

リファレンスガイド

本書について

本書では、Quick MONITOR の各種監視項目の設定方法について説明しています。

はじめてQuick Monitorをお使いになる方は、別冊のクイックスタートをご参照ください。

目次

- 事前準備
 - 1. 自動復旧機能に必要な権限の設定
 - Virtual Machines の自動復旧を有効化したい場合
 - Azure Database for Maria DB の自動復旧を有効化したい場合
 - Azure Database for MySQL フレキシブルサーバーの自動復旧を有効化したい場合
 - 2. Teams を通知方法として選択する場合の準備
 - Teams (テキスト) を利用する場合
 - Teams (音声) を利用する場合
 - Teams Developer Portal でアプリ登録
 - 登録したアプリに対して Azure Portal で権限を付与
 - 認証情報の発行
- 監視するインスタンスの追加・削除
 - Virtual Machines
 - Database
 - URL
- 警告と障害条件設定の変更
 - Virtual Machines
 - Database
 - URL
 - 共通
- 自動復旧設定の変更
- 通知設定の変更
 - 通知方法「メール」
 - 通知方法「Slack」
 - 通知方法「LINE」
 - 通知方法「Chatwork」
 - 通知方法「Mattermost」
 - 通知方法「Teams (テキスト)」
 - 通知方法「Teams (音声)」
- AzureAPIアクセスの設定
 - AzureAPIアクセスの設定の変更
- ダッシュボード
 - Board1 (マネージャー向け)
 - Board2 (監視オペレーター向け)
- その他
 - 言語の変更
 - タイムゾーンの変更
 - パスワードの変更
 - ログアウト

事前準備

1. 自動復旧機能に必要な権限の設定

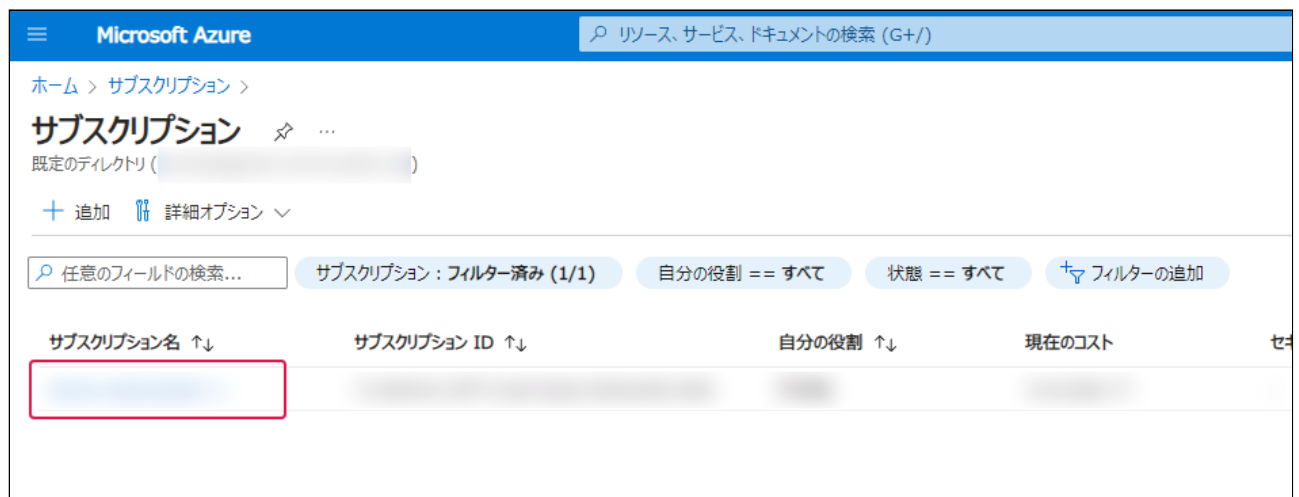
自動復旧機能を有効化したい場合は、インスタンスの再起動権限が必要です。

Virtual Machines の自動復旧を有効化したい場合

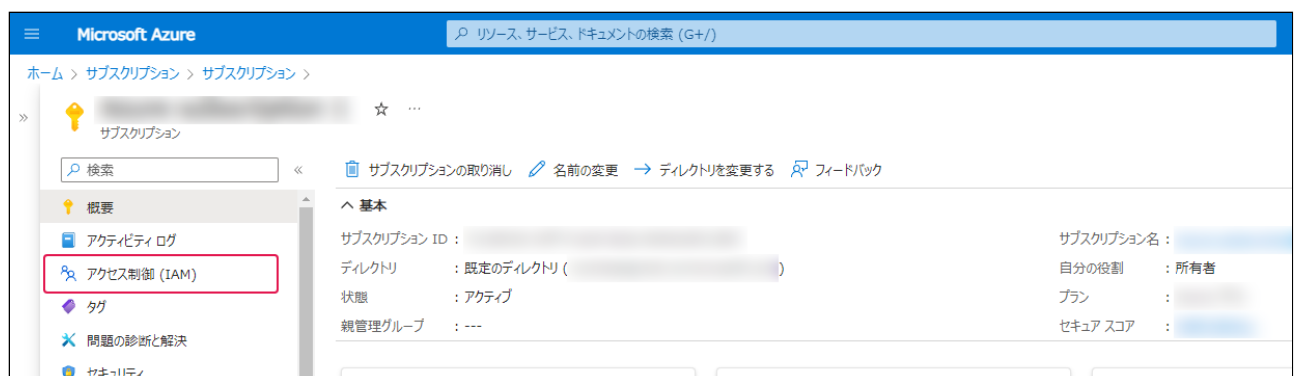
1. [Azure portal](#)にサインインします。
2. サブスクリプション サービスを開きます。



3. 任意のサブスクリプションを選びます。



4. [アクセス制御 (IAM)] を開きます。



5. [追加] のメニューから [カスタムロールの追加] を選びます。



6. 任意のカスタムロール名を入力し、[次へ] をクリックします。



7. [アクセス許可の追加] 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+)

Copilot

ホーム > サブスクリプション > | アクセス制御 (IAM) >

カスタム ロールを作成する

基本 **アクセス許可** 割り当て可能なスコープ JSON 確認と作成

+ アクセス許可の追加 + 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールに追加するアクセス許可を選択します。
ワイルドカード (*) のアクセス許可を追加するには、そのアクセス許可を [JSON] タブに手動で追加する必要があります。 [詳細情報を見る](#)
ワイルドカードのアクセス許可から特定のアクセス許可を除外するには、[権限を除外する] をクリックします。 [詳細情報を見る](#)

権限	↑↓	説明	↑↓	アクセス許可の種類	↑↓
表示するアクセス許可はありません。					

アクセス許可の追加

8. 検索欄に `Microsoft.Compute/virtualMachines/restart/action` を入力し、[Microsoft Compute] 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+)

Copilot

ホーム > サブスクリプション >

カスタム ロールを作成する

基本 **アクセス許可** 割り当て可能なスコープ

+ アクセス許可の追加 + 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールに追加するアクセス許可を選択します。
ワイルドカード (*) のアクセス許可を追加するには、そのアクセス許可を [JSON] タブに手動で追加する必要があります。 [詳細情報を見る](#)
ワイルドカードのアクセス許可から特定のアクセス許可を除外するには、[権限を除外する] をクリックします。 [詳細情報を見る](#)

アクセス許可の追加

① カスタム ロールに追加するアクセス許可を検索します。たとえば、仮想マシンに関連するアクセス許可を検索するには、「仮想マシン」

Microsoft.Compute/virtualMachines/restart/action **1 検索**

Microsoft Compute
クラウド コンピューティングの容量とスケール オンデマンド (仮想マシンなど) にアクセスし、使用するリソースのみの料金を支払います。

2 クリック

9. [その他: 仮想マシンの再起動] にチェックをいれて [追加] 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+)

Copilot

ホーム > サブスクリプション >

カスタム ロールを作成する

基本

アクセス許可

割り当て可能なスコープ

+ アクセス許可の追加

+ 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールにワイルドカード (*) のアクセス許可を追加するには、そのワイルドカードのアクセス許可から特定のアクセス許可を選択します。

権限

表示するアクセス許可はありません。

Microsoft.Compute のアクセス許可

< すべてのリソース プロバイダー

カスタム ロールに追加するアクセス許可を検索します。たとえば、仮想マシンに関連するアクセス許可を検索するには、"仮想マシン" を検索します。

Microsoft.Compute/virtualMachines/restart/action

Actions

データ アクション

権限

説明

Microsoft.Compute/virtualMachines

その他 : 仮想マシンの再起動 ⓘ

仮想マシンを再起動します

1 チェックをいれる

2 クリック

確認と作成

前へ

次へ

追加

キャンセル

6 / 122

10. [確認と作成] 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+/)

Copilot

ホーム > サブスクリプション > | アクセス制御 (IAM) >

カスタム ロールを作成する

基本

アクセス許可

割り当て可能なスコープ

JSON

確認と作成

+ アクセス許可の追加

+ 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールに追加するアクセス許可を選択します。
ワイルドカード (*) のアクセス許可を追加するには、そのアクセス許可を [JSON] タブに手動で追加する必要があります。 [詳細情報を見る](#)
ワイルドカードのアクセス許可から特定のアクセス許可を除外するには、[権限を除外する] をクリックします。 [詳細情報を見る](#)

権限	説明	アクセス許可の種類
Microsoft.Compute/virtualMachines/restart/...	仮想マシンを再起動します	Action

確認と作成

前へ

次へ

11. [作成] 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 >

アクセス制御 (IAM) >

カスタム ロールを作成する ...

基本

アクセス許可

割り当て可能なスコープ

JSON

確認と作成

基本

ロール名	仮想マシンの再起動
ロールの説明	ロールの説明は提供されていません

アクセス許可

Action	Microsoft.Compute/virtualMachines/restart/action
--------	--

割り当て可能なスコープ

スコープ	/subscriptions/
------	-----------------

作成

前へ

12. [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。



13. [種別] をクリックし、[カスタムロール] を選びます。



14. 作成したカスタムロールを選んで、[次へ] 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 > | 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 条件 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](#)

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。

検索: 種類: カスタム ロール カテゴリ: すべて

名前 ↑↓	説明 ↑↓	種類 ↑↓	カテゴリ ↑↓
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
仮想マシンの再起動		CustomRole	なし

検索結果: 1 - 7 / 7 件。

レビューと割り当て 前へ **次へ** 2 クリック

15. [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 > | 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** 条件 レビューと割り当て

選択されたロール 仮想マシンの再起動

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 1 選択
☐ マネージド ID

メンバー **+ メンバーを選択する** 2 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

16. 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 ①

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

17. 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 >

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

条件

レビューと割り当て

選択されたロール

仮想マシンの再起動

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
QuickMONITOR Bot		アプリ

Description

省略可能

レビューと割り当て

前へ

次へ

18. 再度 [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 > | 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

条件

レビューと割り当て

ロール

仮想マシンの再起動

スコープ

/subscriptions/

メンバー	名前	オブジェクト ID	種類
	QuickMONITOR Bot		アプリ

説明

説明なし

レビューと割り当て

前へ

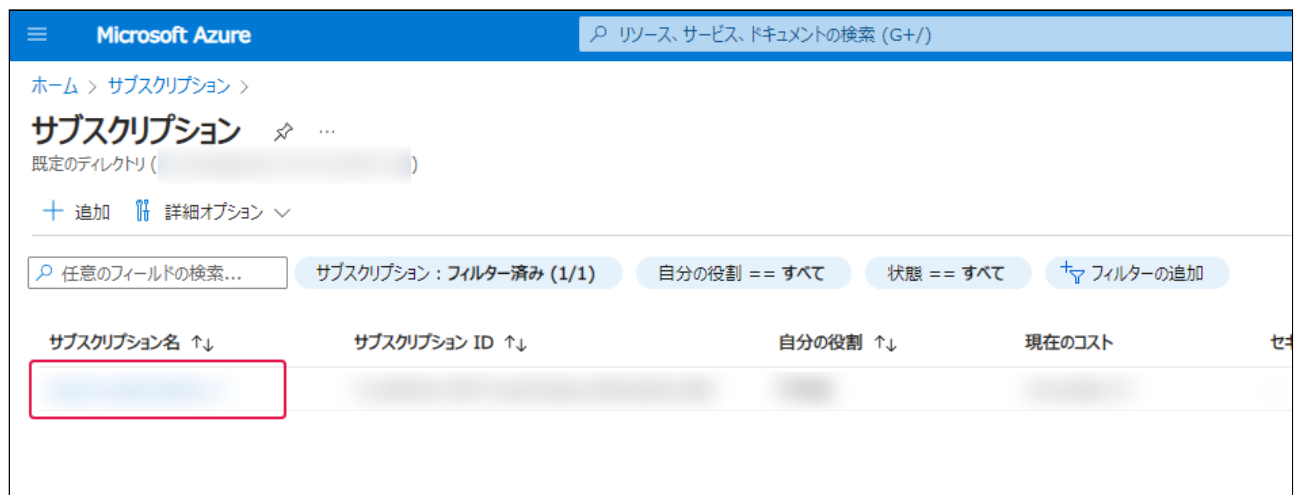
次へ

Azure Database for Maria DB の自動復旧を有効化したい場合

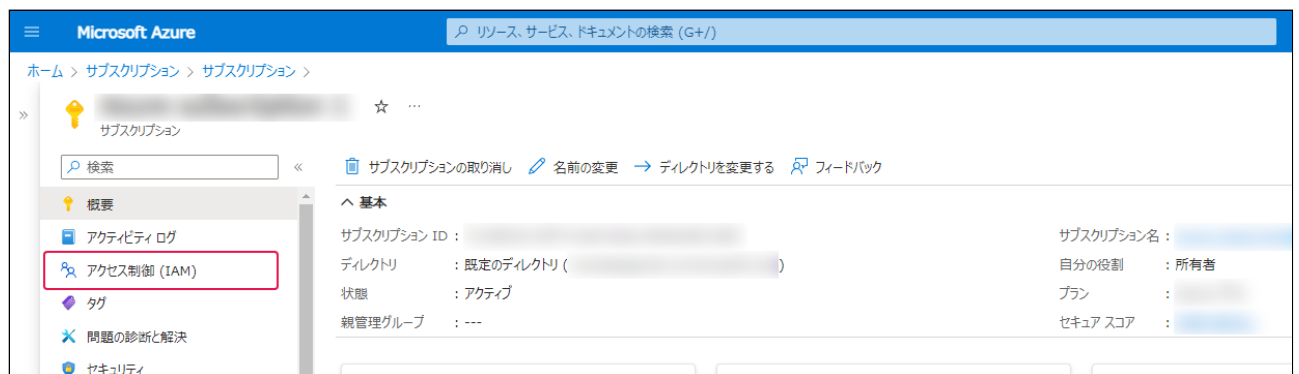
1. [Azure portal](#)にサインインします。
2. サブスクリプション サービスを開きます。



3. 任意のサブスクリプションを選びます。



4. [アクセス制御 (IAM)] を開きます。



5. [追加] のメニューから [カスタムロールの追加] を選びます。



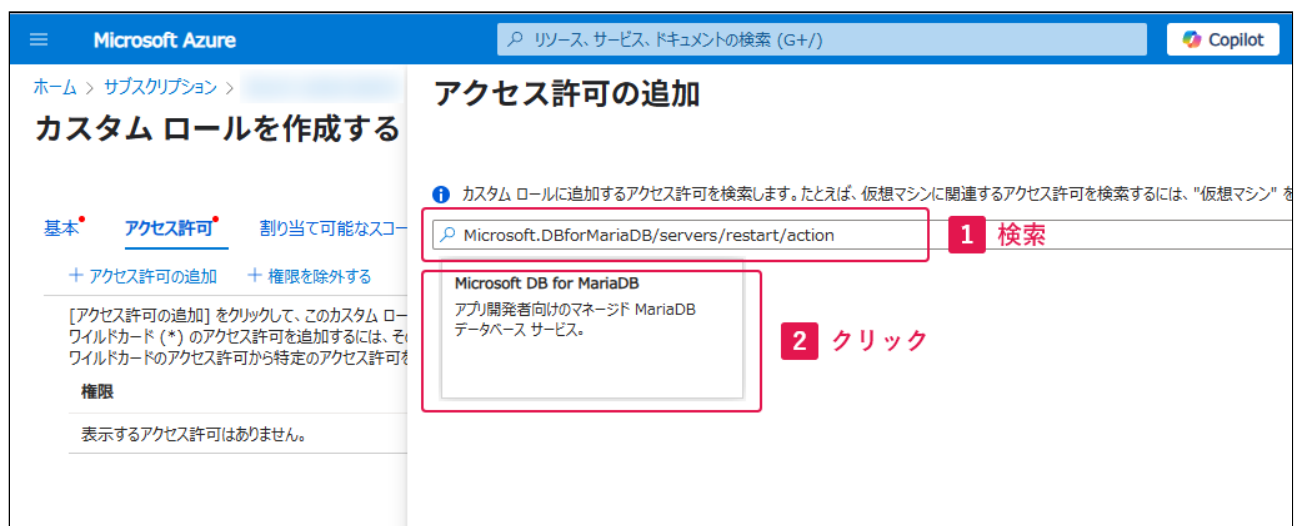
6. 任意のカスタムロール名を入力し、[次へ] をクリックします。



7. [アクセス許可の追加] をクリックします。



8. 検索欄に `Microsoft.DBforMariaDB/servers/restart/action` を入力し、[Microsoft DB for Maria DB] をクリックします。



9. [その他: Restart MariaDB Server] にチェックをいれて [追加] 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+)

Copilot

ホーム > サブスクリプション >

カスタム ロールを作成する

基本

アクセス許可

割り当て可能なスコア

+ アクセス許可の追加

+ 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールカード (*) のアクセス許可を追加するには、そのカードのアクセス許可から特定のアクセス許可を選択します。

権限

表示するアクセス許可はありません。

Microsoft.DBforMariaDB のアクセス許可

すべてのリソース プロバイダー

カスタム ロールに追加するアクセス許可を検索します。たとえば、仮想マシンに関連するアクセス許可を検索するには、「仮想マシン」を検索します。

Microsoft.DBforMariaDB/servers/restart/action

Actions

データ アクション

権限

説明

Microsoft.DBforMariaDB/servers

その他 : Restart MariaDB Server

Restarts a specific server.

1 チェックをいれる

2 クリック

追加

キャンセル

10. [確認と作成] 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+/)

Copilot

ホーム > サブスクリプション > | アクセス制御 (IAM) >

カスタム ロールを作成する ...

