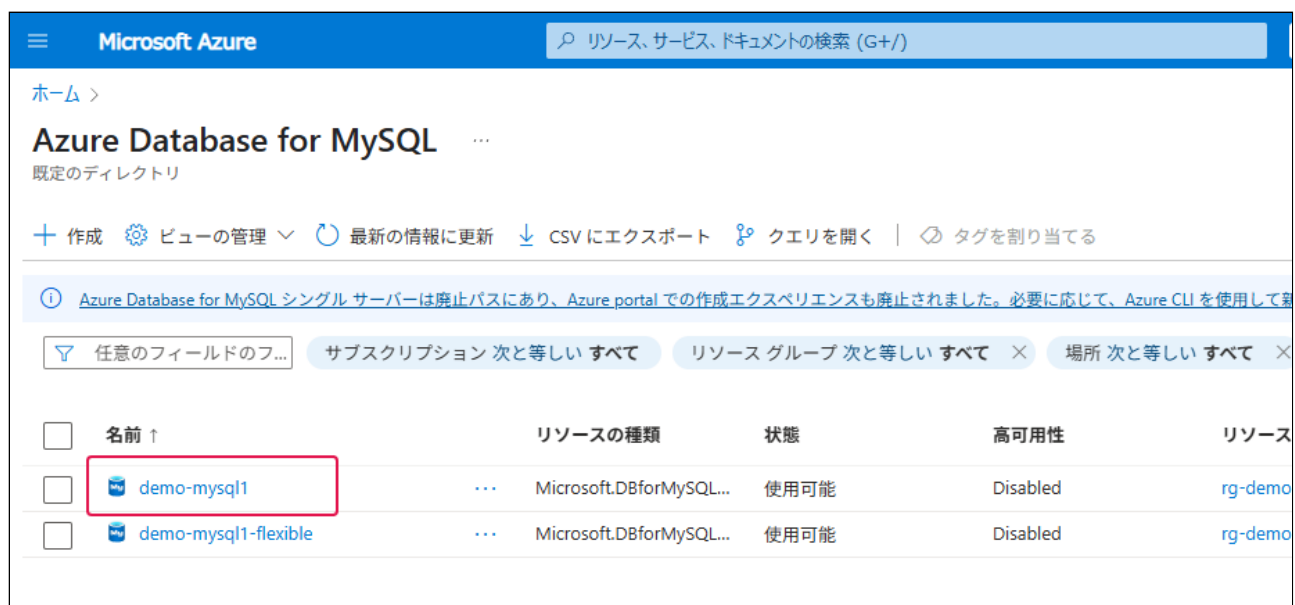
2. MySQL へのアクセス許可設定

Azure Portal にサインインして操作してください。

1. Azure Database for MySQL サービスを開きます。



2. アクセス許可を行いたいインスタンス名をクリックします。



3. [設定] の [ネットワーク] を開きます。

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and navigation menu. The breadcrumb trail is 'ホーム > Azure Database for MySQL > demo-mysql1'. The left sidebar contains a list of settings: '概要' (Overview), 'アクティビティ ログ' (Activity Log), 'アクセス制御 (IAM)' (Access Control (IAM)), 'タグ' (Tags), '問題の診断と解決' (Troubleshooting), 'Learning center', 'リソース ビジュアライザー' (Resource Visualizer), and '設定' (Settings). Under '設定', 'コンピューティングとストレージ' (Compute and Storage) is expanded, and 'ネットワーク' (Network) is highlighted with a red rectangular box. The main content area displays the 'demo-mysql1' resource details under the '基本' (Basic) tab. It includes fields for 'サブスクリプション' (Subscription), 'サブスクリプション ID' (Subscription ID), 'リソース グループ' (Resource Group) set to 'rg-demo', '状態' (Status) as 'Ready', and '場所' (Location) as 'Japan East'. There are also links for 'タグ (編集)' (Tags) and 'タグの追加' (Add tag). At the bottom of the main content area, there are tabs for 'はじめに' (Get started), 'プロパティ' (Properties), '推奨' (Recommendations), '監視中' (Monitoring), and 'チュートリアル' (Tutorials).