基本

アクセス許可

割り当て可能なスコープ

JSON

確認と作成

+ アクセス許可の追加

+ 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールに追加するアクセス許可を選択します。
ワイルドカード (*) のアクセス許可を追加するには、そのアクセス許可を [JSON] タブに手動で追加する必要があります。 [詳細情報を見る](#) 
ワイルドカードのアクセス許可から特定のアクセス許可を除外するには、[権限を除外する] をクリックします。 [詳細情報を見る](#) 

権限	↑↓	説明	↑↓	アクセス許可の種類	↑↓
Microsoft.DBforMariaDB/servers/restart/acti...		Restarts a specific server.		Action	

確認と作成

前へ

次へ

11. [作成] 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 >

| アクセス制御 (IAM) >

カスタム ロールを作成する ...

基本

アクセス許可

割り当て可能なスコープ

JSON

確認と作成

基本

ロール名	MariaDB Servers 再起動
ロールの説明	ロールの説明は提供されていません

アクセス許可

Action	Microsoft.DBforMariaDB/servers/restart/action
--------	---

割り当て可能なスコープ

スコープ	/subscriptions/
------	-----------------

作成

前へ

12. [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。



13. [種別] をクリックし、[カスタムロール] を選びます。



14. 作成したカスタムロールを選んで、[次へ] 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 > | 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 条件 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](#)

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。

検索: 種類: カスタム ロール カテゴリ: すべて

名前 ↑↓	説明 ↑↓	種類 ↑↓	カテゴリ ↑↓
MariaDB Servers 再起動		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし

検索結果: 1 - 7 / 7 件。

レビューと割り当て 前へ **次へ** 2 クリック

15. [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 > | 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** 条件 レビューと割り当て

選択されたロール MariaDB Servers 再起動

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 **1 選択**
☐ マネージド ID

メンバー **+ メンバーを選択する** **2 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

16. 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 ①

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

17. 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 >

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

条件

レビューと割り当て

選択されたロール

MariaDB Servers 再起動

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
QuickMONITOR Bot		アプリ

Description

省略可能

レビューと割り当て

前へ

次へ

18. 再度 [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 >

| 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

条件

レビューと割り当て

ロール	MariaDB Servers 再起動		
スコープ	/subscriptions/		
メンバー	名前	オブジェクト ID	種類
	QuickMONITOR Bot		アプリ
説明	説明なし		

レビューと割り当て

前へ

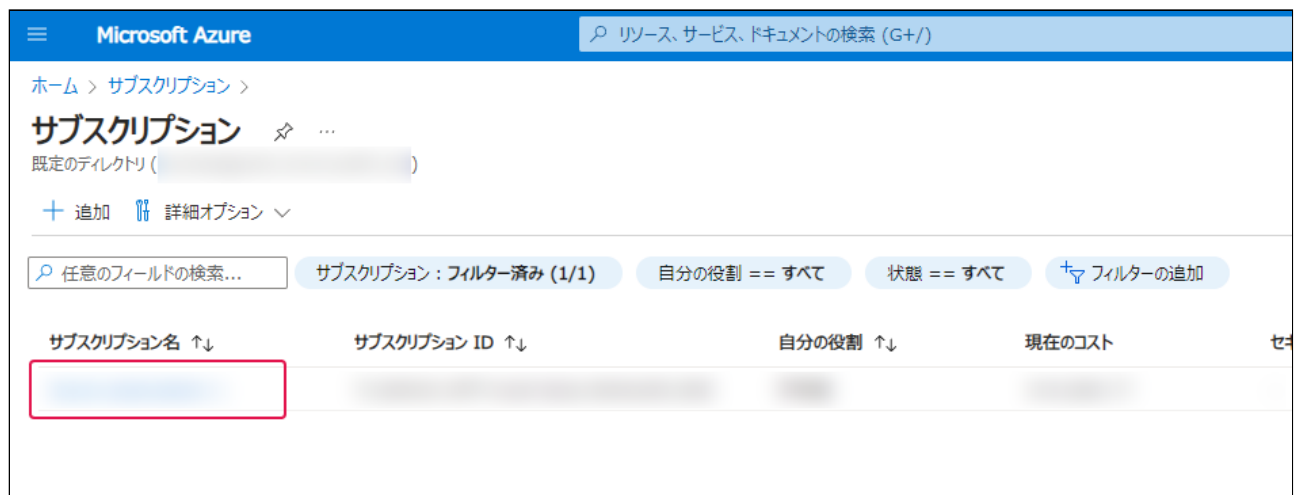
次へ

Azure Database for MySQL フレキシブルサーバーの自動復旧を有効化したい場合

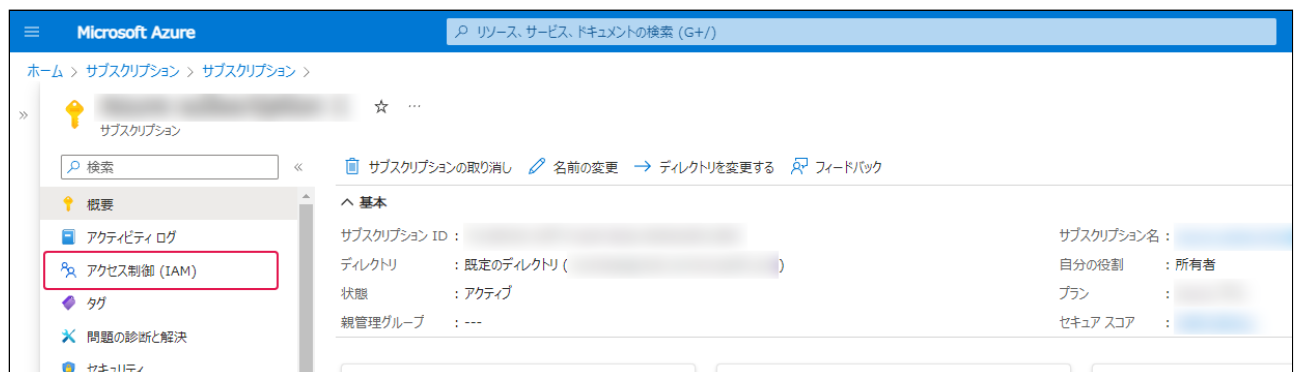
1. [Azure portal](#)にサインインします。
2. サブスクリプション サービスを開きます。



3. 任意のサブスクリプションを選びます。



4. [アクセス制御 (IAM)] を開きます。



5. [追加] のメニューから [カスタムロールの追加] を選びます。



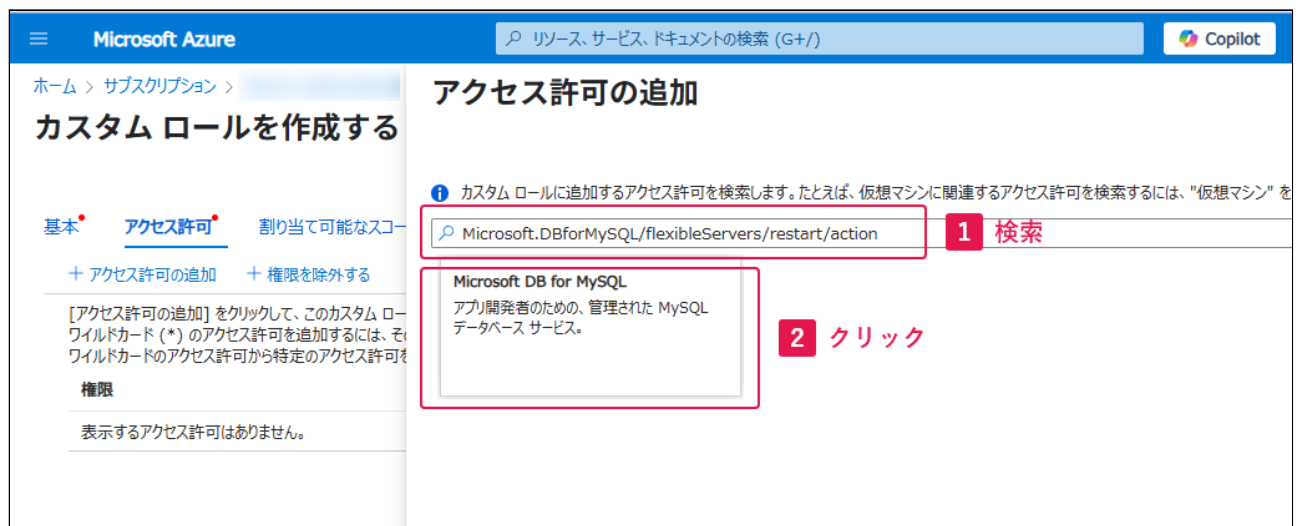
6. 任意のカスタムロール名を入力し、[次へ] をクリックします。



7. [アクセス許可の追加] をクリックします。



8. 検索欄に `Microsoft.DBforMySQL/flexibleServers/restart/action` を入力し、[Microsoft DB for MySQL] をクリックします。



9. [その他: Restart MySQL Server] にチェックをいれて [追加] 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+/)

Copilot

ホーム > サブスクリプション >

カスタム ロールを作成する

基本

アクセス許可

割り当て可能なスコープ

+ アクセス許可の追加

+ 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロール ワイルドカード (*) のアクセス許可を追加するには、そのワイルドカードのアクセス許可から特定のアクセス許可を選択します。

権限

表示するアクセス許可はありません。

Microsoft.DBforMySQL のアクセス許可

< すべてのリソース プロバイダー

カスタム ロールに追加するアクセス許可を検索します。たとえば、仮想マシンに関連するアクセス許可を検索するには、"仮想マシン" を検索します。

Microsoft.DBforMySQL/flexibleServers/restart/action

Actions

データ アクション

権限

説明

Microsoft.DBforMySQL/flexibleServers

その他 : Restart MySQL Server

Restarts a specific server.

1 チェックをいれる

2 クリック

確認と作成

前へ

次へ

追加

キャンセル

28 / 122

10. [確認と作成] 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+/)

Copilot

ホーム > サブスクリプション > | アクセス制御 (IAM) >

カスタム ロールを作成する ...

基本 **アクセス許可** 割り当て可能なスコープ JSON 確認と作成

+ アクセス許可の追加 + 権限を除外する

[アクセス許可の追加] をクリックして、このカスタム ロールに追加するアクセス許可を選択します。
ワイルドカード (*) のアクセス許可を追加するには、そのアクセス許可を [JSON] タブに手動で追加する必要があります。 [詳細情報を見る](#) 

ワイルドカードのアクセス許可から特定のアクセス許可を除外するには、[権限を除外する] をクリックします。 [詳細情報を見る](#) 

権限	↑↓	説明	↑↓	アクセス許可の種類	↑↓
Microsoft.DBforMySQL/flexibleServers/resta...		Restarts a specific server.		Action	

確認と作成

前へ

次へ

11. [作成] 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 >

アクセス制御 (IAM) >

カスタム ロールを作成する ...

基本

アクセス許可

割り当て可能なスコープ

JSON

確認と作成

基本

ロール名	MySQL Flexible Servers 再起動
ロールの説明	ロールの説明は提供されていません

アクセス許可

Action	Microsoft.DBforMySQL/flexibleServers/restart/action
--------	---

割り当て可能なスコープ

スコープ	/subscriptions/
------	-----------------

作成

前へ

12. [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。



13. [種別] をクリックし、[カスタムロール] を選びます。



14. 作成したカスタムロールを選んで、[次へ] 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 > | 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 条件 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](#)

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。

検索: 種類: カスタム ロール カテゴリ: すべて

名前 ↑↓	説明 ↑↓	種類 ↑↓	カテゴリ ↑↓
		CustomRole	なし
		CustomRole	なし
MySQL Flexible Servers 再起動		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし
		CustomRole	なし

検索結果: 1 - 7 / 7 件。

レビューと割り当て 前へ 次へ

15. [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 > | 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** 条件 レビューと割り当て

選択されたロール MySQL Flexible Servers 再起動

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

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

16. 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 ①

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

17. 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 > | 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

条件

レビューと割り当て

選択されたロール

MySQL Flexible Servers 再起動

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
QuickMONITOR Bot		アプリ

Description

省略可能

レビューと割り当て

前へ

次へ

18. 再度 [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 >

| 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

条件

レビューと割り当て

ロール	MySQL Flexible Servers 再起動		
スコープ	/subscriptions/		
メンバー	名前	オブジェクト ID	種類
	QuickMONITOR Bot		アプリ
説明	説明なし		