4. [パブリックアクセス] にチェックを入れます。

The screenshot shows the 'demo-mysql1 | ネットワーク' (Network) page in the Microsoft Azure portal. The breadcrumb trail is 'ホーム > Azure Database for MySQL > demo-mysql1'. The left sidebar is the same as in the previous screenshot, with '設定' (Settings) expanded and 'ネットワーク' (Network) selected. The main content area is titled 'demo-mysql1 | ネットワーク' and includes a search bar and action buttons like '保存' (Save), '破棄' (Delete), 'SSL 証明書のダウンロード' (Download SSL certificate), 'フィードバック' (Feedback), and 'FAQ'. The page contains several sections: 'TLS/SSL 接続が適用されました' (TLS/SSL connection applied), 'パブリック アクセス' (Public Access), and 'ファイアウォール規則' (Firewall rules). The 'パブリック アクセス' section has a checkbox labeled 'パブリック IP アドレスを使用したインターネット経由でのこのリソースへのパブリック アクセスを許可する' (Allow public access to this resource over the Internet using public IP addresses), which is checked and highlighted with a red rectangular box. The 'ファイアウォール規則' section mentions that inbound connections from specified IP addresses to port 3306 are allowed.

5. ファイアウォール規則を入力します。

- ファイアウォール規則名: 任意 (例: Quick MONITOR)
- 開始 IP アドレス: 本サービスの利用開始時にお知らせしている IP アドレス
- 終了 IP アドレス: 本サービスの利用開始時にお知らせしている IP アドレス

ファイアウォール規則
以下で指定した IP アドレスからのインバウンド接続は、このサーバーのポート 3306 に対して許可されます。 [詳細情報](#)

一部のネットワーク環境では、サーバーにアクセスするのに必要な実際の公開 IP アドレスを報告しない可能性があります。IP アドレスを追加してもサーバーにアクセスできない場合は、ネットワーク管理者にお問い合わせください。

☒ Azure 内の任意の Azure サービスにこのサーバーへのパブリック アクセスを許可する ①

+ 現在のクライアント IP アドレスを追加する () + 0.0.0.0 から 255.255.255.255 を追加する

ファイアウォール規則名	開始 IP アドレス	終了 IP アドレス	

6. [保存] をクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Azure Database for MySQL > demo-mysql1

demo-mysql1 | ネットワーク ☆ ...

Azure Database for MySQL のフレキシブル サーバー

検索

保存

破棄

SSL 証明書のダウンロード

フィードバック

FAQ

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

問題の診断と解決

Learning center

リソース ビジュアライザー

TLS/SSL 接続が適用されました

既定では、TLS/SSL がサーバーに適用されます。上記のメニューから SSL パブリック証明書をダウンロードできます。SS
ください。
stls_version サーバー パラメーターを設定して、TLS のバージョンを変更することもできます。 [詳細情報](#)