レビューと割り当て

前へ

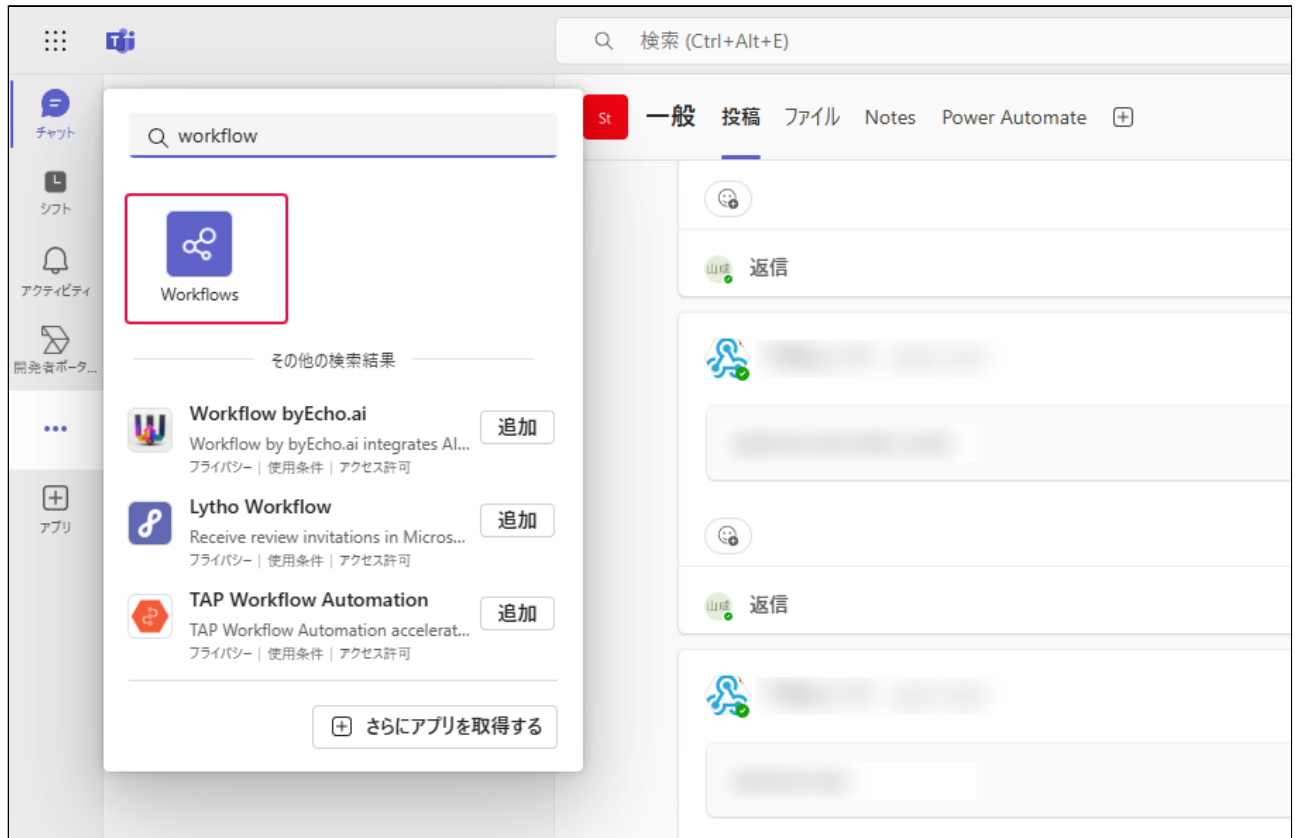
次へ

2. Teams を通知方法として選択する場合の準備

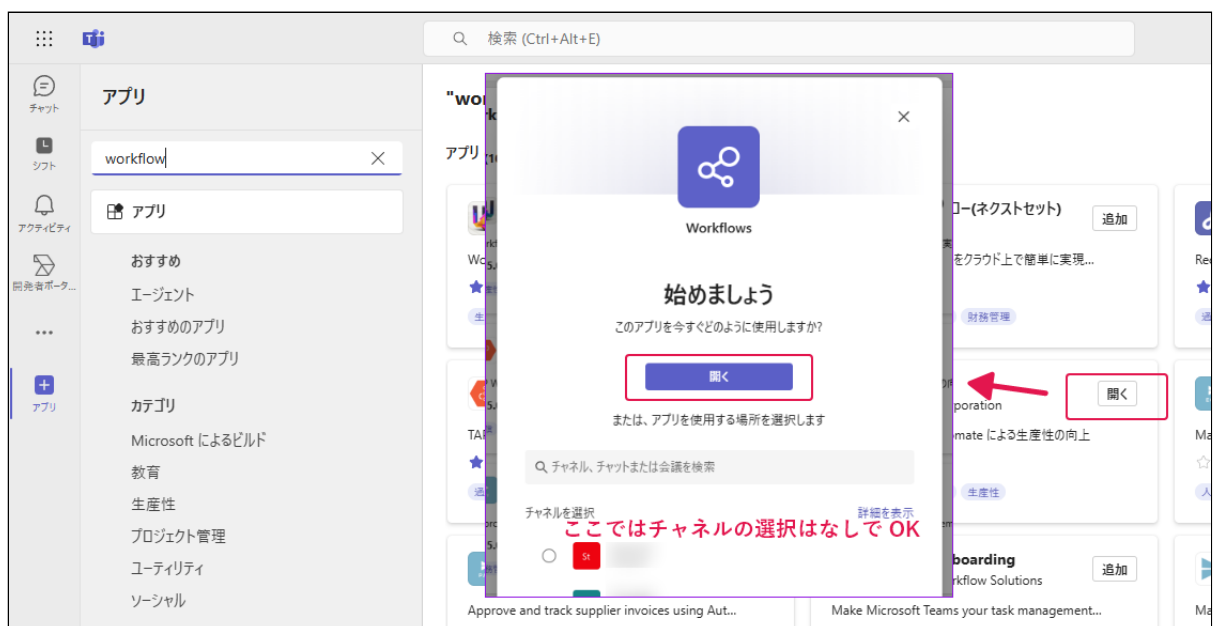
Teams (テキスト) を利用する場合

Teams アプリまたはブラウザでアクセスした Teams から操作します。

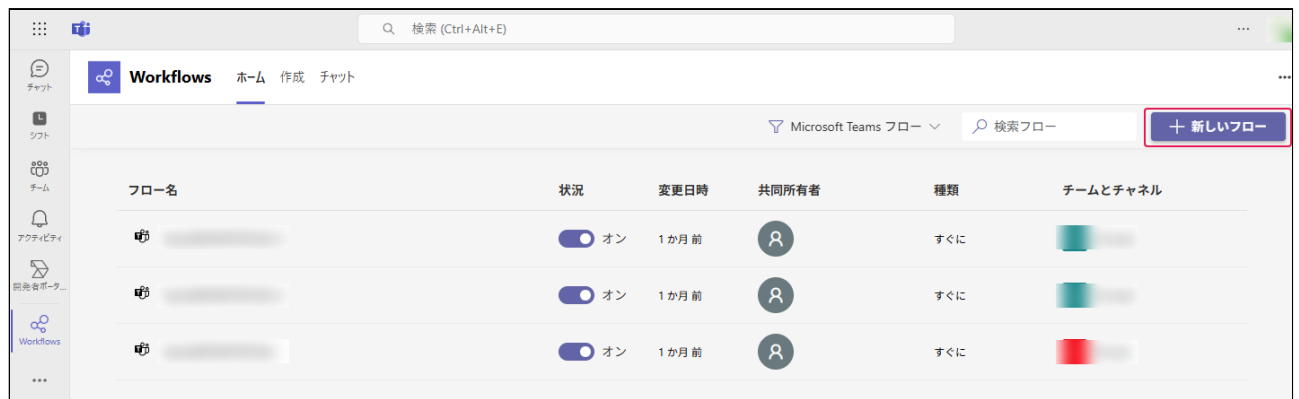
1. [Workflows] アプリを開きます。



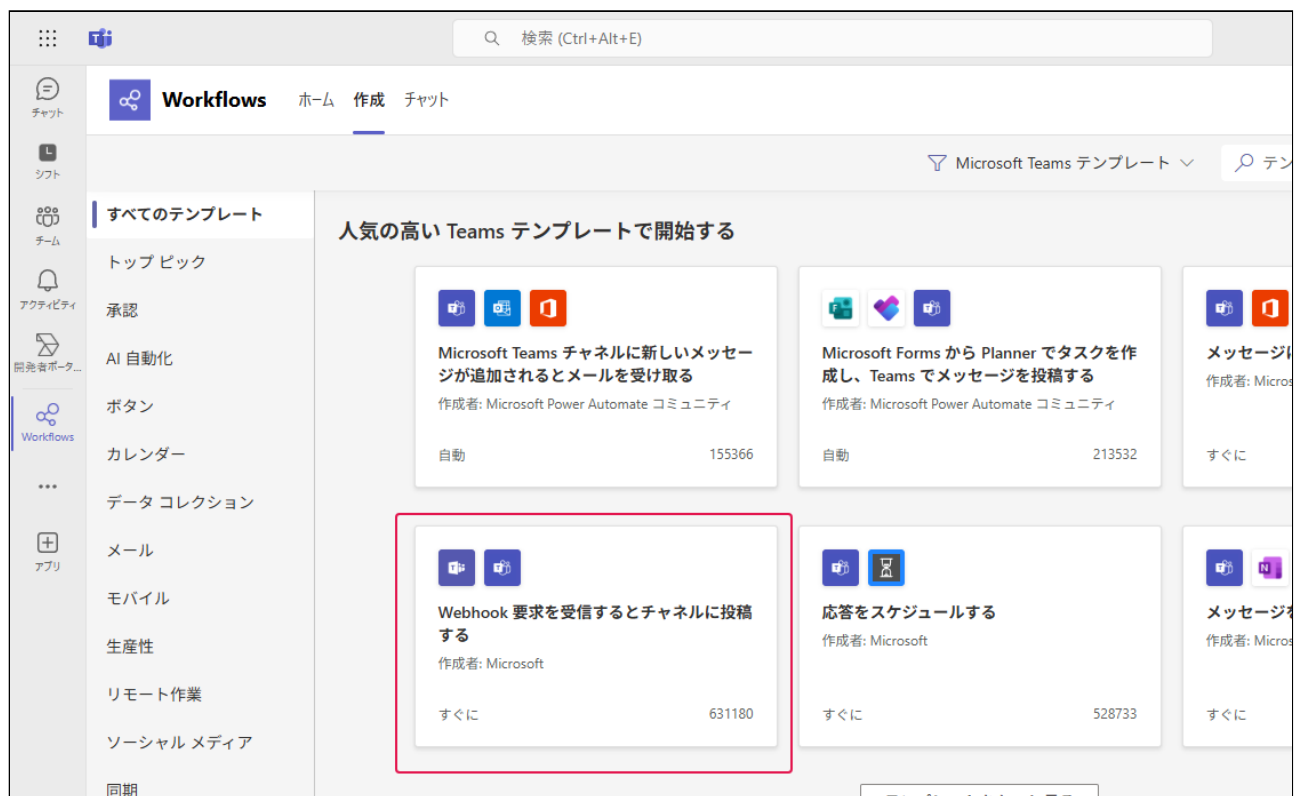
- 検索結果に表示されない場合は、[さらにアプリを取得する] をクリックして再度検索し、[Workflows] の [開く] をクリックします。



2. [新しいフロー] をクリックします。



3. [Webhook 要求を受信するとチャンネルに投稿する] をクリックします。



4. フロー名に任意の名前を入力し、[次へ] をクリックします。

フローの作成

Webhook 要求を受信するとチャンネルに投稿する
フローの種類: すぐに

Webhook 要求を受信すると、Microsoft Teams のチャンネルにカードを投稿する

フロー名
Quick MONITOR Bot

1 入力 (例: Quick MONITOR Bot) サインイン*

このフローは次のアプリを使用します。緑のチェックは準備完了を意味します。

Microsoft Teams

2 クリック

次へ キャンセル

5. 通知を送りたいチームとチャンネルを選択し、[フローの作成] をクリックします。

フローの作成

Webhook 要求を受信するとチャンネルに投稿する
フローの種類: すぐに

Webhook 要求を受信すると、Microsoft Teams のチャンネルにカードを投稿する

1 チームを選択

2 チャンネルを選択

3 クリック

戻る フローの作成 キャンセル

6. 表示されている URL を控えておきます。

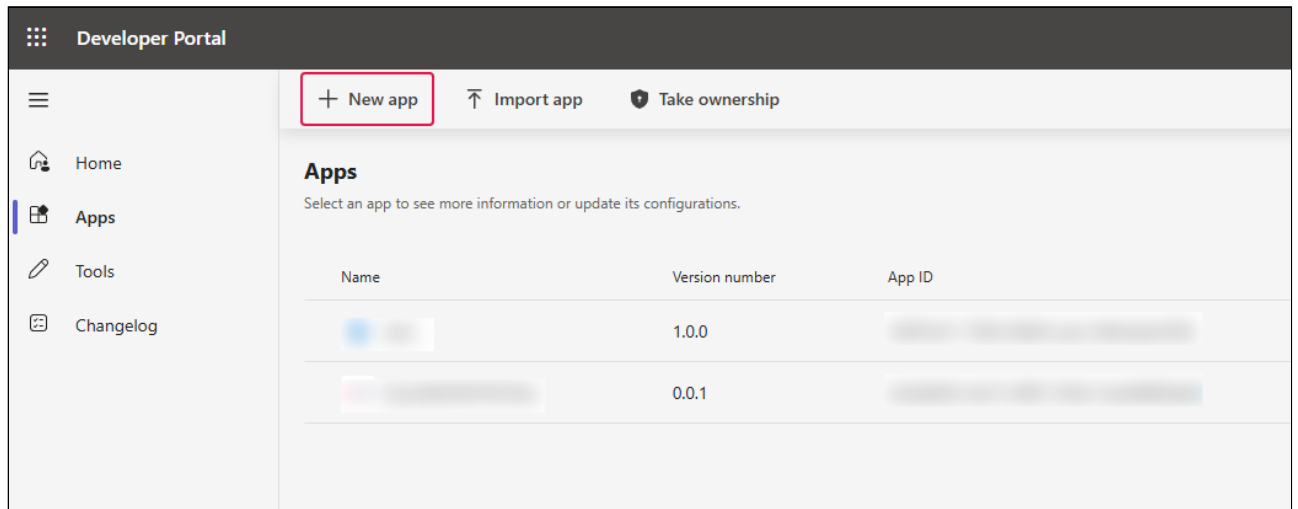


Teams (音声) を利用する場合

Quick MONITOR からの通知を Teams の音声通話で受け取る場合、Teams Developer Portal と Azure Portal での操作が必要です。

Teams Developer Portal でアプリ登録

1. [Teams Developer Portal](#) にサインインします。
2. [New app] をクリックします。



3. 任意の名前を入力し、[Add] をクリックします。

The 'Create a new app' dialog box is shown. It has a 'Name*' input field containing 'Quick MONITOR Bot', which is highlighted with a red box and labeled '1 入力 (例: Quick MONITOR Bot)'. Below it, the 'Manifest version' is set to 'Latest stable (1.20)'. At the bottom right, there are 'Cancel' and 'Add' buttons. The 'Add' button is highlighted with a red box and labeled '2 クリック'.

4. 必要な情報を入力し、[Save] をクリックします。

- Short description の例: Quick MONITOR 音声通知 Bot
- Developer information の例
 - Developer or company name: Rworks, Inc.
 - Website: <https://www.rworks.jp/>
- App URLs の例
 - Privacy policy: <https://www.rworks.jp/>
 - Terms of use: <https://www.rworks.jp/>

The screenshot shows the 'Developer Portal' interface for an app named 'Quick MONITOR Bot'. At the top, there are navigation buttons: '< Apps', 'Save' (highlighted with a red box), and 'Revert'. The left sidebar contains a menu with 'Overview', 'Dashboard', 'Analytics', 'Configure', 'Advanced', and 'Develop'. The 'Configure' section is expanded, showing 'Basic information', 'Branding', 'App features', 'App package editor' (with a 'New' badge), 'Permissions', 'Single sign-on', 'Languages', and 'Domains'. The main content area is titled 'Basic information' and includes a link to 'See best practices'. It contains fields for 'App names' (Short name and Full name), 'App ID' (with a copy icon), and 'Descriptions' (Short description).

Developer Portal

< Apps **Save** Revert

Quick MONITOR Bot

Overview ▾

Dashboard

Analytics

Configure ▾

Basic information

Branding

App features

App package editor **New**

Permissions

Single sign-on

Languages

Domains

Advanced >

Develop ▾

Open in Microsoft 365 Agents Toolkit

Basic information

This is the information users see on your app details page in Teams. [See best practices.](#)

App names

A short name (30 characters or less) is required. Include a longer version if your preferred name exceeds 30 characters.

Short name - 30 characters or less*

Quick MONITOR Bot

Full name - up to 100 characters (optional)

Enter a longer, preferred name (displays if more than 30 characters)

App ID

Your app's identifier that's generated by Microsoft and unique to your org.

[Redacted App ID]

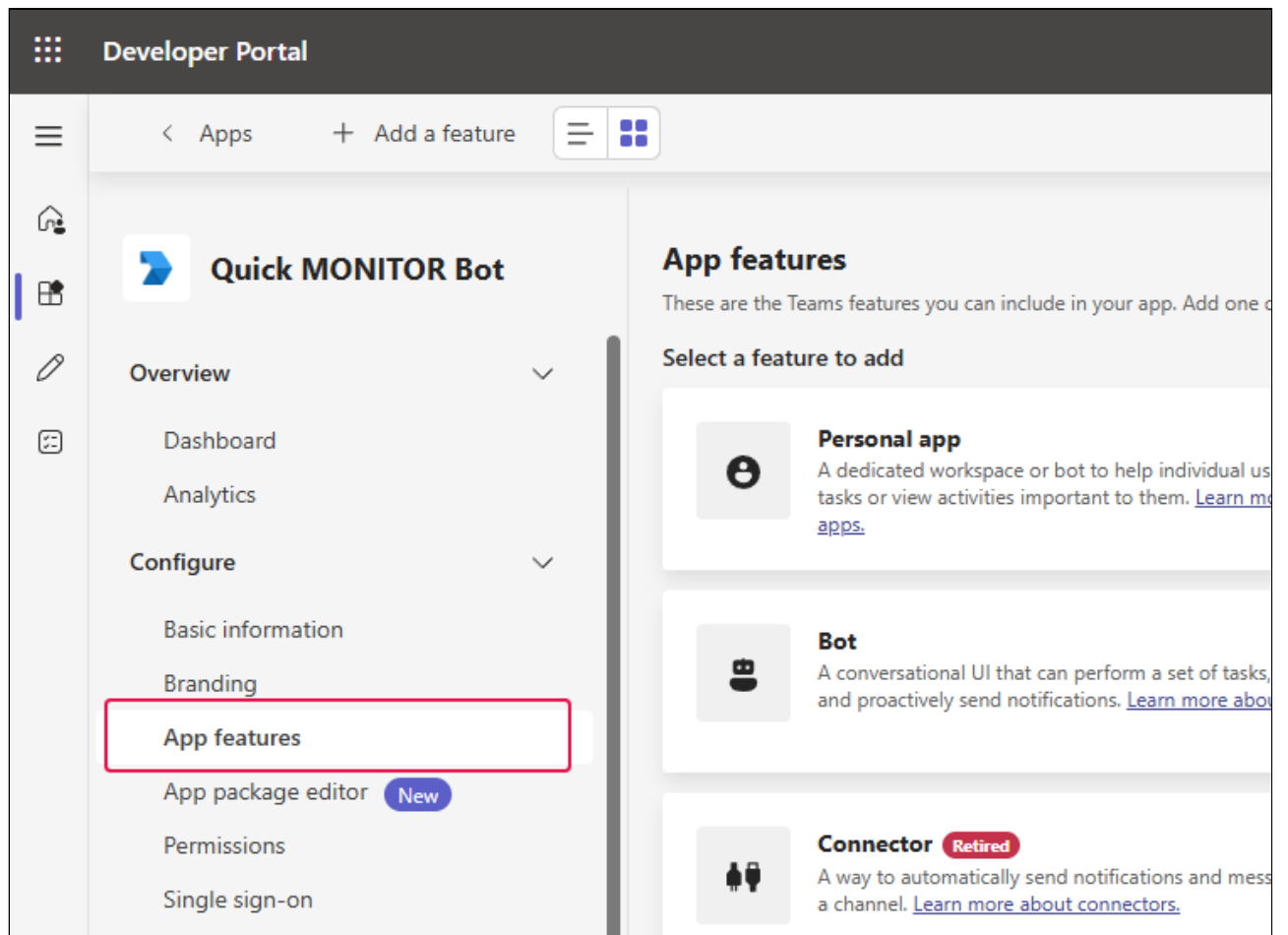
Descriptions

Short and long descriptions must be different. If you're publishing your app to the Teams Store, the descriptions in your submission must match the ones here.

Short description - 80 characters or less*

[Redacted Short Description]

5. [Configure] の [App features] に移動します。




6. [Bot] をクリックします。


App features

These are the Teams features you can include in your app. Add one or more features depending on your app's use cases. [Learn more about app features.](#)


Select a feature to add

**Personal app**


A dedicated workspace or bot to help individual users focus on their own tasks or view activities important to them. [Learn more about personal apps.](#)

**Group and channel app**


A space to display hosted app experiences (such as a list or dashboard) in team channels and group chats. [Learn more about group and channel apps.](#)

**Bot**


A conversational UI that can perform a set of tasks, reply to questions, and proactively send notifications. [Learn more about bots.](#)

**Message extension**


A shortcut for inserting your app's content or acting on a message without navigating away from a conversation. [Learn more about message extensions.](#)

**Connector** Retired


A way to automatically send notifications and messages from your app to a channel. [Learn more about connectors.](#)

**Meeting extension**

Options for integrating your app with the Teams meeting experience, including the meeting stage and chat. [Learn more about meeting extensions.](#)

**Scene**

A custom virtual scene people can use in their Teams Together mode meetings.

**Activity feed notification**

Keep users informed and engaged with app notifications in the activity feed. [Learn more about activity feed notifications.](#)

7. [Create a new bot] をクリックします。

< Bot

Bots are conversational apps that perform a specific set of tasks. They communicate with users, respond to their questions, and proactively notify them about changes and other events. [Learn more about designing Teams bots.](#)

Identify your bot

☒ Select an existing bot

Select an existing bot

Create a new bot

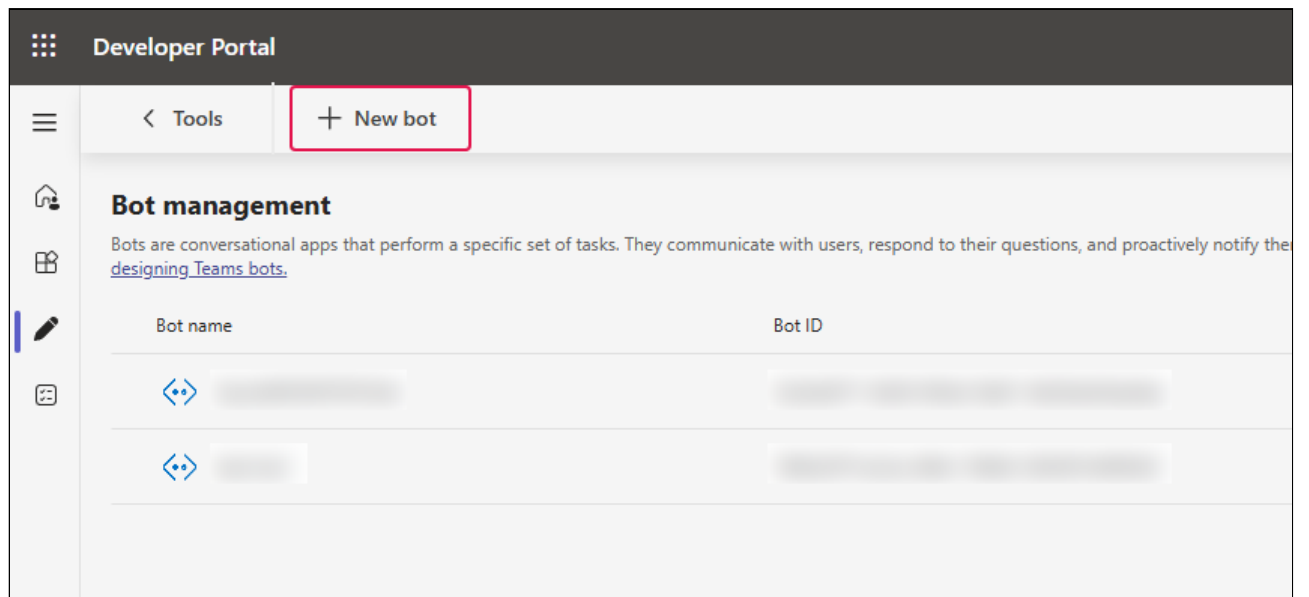
☐ Enter a bot ID

XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

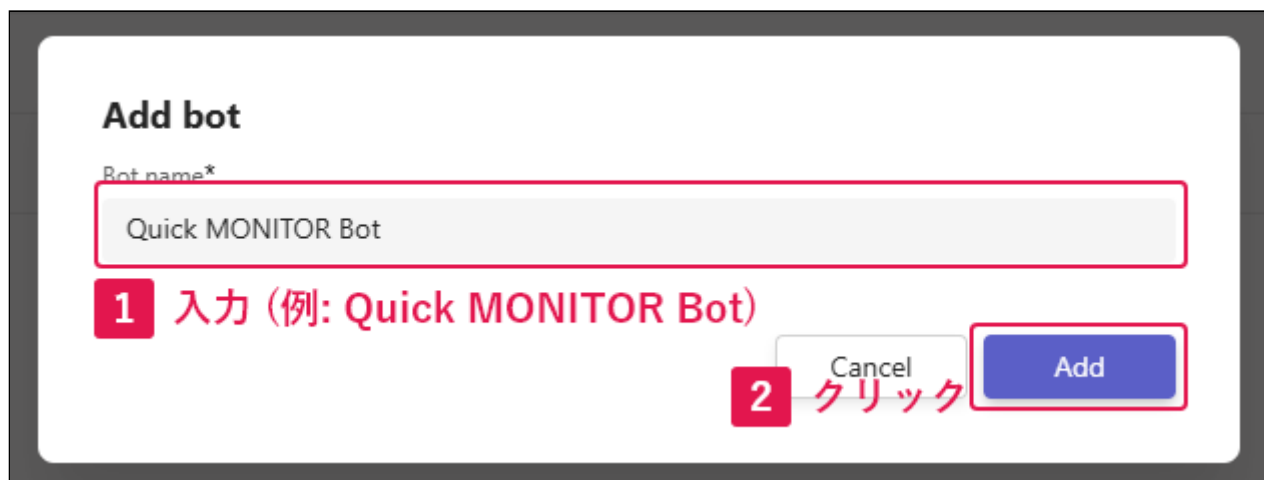
What can your bot do?

☐ Upload and download files

8. [New bot] をクリックします。

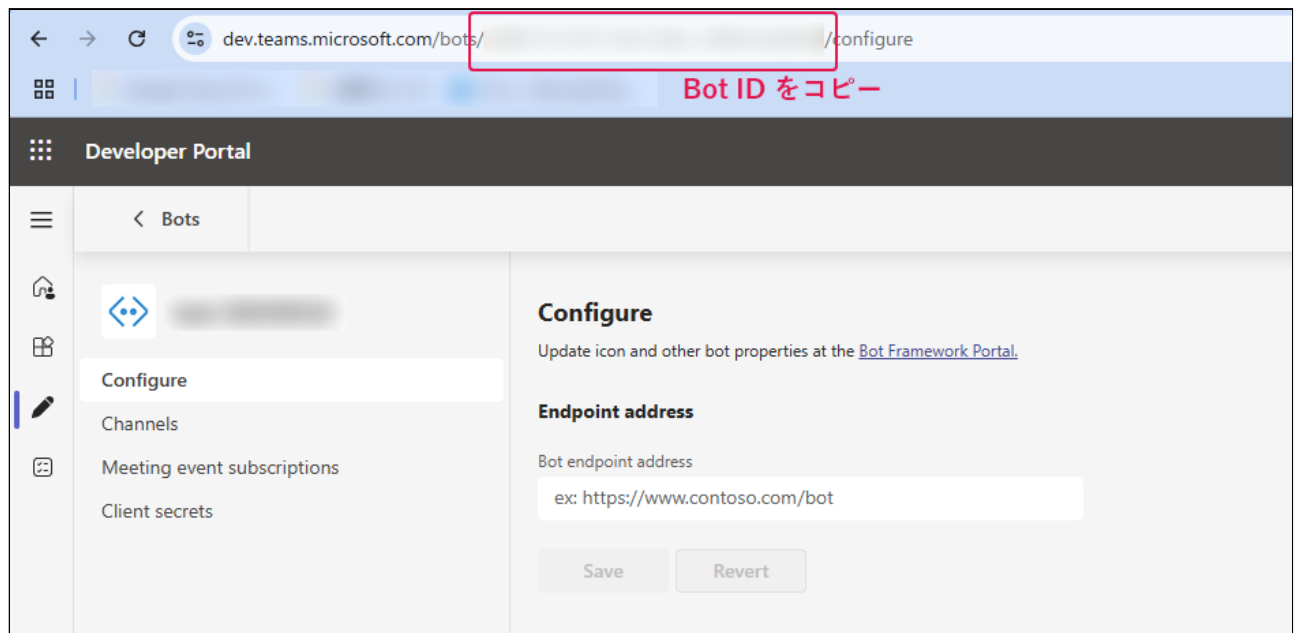


9. 任意の名前を入力し、[Add] をクリックします。

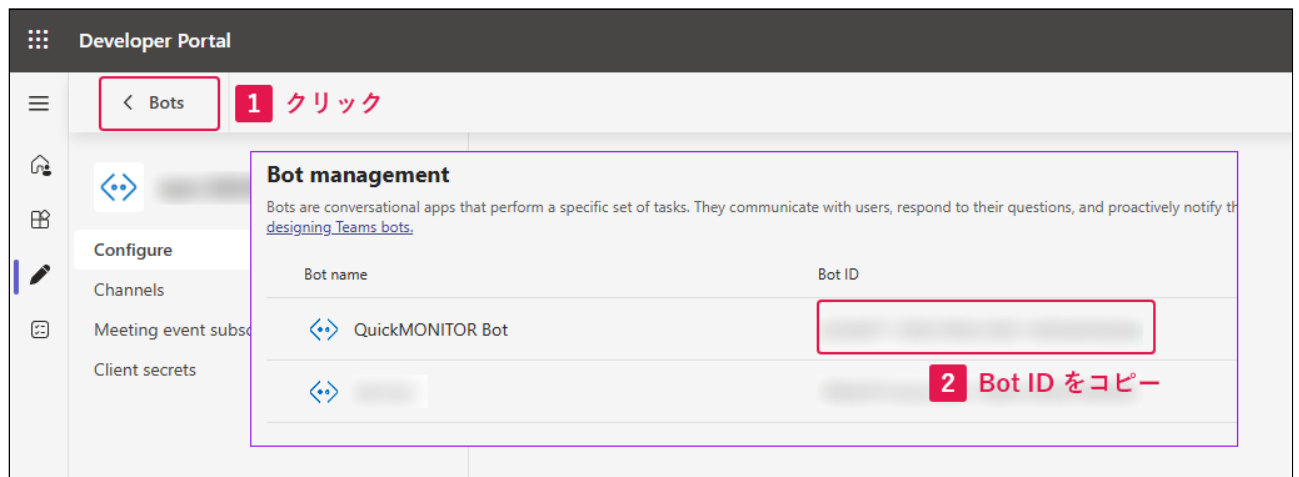


10. 次のいずれかの方法で Bot ID を控えておきます。

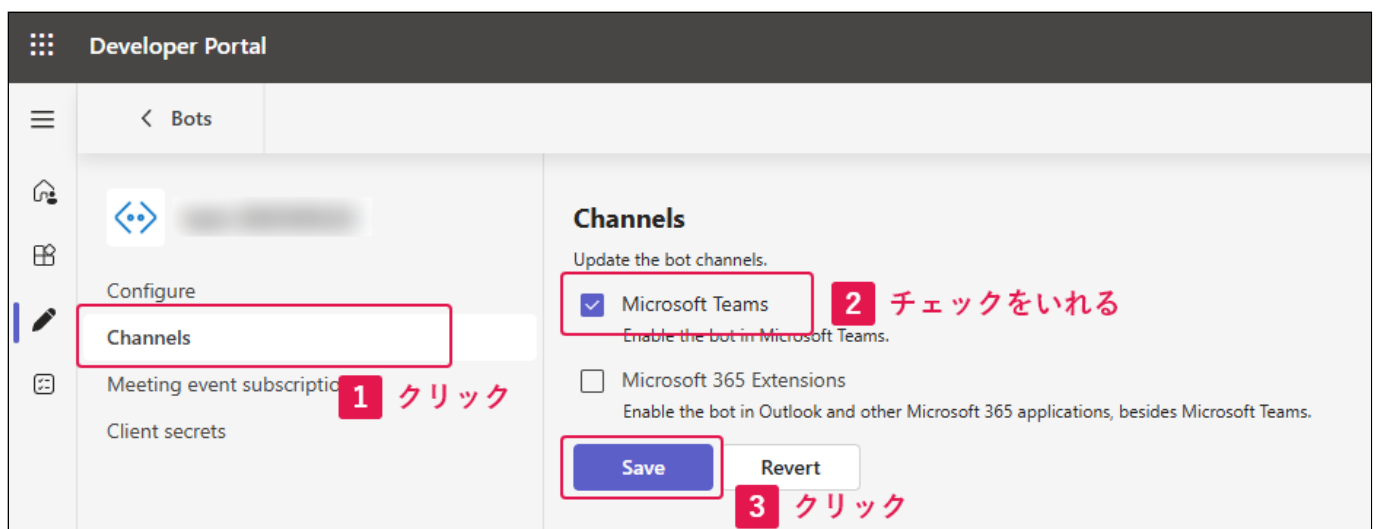
- URL からコピー



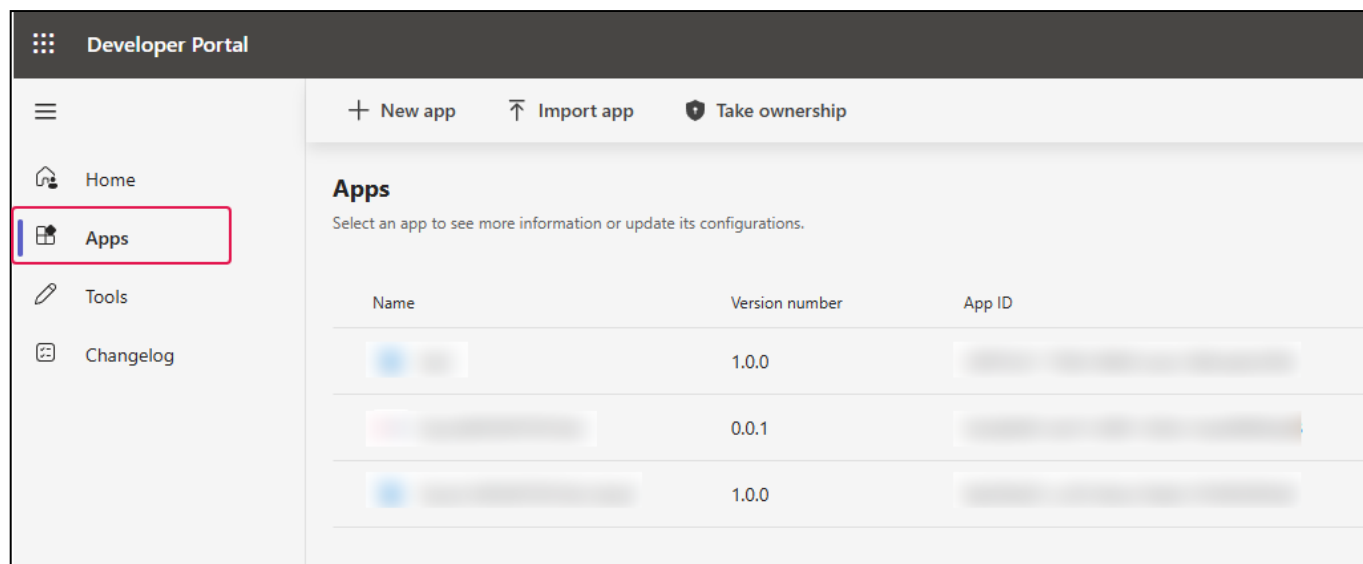
- [Bots] をクリックして戻った画面でコピー



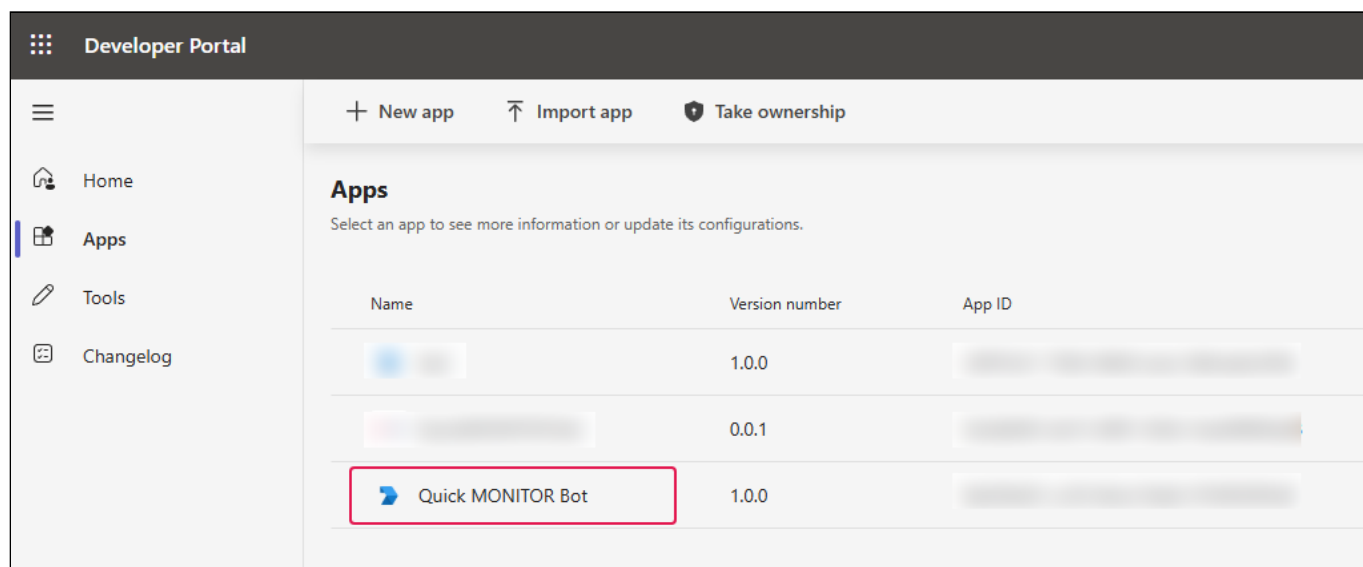
11. Channels に移動し、Microsoft Teams にチェックをいれて [Save] をクリックします。



12. 画面左のメニューから [Apps] に移動します。



13. 登録したアプリをクリックします。



14. [Configure] の [Basic information] に移動します。

The screenshot shows the 'Developer Portal' interface for a bot named 'Quick MONITOR Bot'. The left sidebar contains a navigation menu with sections: Overview, Configure, Advanced, and Develop. The 'Configure' section is expanded, and the 'Basic information' option is highlighted with a red rectangle. The main content area is titled 'Basic information' and includes instructions for app names and descriptions. The 'App names' section has input fields for 'Short name' (containing 'Quick MONITOR Bot') and 'Full name' (with a placeholder 'Enter a longer, preferred name...'). The 'App ID' section shows a blurred identifier with a copy icon. The 'Descriptions' section has a 'Short description' input field.

Developer Portal

< Apps Save Revert

Quick MONITOR Bot

Overview ▾

- Dashboard
- Analytics

Configure ▾

- Basic information**
- Branding
- App features
- App package editor **New**
- Permissions
- Single sign-on
- Languages
- Domains

Advanced >

Develop ▾

Open in Microsoft 365 Agents Toolkit

Basic information

This is the information users see on your app details page in Teams. [See best practices.](#)

App names

A short name (30 characters or less) is required. Include a longer version if your preferred name exceeds 30 characters.

Short name - 30 characters or less*

Quick MONITOR Bot

Full name - up to 100 characters (optional)

Enter a longer, preferred name (displays if more than 30 characters)

App ID

Your app's identifier that's generated by Microsoft and unique to your org.

[Blurred App ID] 📋

Descriptions

Short and long descriptions must be different. If you're publishing your app to the Teams Store, the descriptions in your submission must match the ones here.

Short description - 80 characters or less*

[Blurred Short Description]

15. Bot ID を [Application (client) ID] に入力して [Save] をクリックします。

Developer Portal

< Apps Save Revert

Quick MONITOR Bot (test)

Overview

- Dashboard
- Analytics

Configure

- Basic information**
- Branding
- App features
- App package editor **New**
- Permissions
- Single sign-on
- Languages
- Domains

Advanced

Develop

- Open in Microsoft 365 Agents Toolkit

Publish

App URLs

You must provide links to your privacy policy and terms of use. [Learn more about best practices for links.](#)

Privacy policy*

Terms of use*

Example: <https://www.example.com/termsfuse>

Application (client) ID*

Specify the app ID assigned when you registered your app with Azure Active Directory.