パブリック アクセス

☒ パブリック IP アドレスを使用したインターネット経由でのこのリソースへのパブリック アクセスを許可する ①

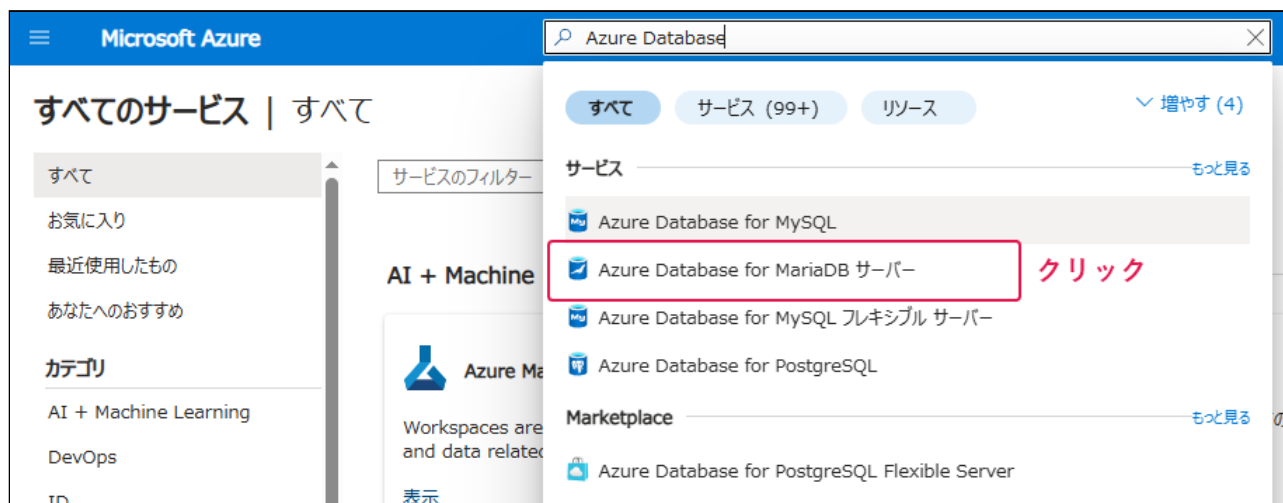
ファイアウォール規則

16 / 29

3. MariaDB へのアクセス許可設定

Azure Portal にサインインして操作してください。

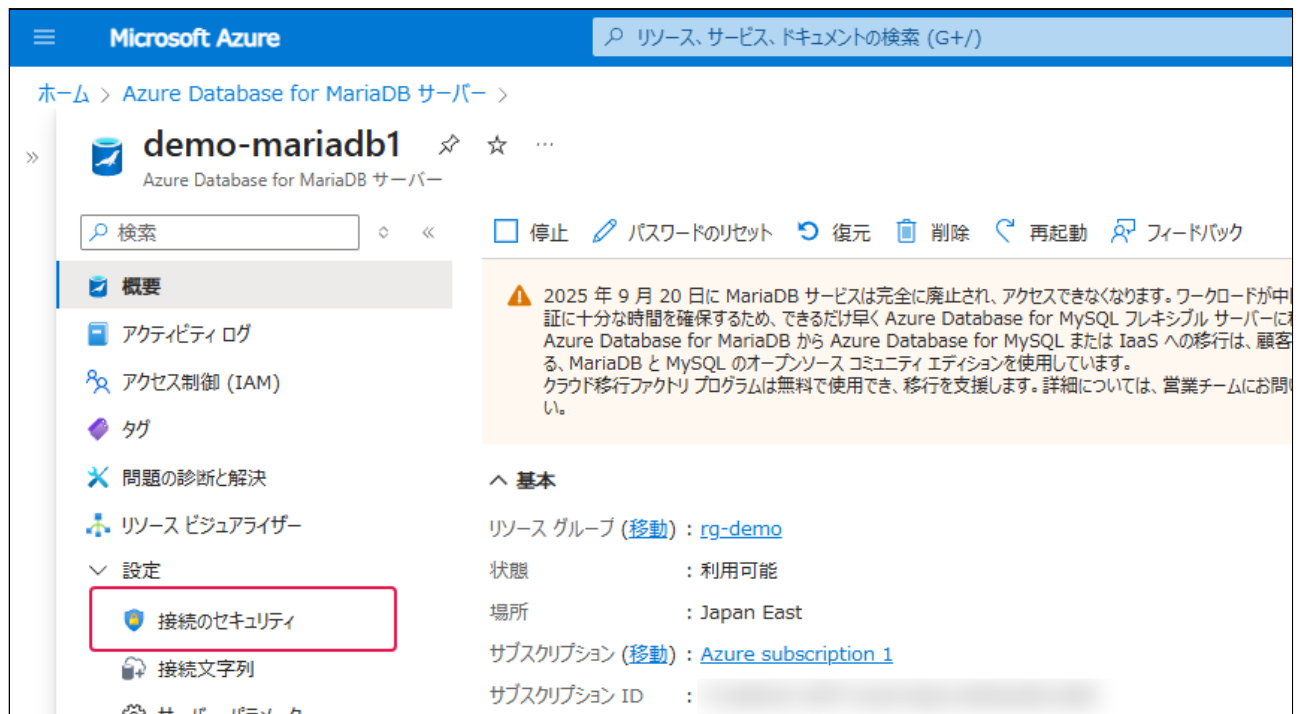
1. Azure Database for MariaDB サーバー サービスを開きます。



2. アクセス許可を行いたいインスタンス名をクリックします。



3. [設定] の [接続のセキュリティ] を開きます。



Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Azure Database for MariaDB サーバー >

demo-mariadb1

Azure Database for MariaDB サーバー

検索

停止 パスワードのリセット 復元 削除 再起動 フィードバック

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

問題の診断と解決

リソース ビジュアライザー

設定

接続のセキュリティ

接続文字列

サーバー パラメーター

2025 年 9 月 20 日に MariaDB サービスは完全に廃止され、アクセスできなくなります。ワークロードが中証に十分な時間を確保するため、できるだけ早く Azure Database for MySQL フレキシブル サーバーに Azure Database for MariaDB から Azure Database for MySQL または IaaS への移行は、顧客、MariaDB と MySQL のオープンソース コミュニティ エディションを使用しています。クラウド移行ファクトリ プログラムは無料で使用でき、移行を支援します。詳細については、営業チームにお問い合わせ。

基本

リソース グループ (移動) : rg-demo

状態 : 利用可能

場所 : Japan East

サブスクリプション (移動) : Azure subscription 1

サブスクリプション ID :

4. ファイアウォール規則を入力します。

- ファイアウォール規則名: 任意 (例: Quick MONITOR)
- 開始 IP: 本サービスの利用開始時にお知らせしている IP アドレス
- 終了 IP: 本サービスの利用開始時にお知らせしている IP アドレス



ファイアウォール規則

一部のネットワーク環境では、サーバーにアクセスするのに必要な実際の公開 IP アドレスを報告しない可能性があります。IP アドレスを追加してもサーバーにアクセスできない場合は、ネットワーク管理者にお問い合わせください。

Azure サービスへのアクセスを許可 ☒ いいえ ☐ はい

+ 現在のクライアント IP アドレスを追加する () + 0.0.0.0 から 255.255.255.255 を追加する

ファイアウォール規則名	開始 IP	終了 IP
ファイアウォール規則名	開始 IP	終了 IP

5. [保存] をクリックします。

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb navigation shows 'ホーム > Azure Database for MariaDB サーバー > demo-mariadb1'. The main content area is titled 'demo-mariadb1 | 接続のセキュリティ' (demo-mariadb1 | Connection Security). On the left, there's a sidebar with navigation links: '概要' (Overview), 'アクティビティ ログ' (Activity Log), 'アクセス制御 (IAM)' (Access Control (IAM)), 'タグ' (Tags), '問題の診断と解決' (Troubleshooting and Resolution), and 'リソース プロビジョニング' (Resource Provisioning). The main content area has a search bar and a toolbar with buttons: '保存' (Save), '破棄' (Delete), and 'クライアント IP の追加' (Add Client IP). The '保存' button is highlighted with a red box. Below the toolbar, there's a section titled 'ファイアウォール規則' (Firewall Rule). It contains an information icon and a message: '一部のネットワーク環境では、サーバーにアクセスするのに必要な実際の公開 IP アドレスを指定してください。' (In some network environments, you must specify the actual public IP address required to access the server). At the bottom, there's a toggle switch for 'Azure サービスへのアクセスを許可' (Allow access to Azure services), which is currently set to 'いいえ' (No).