1 控えておいた Bot ID を入力

Microsoft Partner ID

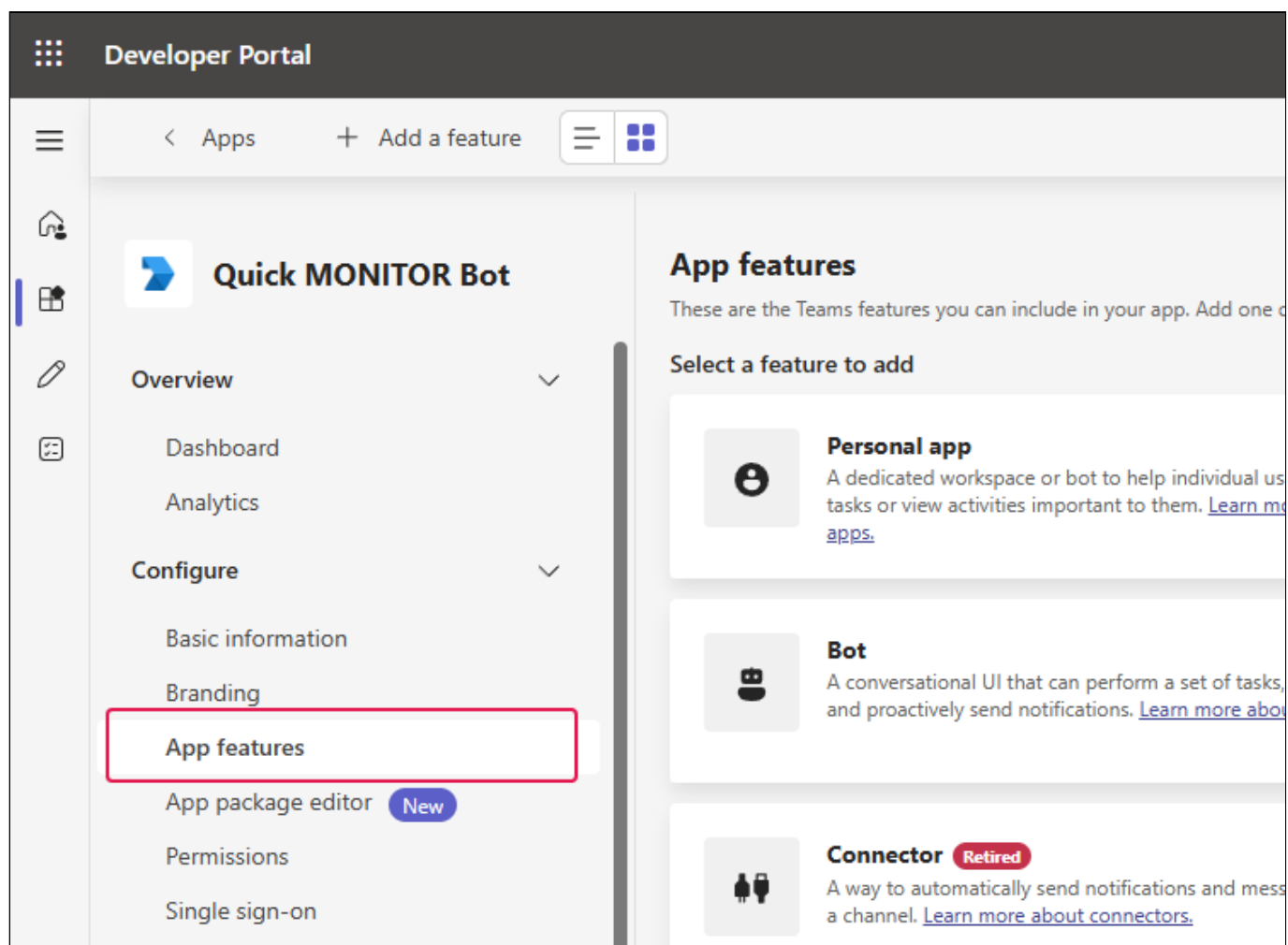
If you're part of the Microsoft AI Cloud Partner Program, specify your Partner ID. [Learn more about partnering with Microsoft.](#)

XXXXXXXXXX

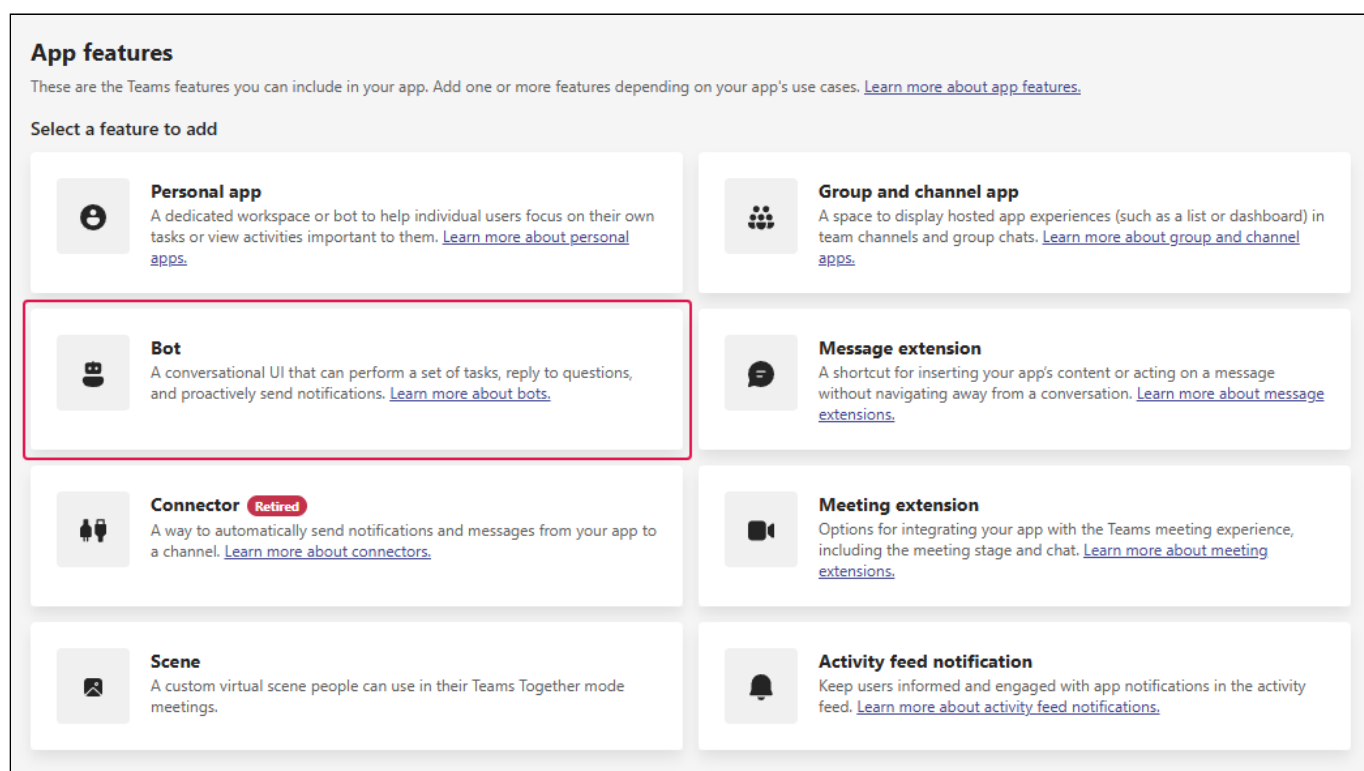
2 クリック

Save Revert

16. [Configure] の [App features] に移動します。



17. [Bot] をクリックします。



18. 以下を参考に入力し、[Save] をクリックします。

Developer Portal

< Apps Save Revert

Quick MONITOR Bot

Overview

- Dashboard
- Analytics

Configure

- Basic information
- Branding
- App features
- App package editor **New**
- Permissions
- Single sign-on
- Languages
- Domains

Advanced

Develop

- Open in Microsoft 365 Agents Toolkit

Publish

- App validation **New**
- Publish to org
- Publish to Store

< Bot

Bots are conversational apps that perform a specific set of tasks. They communicate with users, respond to their questions, and proactively respond to user needs. [more about designing Teams bots.](#)

Identify your bot

☒ Select an existing bot

QuickMONITOR Bot () **1 作成した Bot を選択**

[Create a new bot](#)

☐ Enter a bot ID

What can your bot do?

- ☐ Upload and download files
- ☐ Only send notifications (one-way conversations)
- ☒ Support audio calls **2 チェックをいれる**
- ☐ Support video calls

Select the scopes where people can use your bot

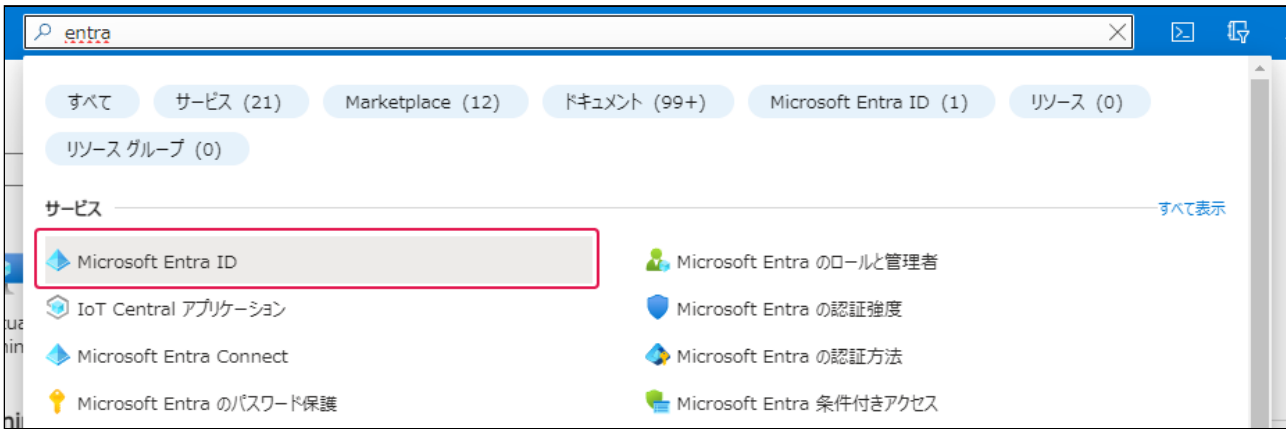
- ☒ Personal **3 チェックをいれる**
- ☒ Team
- ☐ Group Chat

4 クリック

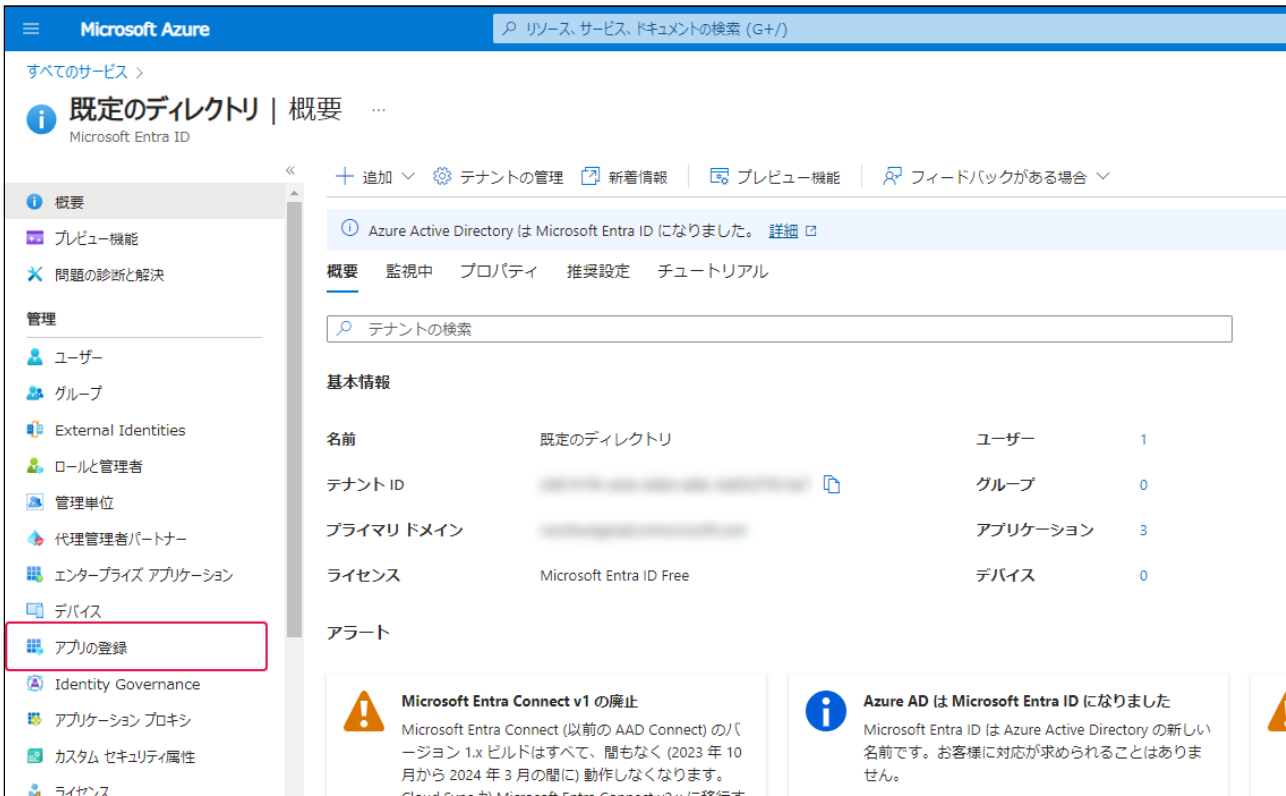
Save Revert

登録したアプリに対して Azure Portal で権限を付与

- 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. Teams Developer Portal で登録したアプリを選択します。

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The left sidebar contains a navigation menu with options like '概要' (Overview), 'プレビュー機能' (Preview features), '問題の診断と解決' (Troubleshooting), and '管理' (Management). The main content area is titled 'アプリの登録' (App Registrations). It displays a list of applications, with 'QuickMONITOR Bot' highlighted in a red box. The application details show it is a 'QuickMONITOR Bot' with a 'QB' icon.

5. [API のアクセス許可] をクリックします。

The screenshot shows the Microsoft Azure portal interface, specifically the 'API のアクセス許可' (API access permissions) page. The left sidebar contains a navigation menu with options like '概要' (Overview), 'クイック スタート' (Quick start), '統合アシスタント' (Integration assistant), '問題の診断と解決' (Troubleshooting), and '管理' (Management). The main content area is titled 'API のアクセス許可'. It displays a list of permissions, with 'API のアクセス許可' highlighted in a red box. The application details show it is a 'QuickMONITOR Bot' with a 'QB' icon.

6. [アクセス許可の追加] をクリックします。

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation links: Home, App Registrations, Overview, Quick Start, Unified Assistant, Troubleshooting and Resolution, and Management. Under Management, there are links for Branding and Properties, Authentication, Certificates and Secrets, Token Configuration, API Access Permissions (highlighted), API Publishing, and App Roles. The main content area is titled 'API のアクセス許可' (API Access Permissions). It includes a search bar, a refresh button, and a feedback link. A warning message states: 'テナント全体の同意を付与すると、そのアプリケーションに対してテナント全体に既に付与されているアクセス許可が取り消される場合があります。ユーザーが...' (Granting consent for the entire tenant may result in access permissions already granted to the entire tenant for that application being revoked. Users...). Below this, a message says: '“管理者の同意が必要” 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。...' (The 'Consent Required by Administrator' column displays the organization's default value. However, user consent can be customized by access permission, user, and app...). The 'Configured Access Permissions' section explains that an application is part of the consent process and that users must grant consent for all access permissions. A red box highlights the '+ アクセス許可の追加' (Add Access Permission) button. Below it, a table lists configured permissions with columns for 'API / アクセス許可の名前' (API / Access Permission Name), '種類' (Type), and '説明' (Description). The table currently shows one entry: 'アクセス許可は追加されませんでした' (Access permission was not added).

7. [Microsoft Graph] をクリックします。

The screenshot shows the Microsoft Azure portal interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'API のアクセス許可' (API Access Permissions). A modal window titled 'API アクセス許可の要求' (API Access Permission Request) is open. It shows a list of APIs to select from. The 'Microsoft Graph' API is highlighted with a red box. Below the list, there are sections for 'よく使用される Microsoft API' (Commonly used Microsoft APIs) and 'Azure Rights Management Services', 'Azure Service Management', 'Dynamics CRM', 'Intune', 'Office 365 Management APIs', and 'OneNote'.

8. [アプリケーションの許可] をクリックします。

The screenshot shows the Microsoft Azure portal interface. The left sidebar is the same as in the previous screenshots. The main content area is titled 'API のアクセス許可' (API Access Permissions). A modal window titled 'API アクセス許可の要求' (API Access Permission Request) is open. It shows the 'Application Permissions' tab selected. The 'Application Permissions' section is highlighted with a red box. Below it, there is a section for 'Access Permissions' with a search bar and a list of permissions. The 'Access Review' and 'Access Review' links are visible at the bottom.

9. 次の4つを検索して表示されたチェックボックスにチェックをいれ、[アクセス許可の追加] をクリックします。

- `Calls.AccessMedia.All`
- `Calls.Initiate.All`
- `Calls.InitiateGroupCall.All`
- `User.Read.All`

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

API のアクセス許可

検索

概要

クイックスタート

統合アシスタント

問題の診断と解決

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

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

API アクセス許可の要求

すべての API

Microsoft Graph
https://graph.microsoft.com/ ドキュメント

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可
アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可
アプリケーションは、サインインしたユーザーとして、バックグラウンド サービスまたはデーモンとして実行されます。

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理する必要のあるアクセス許可を含める必要があります。アクセス許可の追加

アクセス許可の追加

API / アクセス許可の名前

種類

アクセス許可は追加されませんでした

アクセス許可を選択する

検索

1 検索

2 チェックをいれる

3 クリック

アクセス許可の追加

破棄

Calls.AccessMedia.All

Calls.Initiate.All

Calls.InitiateGroupCall.All

User.Read.All

すべて展開

Calls (1)

Calls.AccessMedia.All

Access media streams in a call as an app

Ctrl+Shift+F を押して、お気に入りの入力を追加または削除します

10. [～に管理者の同意を与えます] 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 > | アプリの登録 > | API のアクセス許可

検索 | 最新の情報に更新 | フィードバックがある場合

概要

クイックスタート

統合アシスタント

問題の診断と解決

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

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

アプリケーションに対するアクセス許可を編集しています。ユーザーは、既に同意したことがある場合でも同意が必要になります。

テナント全体の同意を付与すると、そのアプリケーションに対してテナント全体に既に付与されているアクセス許可が取り消される場合があります。ユーザーが自分の代わりに付与済みのアクセス許可は影響を受けません。 [詳細](#)

“管理者の同意が必要”列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ☒ ～に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (4)				
Calls.AccessMedia.All	アプリケー...	Access media streams in a call as an app	はい	MSFT に付与されていません ...
Calls.Initiate.All	アプリケー...	Initiate outgoing 1 to 1 calls from the app	はい	MSFT に付与されていません ...
Calls.InitiateGroupCall.All	アプリケー...	Initiate outgoing group calls from the app	はい	MSFT に付与されていません ...
User.Read.All	アプリケー...	Read all users' full profiles	はい	MSFT に付与されていません ...