4. 初期設定ウィザード

ここでは、Quick MONITOR の初期設定を行います。

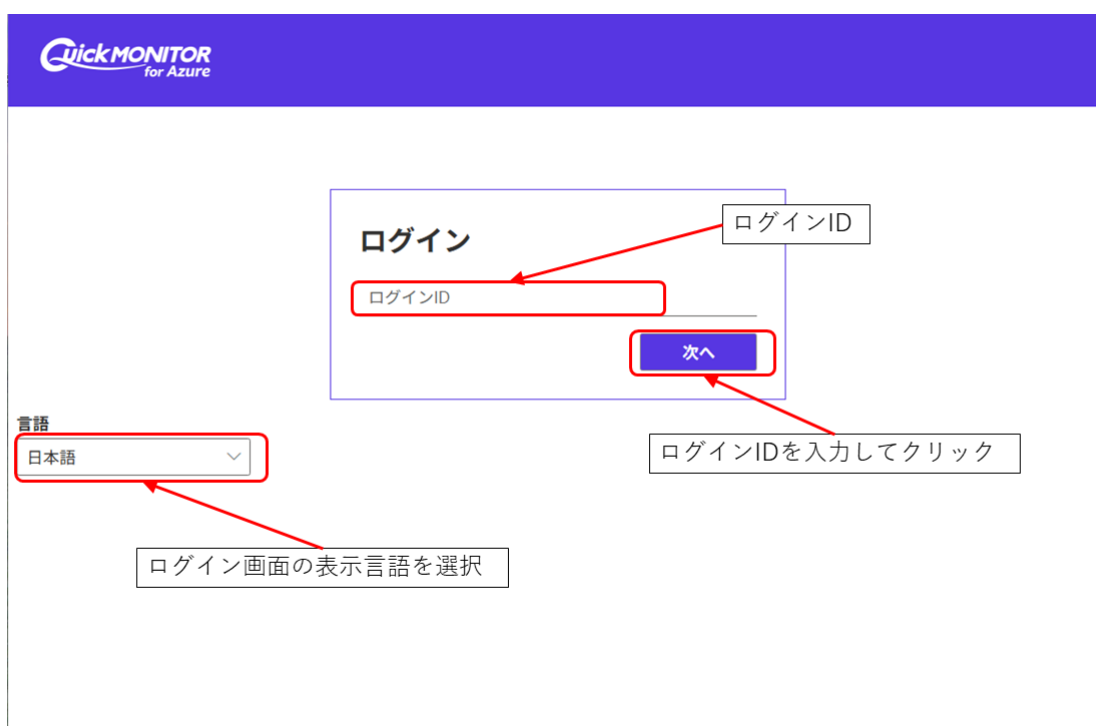
初期設定を進める前に、必要に応じて以下の事前準備を実施してください。

- 自動復旧設定を有効にしたい場合
 - [リファレンスガイド] の「事前準備 - 1. 自動復旧機能に必要な権限の設定」
- 通知方法に Teams を選択したい場合
 - [リファレンスガイド] の「事前準備 - 2. Teams を通知方法として選択する場合の準備」

0. ログイン

ブラウザでサービス提供URLにアクセスして、ログイン画面を表示します。

- ログインIDを入力して、[次へ] ボタンをクリックします。



- 画面が切り替わったら、パスワードを入力して、[ログイン] ボタンをクリックします。

The screenshot shows the login interface for QuickMonitor for Azure. The header is a solid blue bar with the 'QuickMONITOR for Azure' logo on the left. The main content area is white. On the left side, there is a language selection dropdown menu labeled '言語' (Language) with '日本語' (Japanese) selected. In the center, there is a login form. A purple rectangular box highlights the password input field and the login button. Inside this box, the text 'パスワードを入力' (Enter password) is displayed above the input field. The input field itself contains the placeholder text 'パスワード'. To the right of the input field is a blue button with the white text 'ログイン' (Login). Red arrows point from external text boxes to the form elements: one arrow points from a box labeled 'パスワード' to the input field, and another arrow points from a box labeled 'パスワードを入力してクリック' (Click after entering password) to the login button.

1. 初期設定ウィザード Step1: Azure API アクセスの設定

事前準備で用意した下記の各Azure API 認証情報を該当する欄に記述して、[次へ] ボタンをクリックします。

- クライアントID
- アプリケーションシークレット
- テナントまたはドメイン名
- サブスクリプションID

The screenshot shows the 'QuickMONITOR for Azure' initial setup wizard. The top navigation bar is purple with the logo on the left and a user icon on the right. Below the bar is a progress indicator with six steps: 1. Azure API アクセスの設定 (selected), 2. メトリック収集設定, 3. 警告と障害条件設定, 4. 自動復旧設定, 5. 通知設定, and 6. 完了. The main content area is white and contains a welcome message: 'QuickMONITOR for Azure へようこそ'. Below the message is a form with four input fields: 'クライアントID', 'アプリケーションシークレット' (with an eye icon for toggling visibility), 'テナントまたはドメイン名', and 'サブスクリプションID'. A blue '次へ' (Next) button is located at the bottom right of the form.