11. [はい] をクリックします。

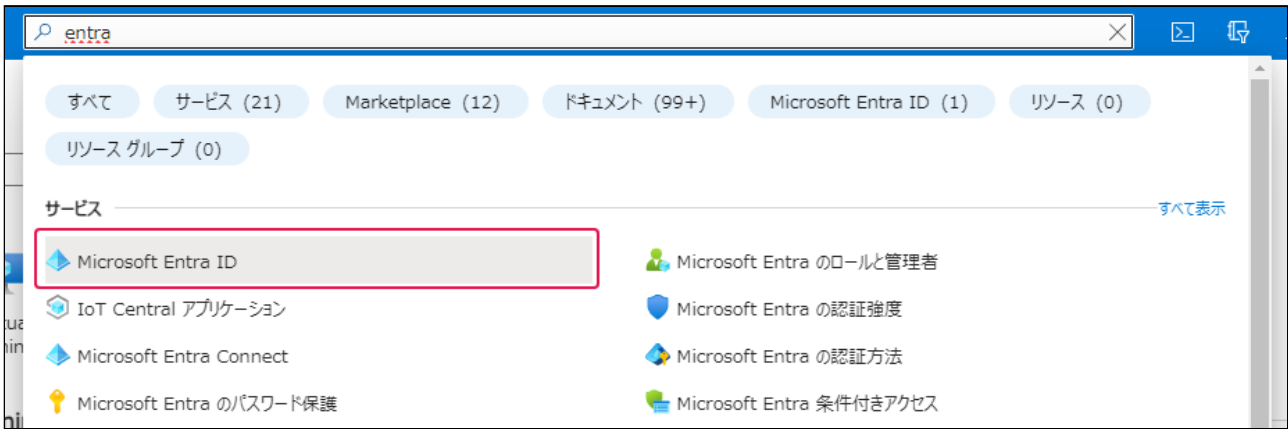
最新の情報に更新 | フィードバックがある場合

管理者の同意の確認を与えます。

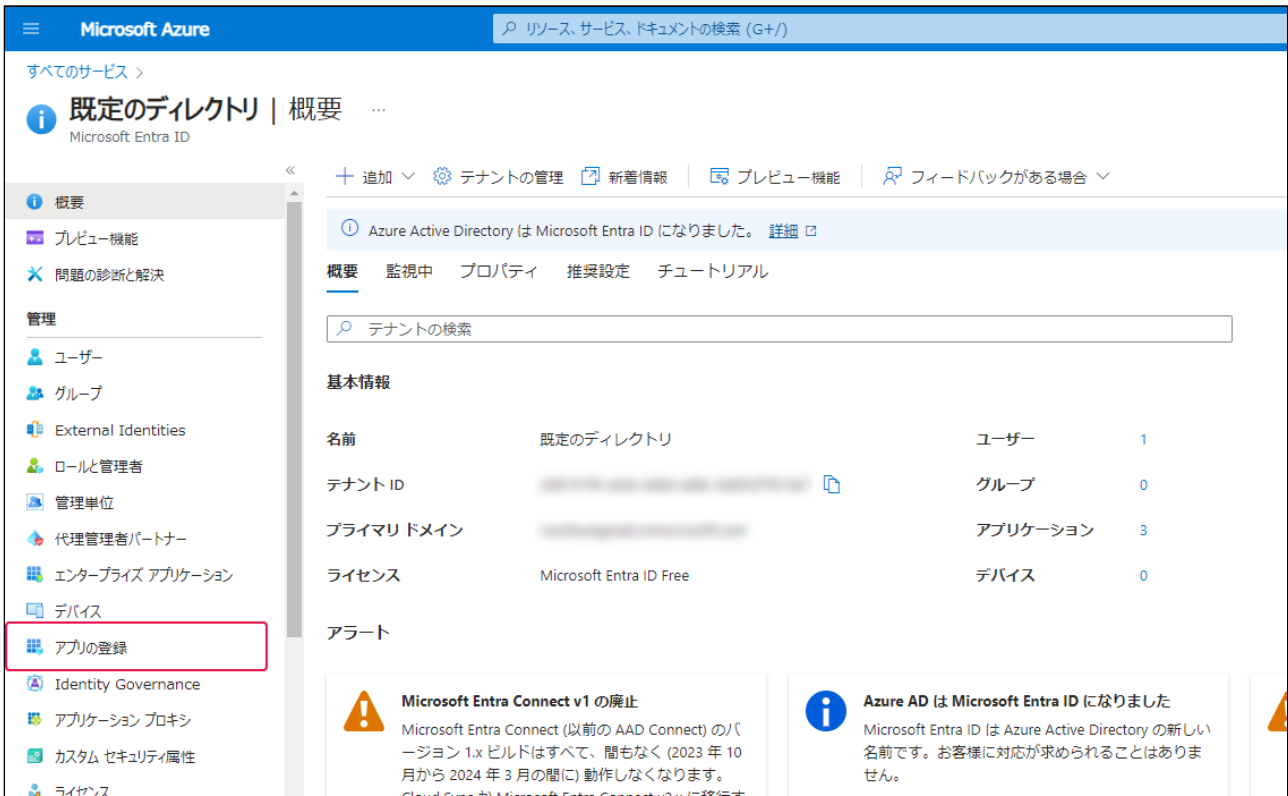
MSFT のすべてのアカウントについて、要求されたアクセス許可に対する同意を付与しますか？ この操作により、このアプリケーションが既に持っている既存の管理者の同意レコードが、以下の一覧の内容に一致するよう更新されます。

認証情報の発行

- 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。



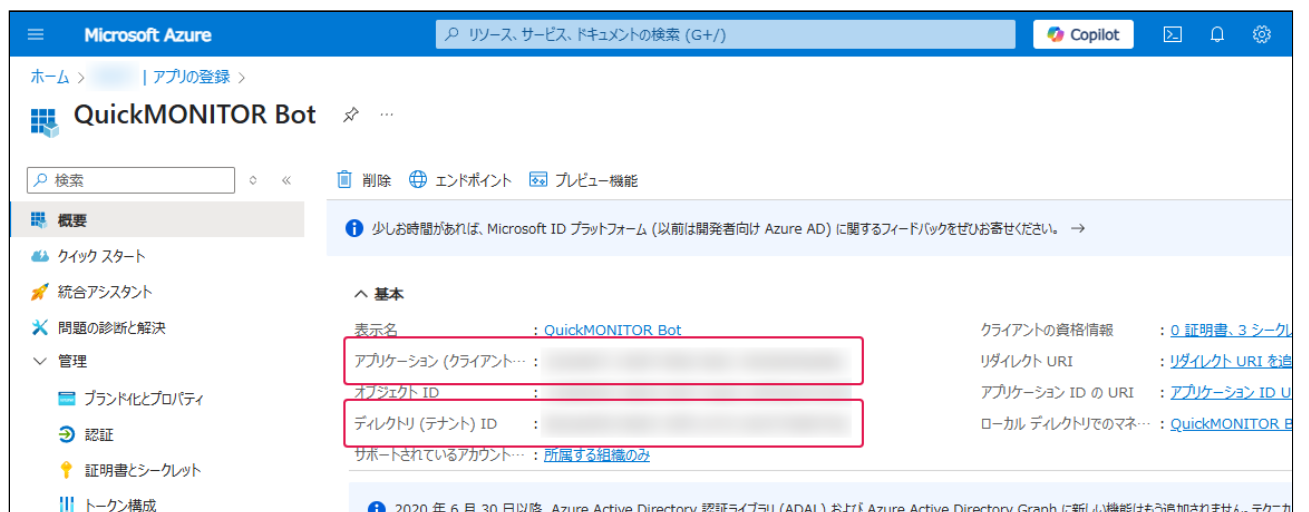
- 3. [アプリの登録] を開きます。



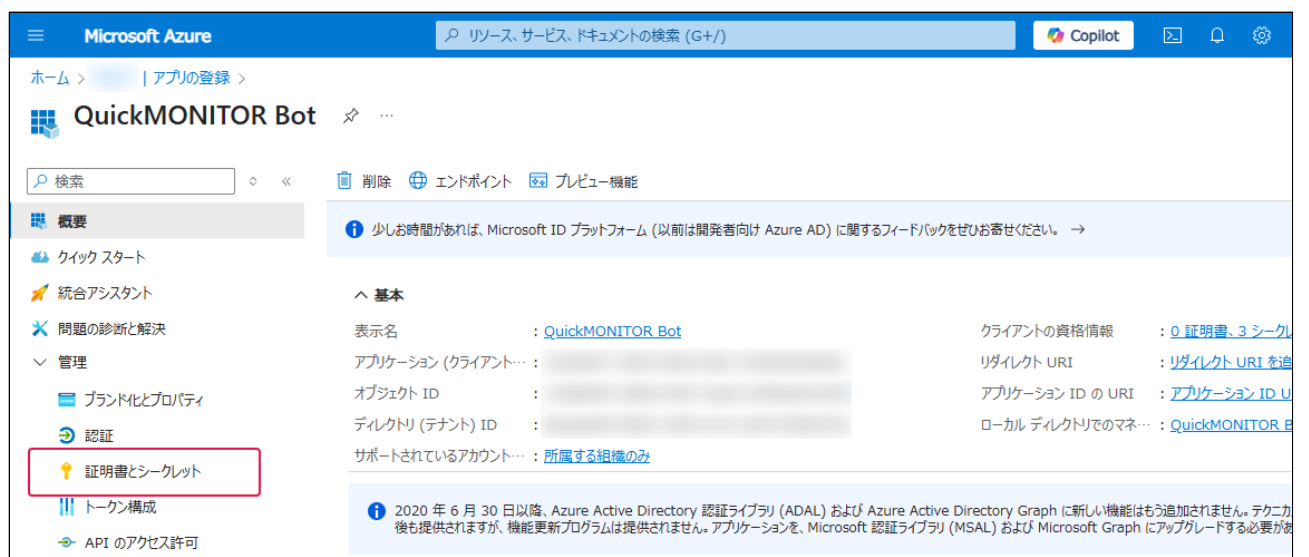
4. Teams Developer Portal で登録したアプリを選択します。



5. アプリケーション (クライアント) ID と ディレクトリ (テナント) ID を控えておきます。



6. [証明書とシークレット] に移動します。



7. [新しいクライアントシークレット] 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 > アプリの登録 > QuickMONITOR Bot'. The main heading is 'QuickMONITOR Bot | 証明書とシークレット'. A left sidebar contains a list of navigation items: '概要', 'クイック スタート', '統合アシスタント', '問題の診断と解決', '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' (highlighted), 'トークン構成', 'API のアクセス許可', 'API の公開', 'アプリ ロール', and '所有者'. The main content area has a search bar and a link 'フィードバックがある場合'. Below this, there's a message: '資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、ものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うこと。' and a note: 'アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。'. There are three tabs: '証明書 (0)', 'クライアント シークレット (3)' (selected), and 'フェデレーション資格情報 (0)'. A description states: 'トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション'. A red box highlights the '+ 新しいクライアント シークレット' button. Below it is a table with columns '説明', '有効期限', and '値'.

8. 画面に従って入力後 [追加] ボタンをクリックします。

The screenshot shows a dialog box titled 'クライアント シークレットの追加' (Add Client Secret). It has a close button (X) in the top right corner. The dialog contains two input fields: '説明' (Description) and '有効期限' (Expiration). The '説明' field has a red box around it with a red number '1' and the text '任意の説明を入力' (Enter an optional description). The '有効期限' field has a red box around it with a red number '2' and the text '任意の期限を入力' (Enter an optional expiration period). The '有効期限' field is a dropdown menu showing '推奨: 180 日 (6 か月)' (Recommended: 180 days (6 months)). At the bottom, there are two buttons: '追加' (Add) and 'キャンセル' (Cancel). The '追加' button is highlighted with a red box and a red number '3' with the text 'クリック' (Click).

9. 作成したクライアントシークレットの値を控えます。

The screenshot shows the Microsoft Azure portal interface for the 'QuickMONITOR Bot' application. The left sidebar contains navigation links such as '概要' (Overview), 'クイック スタート' (Quickstart), '統合アシスタント' (Integration Assistant), '問題の診断と解決' (Troubleshooting), and '管理' (Management). The '管理' section is expanded, showing 'ブランド化とプロパティ' (Branding and Properties), '認証' (Authentication), and '証明書とシークレット' (Certificates and Secrets). The '証明書とシークレット' section is selected, displaying a table of client secrets. The table has columns for '説明' (Description), '有効期限' (Expiration), '値' (Value), and 'シークレット ID' (Secret ID). One secret is listed with a red box highlighting its value, and a copy icon is visible next to it.

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

ホーム > | アプリの登録 > QuickMONITOR Bot

QuickMONITOR Bot | 証明書とシークレット

検索 フィードバックがある場合

概要

クイック スタート

統合アシスタント

問題の診断と解決

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

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

お時間があれば、フィードバックをお寄せください。 →

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに對のものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (4)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID

監視するインスタンスの追加・削除

Virtual Machines

1. 画面左上のメニューアイコンをクリックします。



2. [メトリック収集設定] をクリックします。



3. [Virtual Machines] ボタンをクリックします。



4. 対象インスタンス 欄を変更し、[適用] ボタンをクリックします。

メトリック収集設定

リージョンとインスタンス
対象インスタンスの上限まで残り: 6

対象インスタンス

RG-DEMO/demo-vm1

×

クリックしてインスタンスを追加

RG-DEMO/demo-vm4

RG-DEMO/demo-vm5

RG-DEMO/demo-vm2

RG-DEMO/demo-vm3

適用

・ 監視対象のインスタンス
・ ×をクリックで対象から除外

クリックで対象インスタンスに移動

設定を適用

インターバル

1 時間

30 分

5 分

監視インターバルを選択

61 / 122

Database

1. 画面左上のメニューアイコンをクリックします。



2. [メトリック収集設定] をクリックします。



3. [Database] ボタンをクリックします。



4. 対象インスタンス 欄を変更し、[適用] ボタンをクリックします。

メトリック収集設定

リージョンとインスタンス
対象インスタンスの上限まで残り: 5

・ 監視対象のインスタンス
・ × をクリックで対象から除外

対象インスタンス

rg-demo/demo-mariadb1 × rg-demo/demo-mysql1 ×

クリックしてインスタンスを追加

rg-demo/demo-mysql1-flexible

クリックで対象インスタンスに移動

+ Add

適用

設定を適用

MySQL ユーザー

username

MySQL パスワード

.....

データベースの認証情報を入力

監視インターバルを選択

1 時間

30 分

5 分

URL

1. 画面左上のメニューアイコンをクリックします。



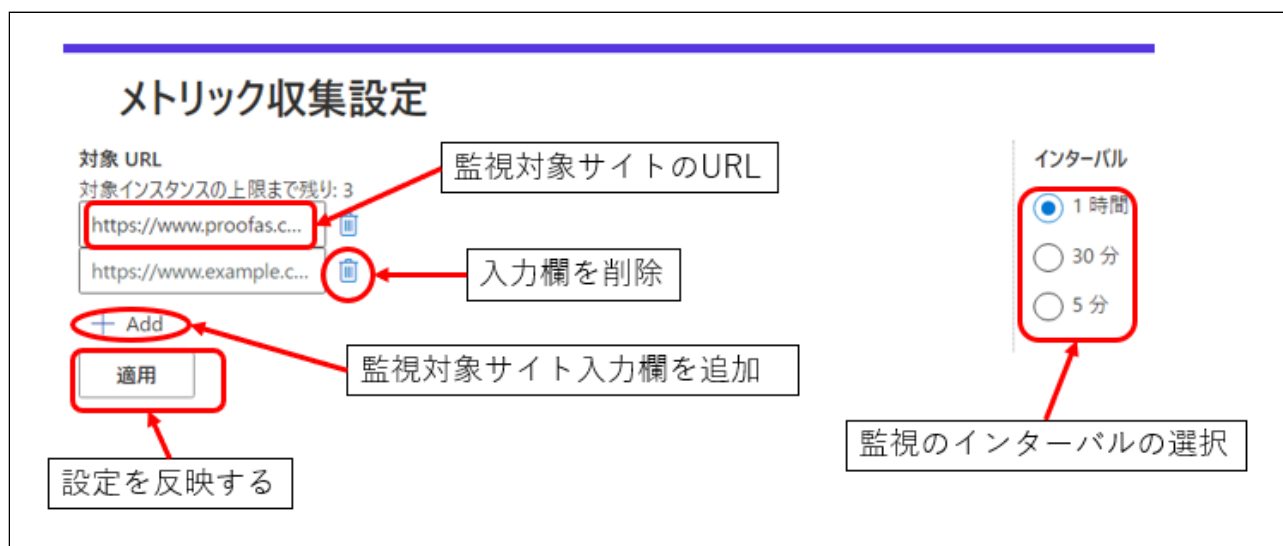
2. [メトリック収集設定] をクリックします。



3. [URL] ボタンをクリックします。



4. 監視したいWebサイトのURLを入力します。



警告と障害条件設定の変更

Virtual Machines

ネットワークパケットの送受信 (NetworkPacketsIn/NetworkPacketsOut)

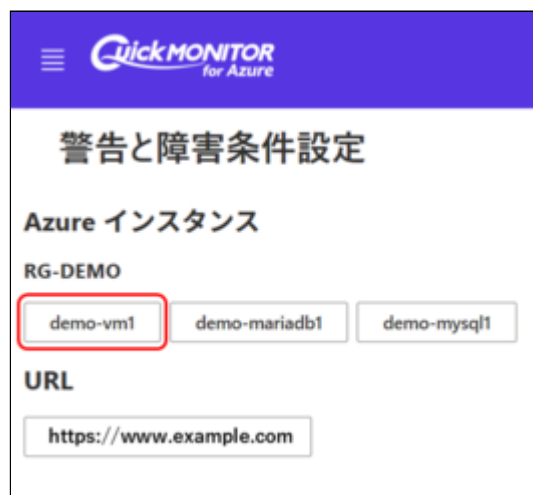
1. 画面左上のメニューアイコンをクリックします。




2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。





4. [NetworkPacketsIn] または、[NetworkPacketsOut] (設定を変更したい方) をクリックします。



警告と障害条件設定

demo-vm1

 Azure API connection	 Instance State (bool)	NetworkPacketsIn
NetworkPacketsOut	CPUUtilization	DiskReadBytes
DiskWriteBytes	DiskReadOps	DiskWriteOps

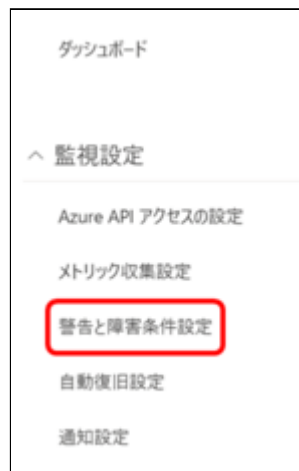
戻る

CPU使用率 (CPUUtilization)

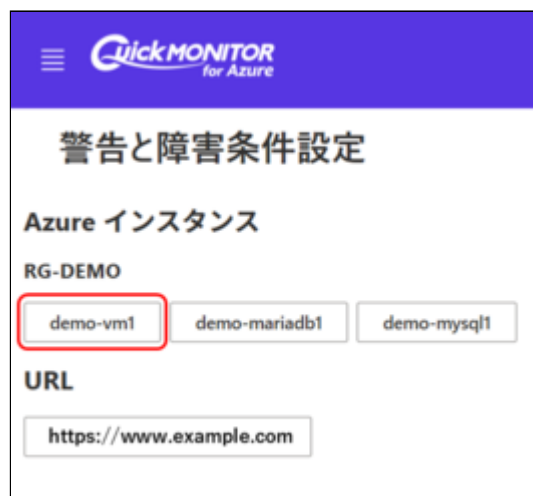
1. 画面左上のメニューアイコンをクリックします。



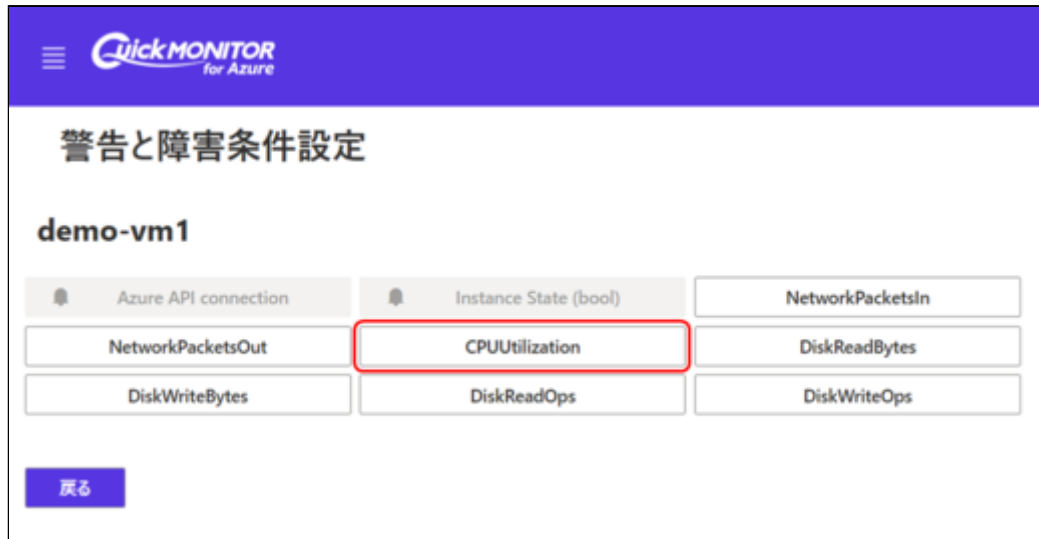
2. [警告と障害条件設定] をクリックします。



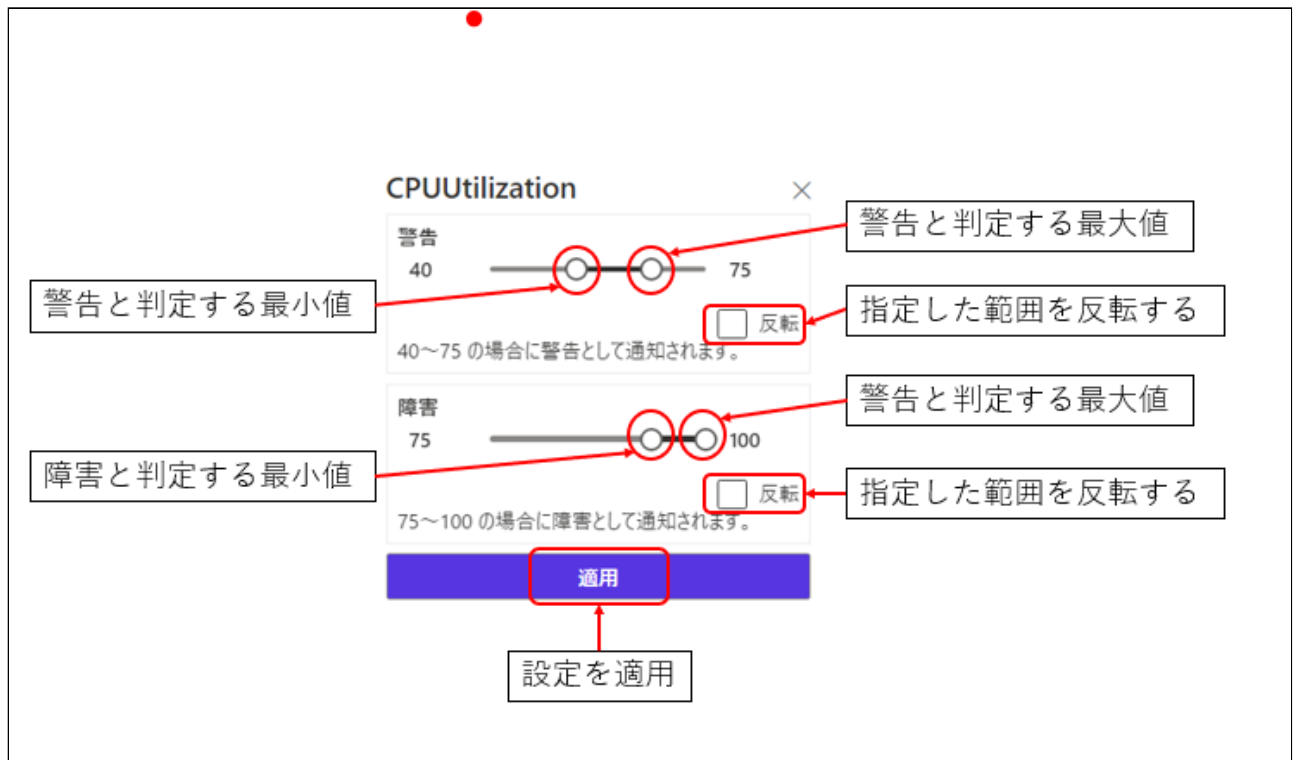
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [CPUUtilization] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

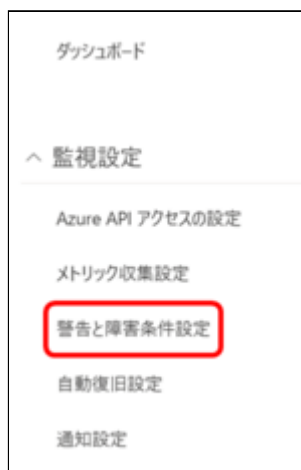


ディスク読み取り/書き込みバイト数 (DiskReadBytes/DiskWriteBytes)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [DiskReadBytes] または、[DiskWriteBytes] (設定を変更したい方) をクリックします。

QuickMONITOR
for Azure

警告と障害条件設定

demo-vm1

Azure API connection	Instance State (bool)	NetworkPacketsIn
NetworkPacketsOut	CPUUtilization	DiskReadBytes
DiskWriteBytes	DiskReadOps	DiskWriteOps

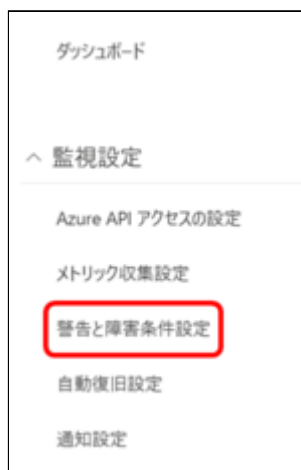
戻る

ディスク読み取り/書き込み回数 (DiskReadOps/DiskWriteOps)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [DiskReadOps] または、[DiskWriteOps] (設定を変更したい方) をクリックします。

QuickMONITOR
for Azure

警告と障害条件設定

demo-vm1

Azure API connection	Instance State (bool)	NetworkPacketsIn
NetworkPacketsOut	CPUUtilization	DiskReadBytes
DiskWriteBytes	DiskReadOps	DiskWriteOps

戻る

5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

DiskReadOps

警告

最小: 25 → 警告と判定する最小値

最大: 50 → 警告と判定する最大値

☐ 反転 → 指定した範囲を反転する

25～50 の場合に警告として通知されます。

障害

最小: 50 → 障害と判定する最小値

最大: 0 → 障害と判定する最大値

☐ 反転 → 指定した範囲を反転する

50 以上の場合に障害として通知されます。

適用 → 設定を適用

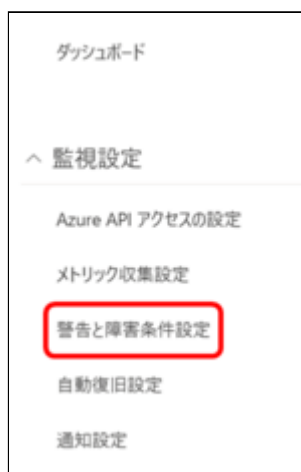
Database

Database のステータス (Database status)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



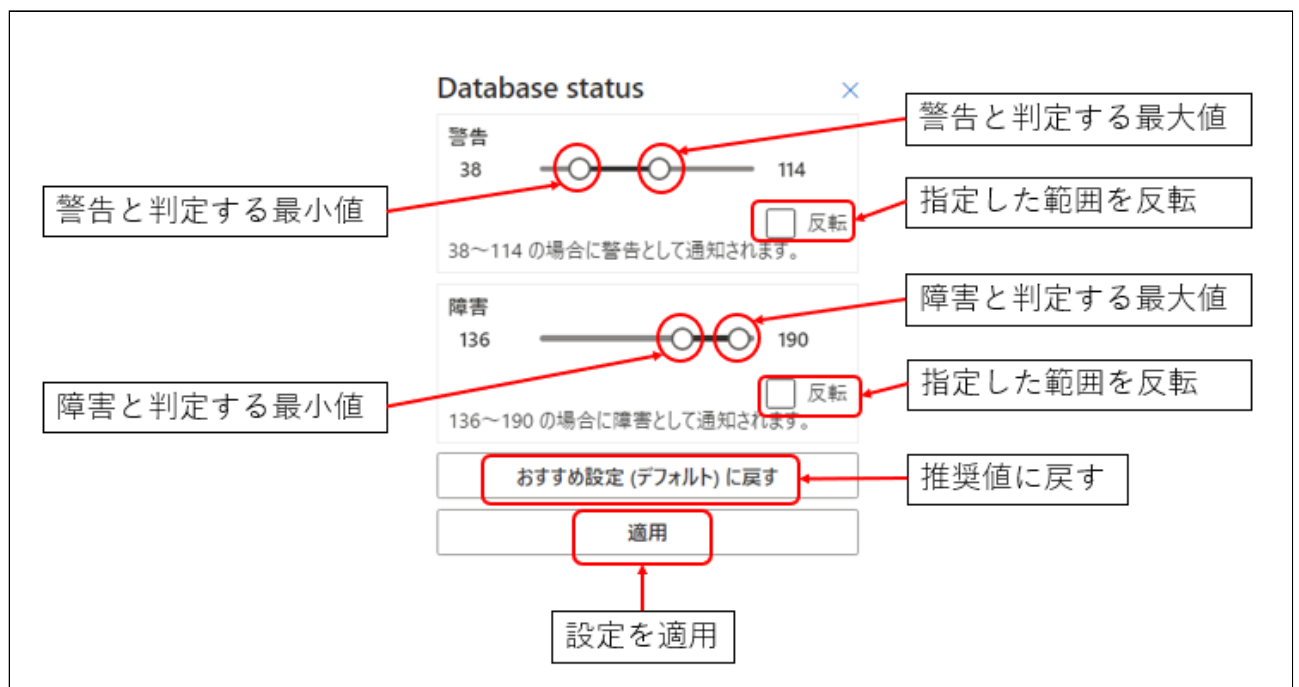
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [Database status] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

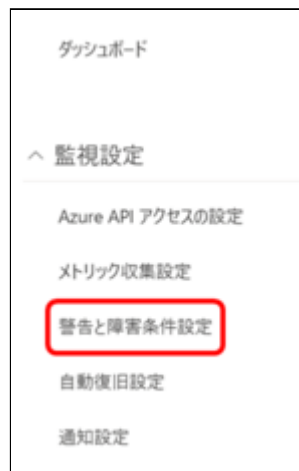


インターネット経由でのアクセス可否 (Publicly Accessible)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



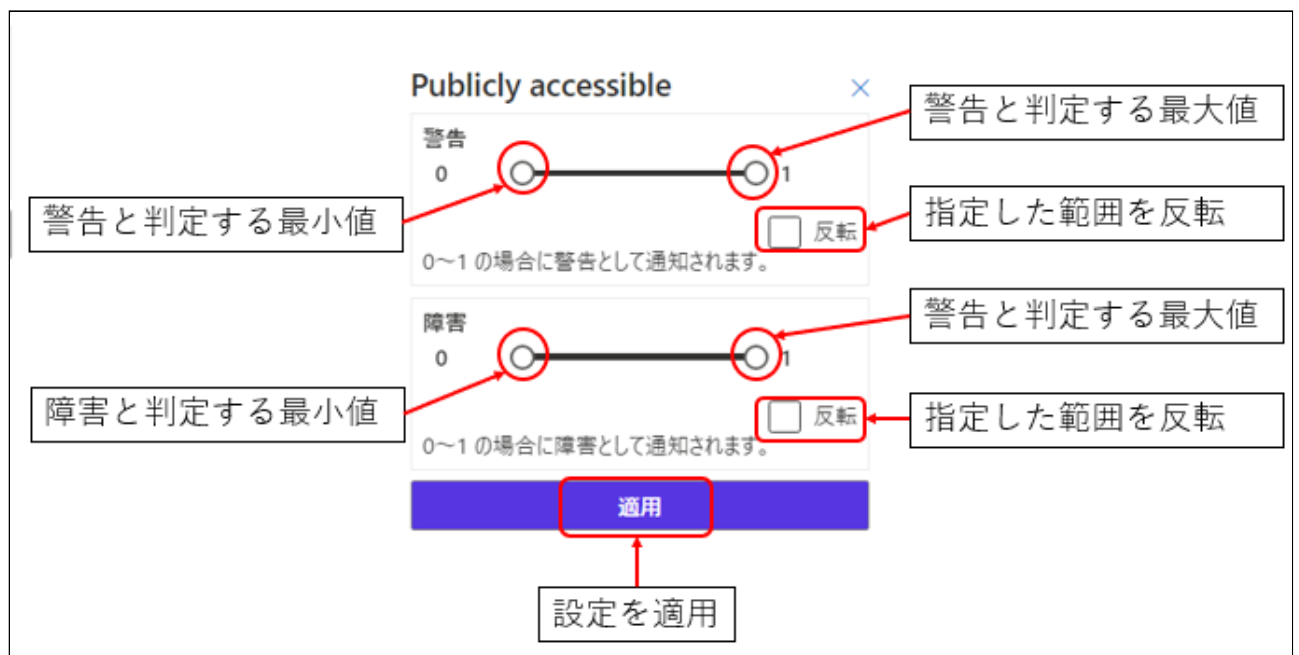
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [Publicly Accessible] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。



クエリ数 (queries)

1. 画面左上のメニューアイコンをクリックします。



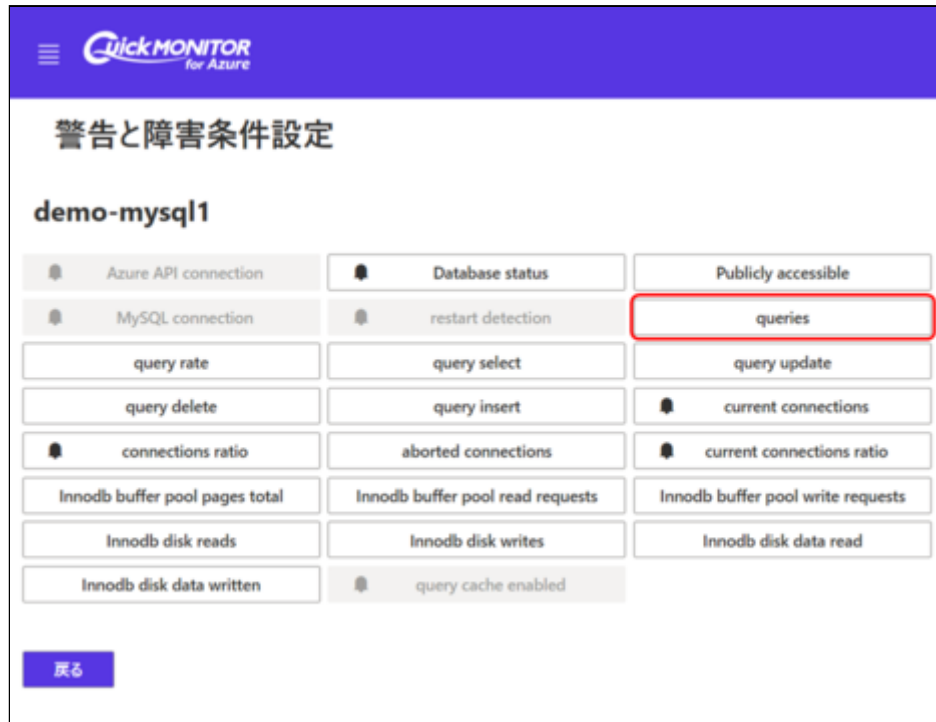
2. [警告と障害条件設定] をクリックします。



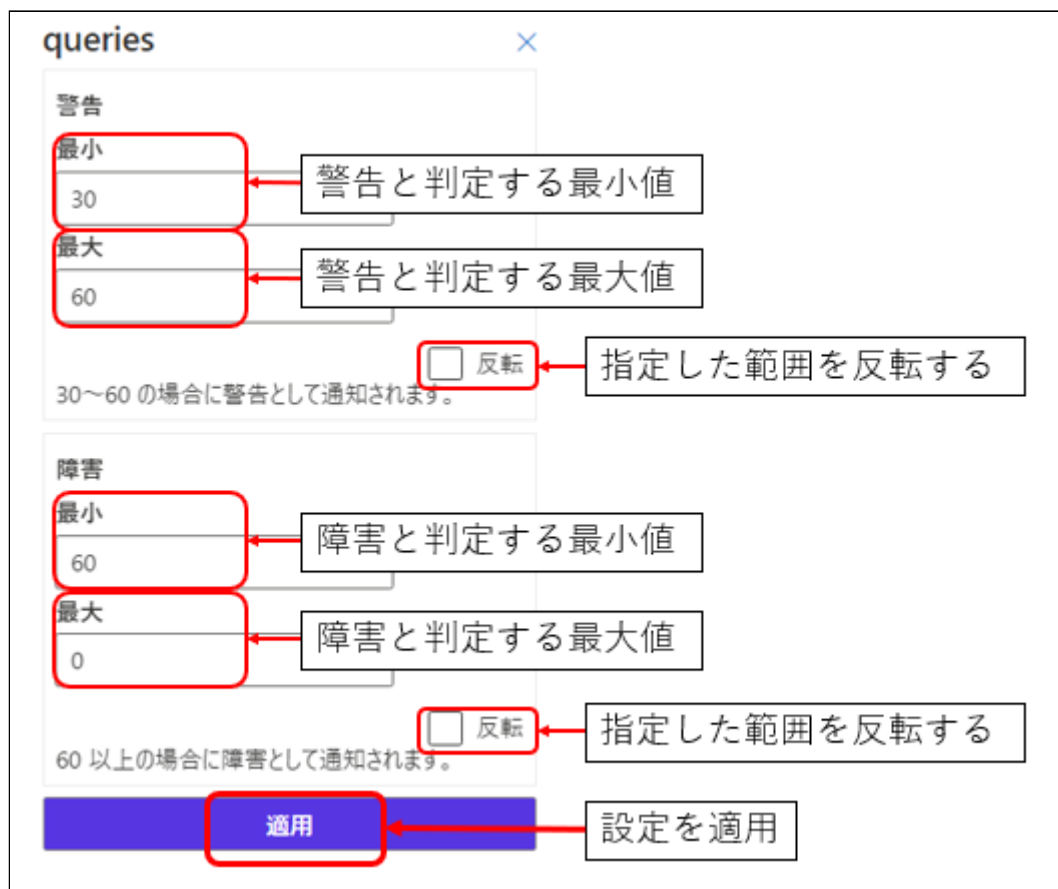
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [queries] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