QuickMONITOR for Azure へようこそ

QuickMONITOR を使い始めるために Azure API の認証情報を入力します。
これらの情報は、QuickMONITOR がメトリックを収集するのに使われます。

クライアントID

アプリケーションシークレット

テナントまたはドメイン名

サブスクリプションID

次へ

現在の権限で利用可能な機能にチェックマークがついています。
もし必要な機能が利用不可能な場合、Azure Portal で権限設定を確認してください。
その後、「権限を再確認する」ボタンをクリックしてください。
確認した内容に問題がなければ「次へ」ボタンをクリックしてください。

1

2

3

4

5

6

Azure API アクセスの設定

メトリック収集設定

警告と障害条件設定

自動復旧設定

通知設定

完了

Azure API アクセス設定の確認

現在の権限で利用可能な機能:

✓ 情報収集・アラート通知

✓ 自動復旧

✓ Virtual Machines

✓ Azure Database for MySQL servers

✓ Azure Database for MySQL flexible servers

✓ Azure Database for MariaDB servers

チェックマークがついた機能が現在利用可能です。
もし必要な機能が利用不可能な場合、Azure Portal で権限設定を確認してください。その後、「権限を再確認する」ボタンをクリックしてください。
確認した内容に問題がなければ「次へ」ボタンをクリックしてください。
必要な機能が決まっていない場合、この設定はあとから変更できます。

認証情報を再入力する

次へ

権限を再確認する

2. 初期設定ウィザード Step2: メトリック収集設定

1. メトリック収集設定 (Virtual Machines)

対象インスタンス 欄に、Virtual Machines インスタンスが表示されます。

この欄内にあるインスタンスを対象に情報収集が行われます。

監視するインスタンスが表示の通りで問題なければ、[適用] ボタンをクリックします。

The screenshot shows the 'Metrics Collection Setup' step (Step 2) of the Azure Monitor initial setup wizard. The progress bar at the top indicates the current step. The 'Target Instances' section lists several VMs: RG-DEMO/demo-vm1, RG-DEMO/demo-vm2, RG-DEMO/demo-vm3, RG-DEMO/demo-vm4, and RG-DEMO/demo-vm5. A red box highlights the first two VMs, with a note '監視対象のインスタンス' (Instances to be monitored) and '× をクリックで対象から除外' (Click × to exclude from target). Another red box highlights the remaining three VMs, with a note 'クリックで対象インスタンスに移動' (Click to move to target instances). The 'Interval' section on the right shows '1 時間' (1 hour) selected, with options for '30 分' (30 min) and '5 分' (5 min). A red box highlights the '適用' (Apply) button, with a note '設定を適用して次に進む' (Apply settings and proceed to the next step). A red box highlights the 'Virtual Machines の設定をスキップ' (Skip Virtual Machines settings) button, with a note 'Virtual Machines の監視を行わない' (Do not monitor Virtual Machines). A red arrow points to the '適用' button with the text '設定を適用して次に進む'.

2. メトリック収集設定 (Database)

対象インスタンス 欄に、Database インスタンスが表示されます。

この欄内にあるインスタンスを対象に情報収集が行われます。

監視するインスタンスが表示の通りで問題なければ、MySQL ユーザー および MySQL パスワード を入力し、[適用] ボタンをクリックします。

インスタンスごとに MySQL ユーザー と MySQL パスワード を変更したい場合には、[Add] ボタンをクリックして入力欄を増やすことで対応できます。

The screenshot shows the 'Metrics Collection Setup' step (Step 2) of the Azure Monitor initial setup wizard for Database. The progress bar at the top indicates the current step. The 'Target Instances' section lists two database instances: rg-demo/demo-mariadb1 and rg-demo/demo-mysql1. A red box highlights the first instance, with a note '監視対象のインスタンス' (Instances to be monitored) and '× をクリックで対象から除外' (Click × to exclude from target). Another red box highlights the second instance, with a note 'クリックで対象インスタンスに移動' (Click to move to target instances). The 'MySQL User' and 'MySQL Password' fields are visible, with a red box highlighting the password field and a note 'データベースの認証情報を入力' (Enter database authentication information). The 'Interval' section on the right shows '1 時間' (1 hour) selected, with options for '30 分' (30 min) and '5 分' (5 min). A red box highlights the '適用' (Apply) button, with a note '設定を適用して次に進む' (Apply settings and proceed to the next step). A red box highlights the 'Database の設定をスキップ' (Skip Database settings) button, with a note 'Database の監視を行わない' (Do not monitor Database). A red arrow points to the '適用' button with the text '設定を適用して次に進む'.

3. メトリック収集設定 (URL)

監視したいWebサイトのURLを入力して [適用] ボタンをクリックします。

3. 初期設定ウィザード Step3: 警告と障害条件設定

ここでは、おすすめ設定のまま変更せず進みます。

警告と障害条件設定をカスタマイズしたい場合は「リファレンスガイド」の「警告と障害条件設定の変更」をご参照ください。

ここまでの操作で、監視対象として選択してきたインスタンスやWebサイトが一覧表示されます。

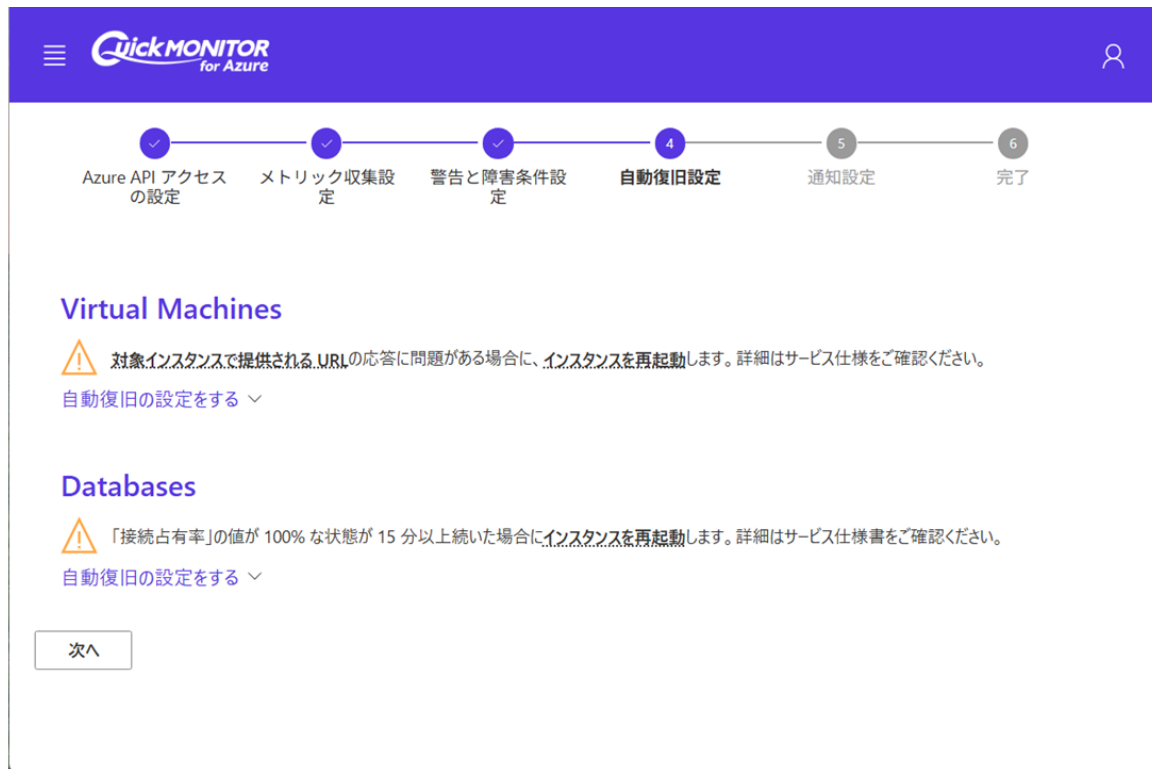
[次へ] ボタンをクリックして進みます。

4. 初期設定ウィザード Step4: 自動復旧設定

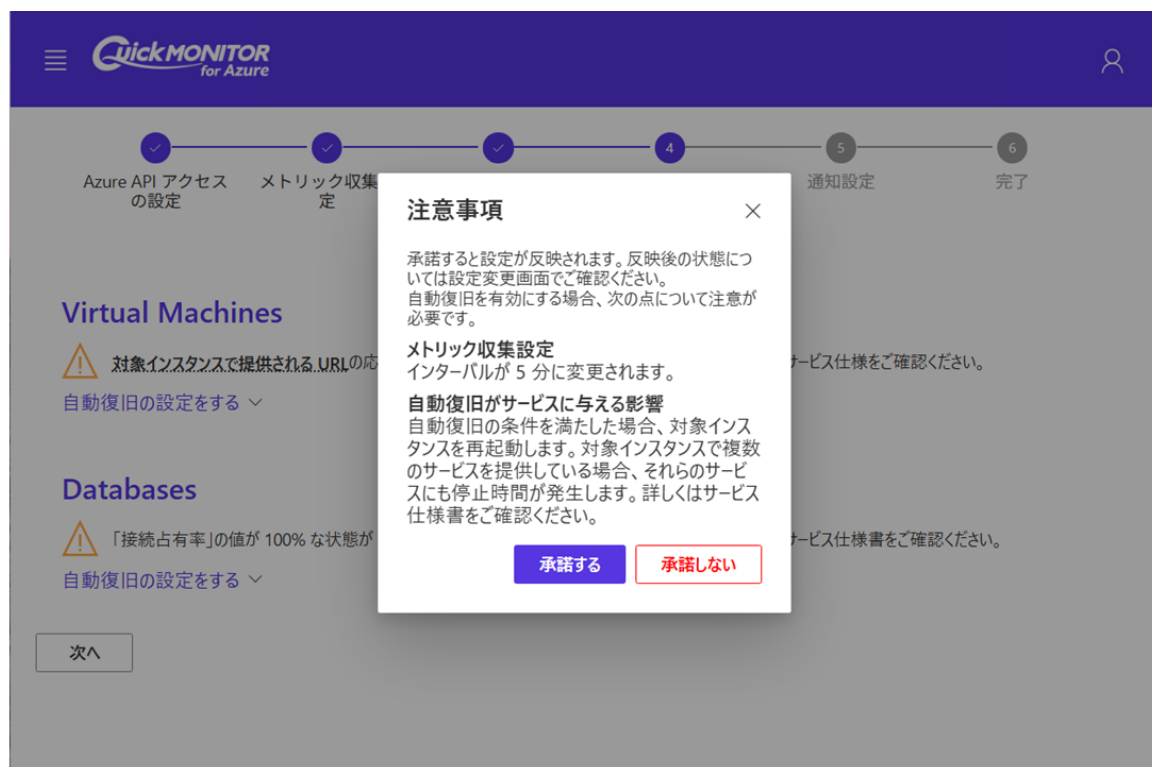
ここでは自動復旧を有効にせず次に進みます。

自動復旧を有効にしたい場合は「リファレンスガイド」の「自動復旧設定の変更」をご参照ください。

[次へ] ボタンをクリックして進みます。



[承諾する] ボタンをクリックして進みます。



5. 初期設定ウィザード Step5: 通知設定

ここでは通知方法に「メール」を選択して進みます。
メール以外について詳しく知りたい場合は、別冊「リファレンスガイド」の「通知設定の変更」をご確認ください。

警告または障害条件を満たした場合の通知先を設定します。通知方法は次の中から選択できます。

- メール
- 電話
- Slack
- LINE
- ChatWork
- Mattermost
- Teams (Text)
- Teams (Call)

通知方法を選択し、各パラメータを入力したら [次へ] ボタンをクリックします。

通知方法

メール

recipient

user@example.com

次へ

プルダウンメニューから「メール」を選択

- 通知先のメールアドレスを記述する
- 通知先のメールアドレスは、"," で区切って複数登録可能

設定を反映する

6. 初期設定ウィザード Step6: 完了

この画面が表示されたら、初期設定はひととおり完了です。

[ダッシュボード] ボタンをクリックします。



初期設定ウィザードを終えたあとの設定変更について

初期設定ウィザードで設定したすべての項目は、あとからでも設定変更できます。
詳しくは、別冊の [リファレンスガイド] をご参照ください。

- 監視するインスタンスの追加・削除
- 監視設定の変更
- 通知設定の変更
- ユーザープロファイルの変更