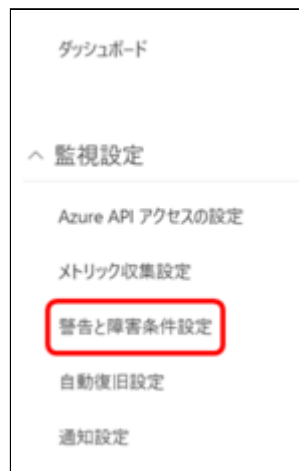


単位時間あたりのクエリ数 (query rate)

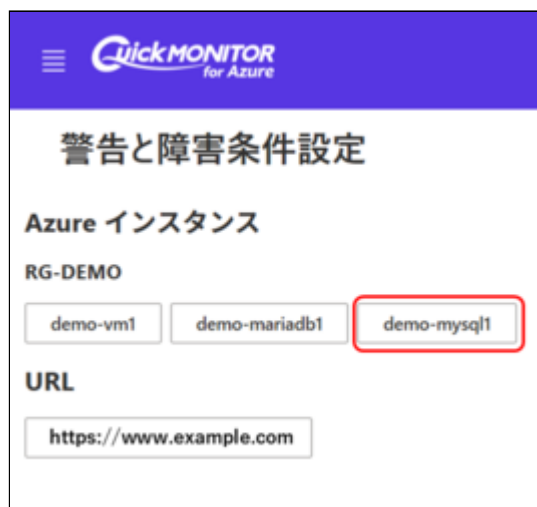
1. 画面左上のメニューアイコンをクリックします。



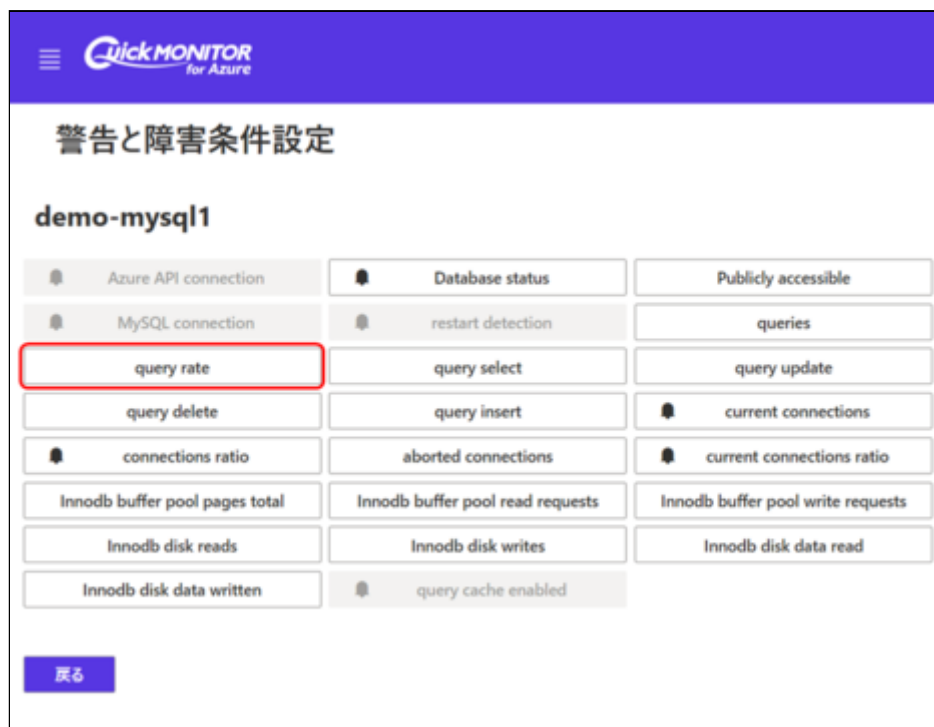
2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [query rate] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

query rate [X]

警告

最小 警告と判定する最小値

最大 警告と判定する最大値

☐ 反転 指定した範囲を反転する

30～50 の場合に警告として通知されます。

障害

最小 障害と判定する最小値

最大 障害と判定する最大値

☐ 反転 指定した範囲を反転する

50 以上の場合に障害として通知されます。

適用 設定を適用

特定のクエリが実行された回数 (query select / query update / query delete / query insert)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



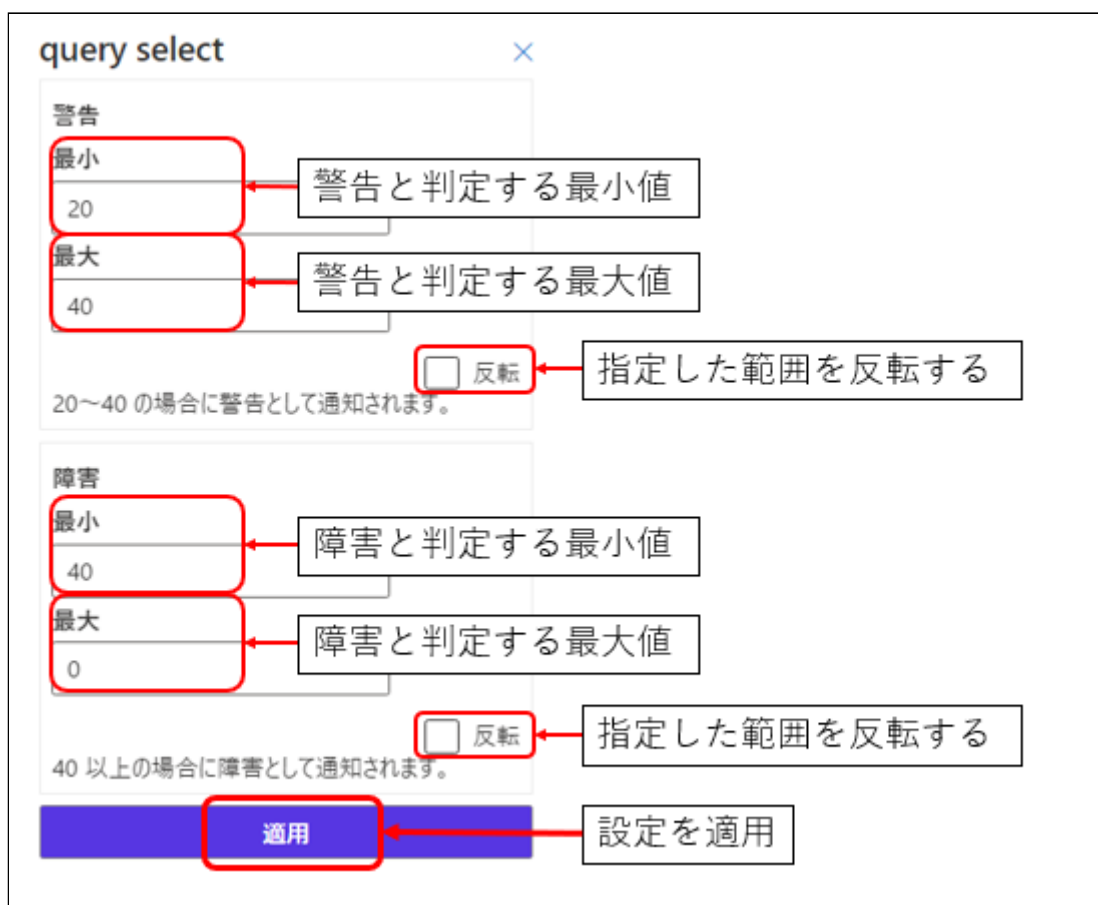
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. 設定を変更したい項目名をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。



現在の接続数 (current connections)

1. 画面左上のメニューアイコンをクリックします。



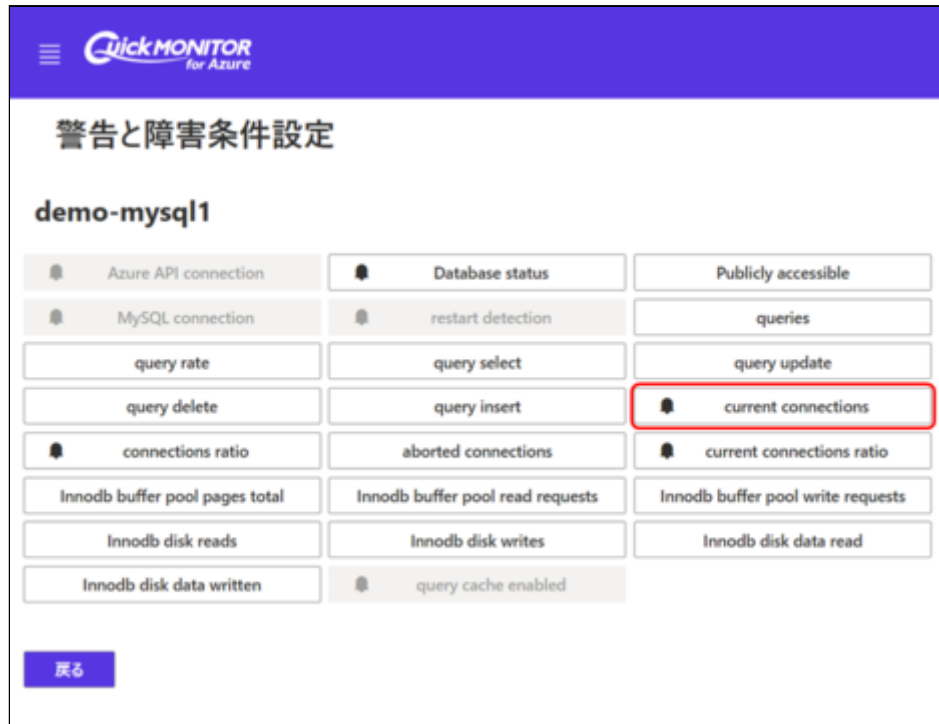
2. [警告と障害条件設定] をクリックします。



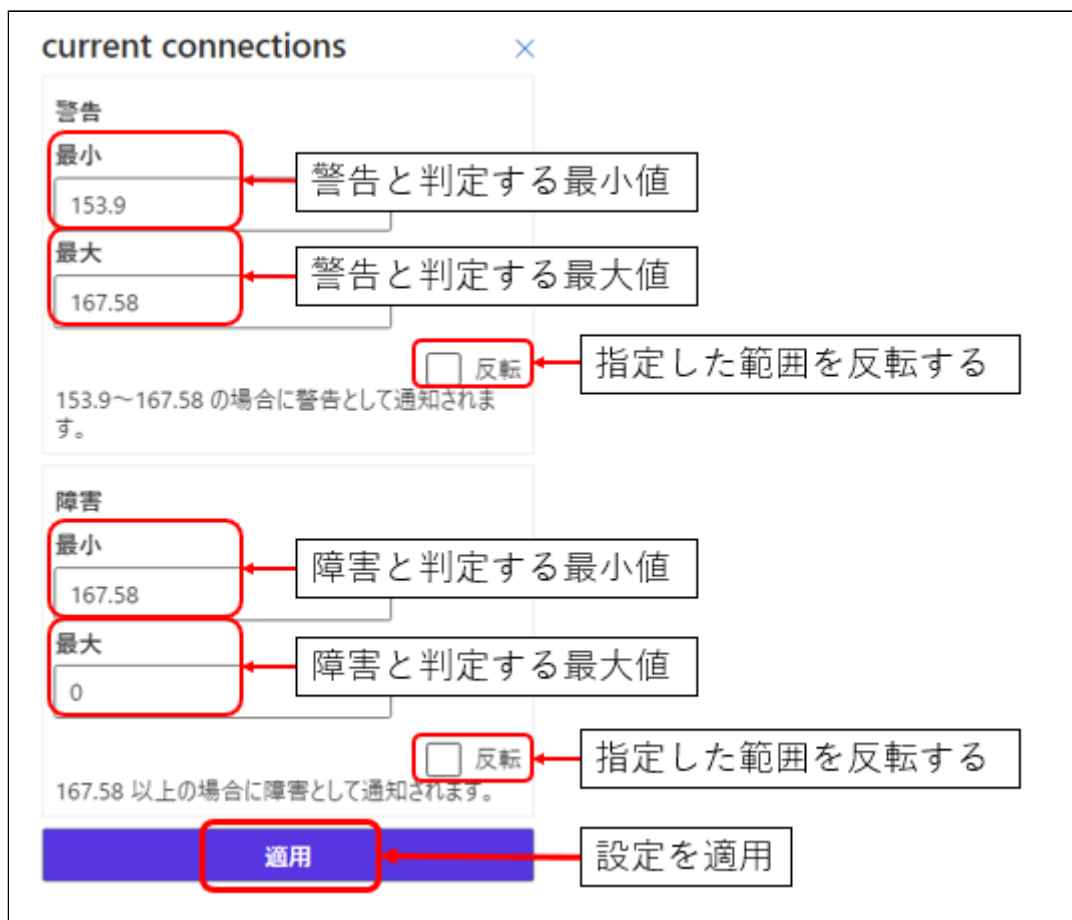
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [current connections] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。



接続占有率 (connections ratio)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



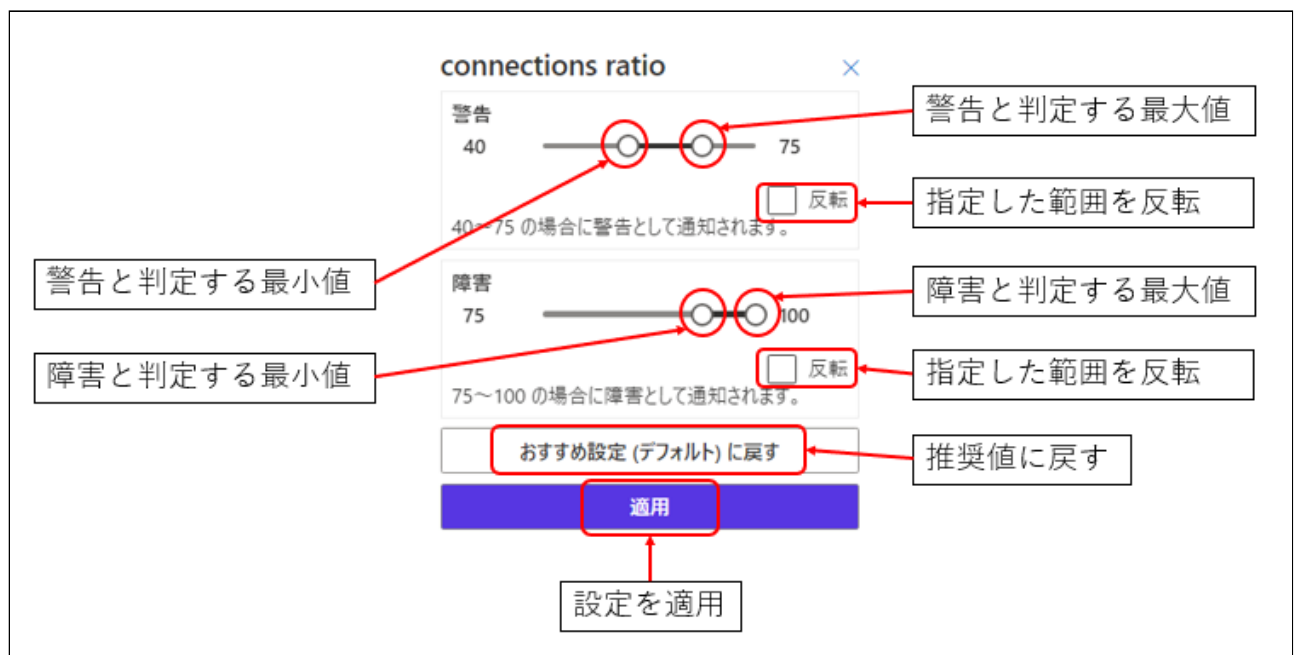
3. 設定を変更した異インスタンス名のボタンをクリックします。



4. [connections ratio] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

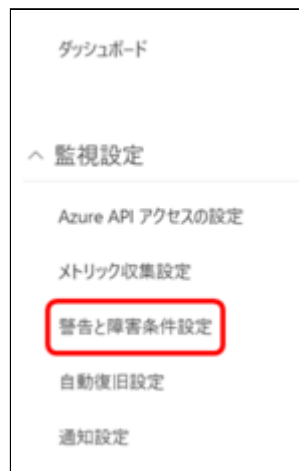


中止された接続の回数 (aborted connections)

1. 画面左上のメニューアイコンをクリックします。



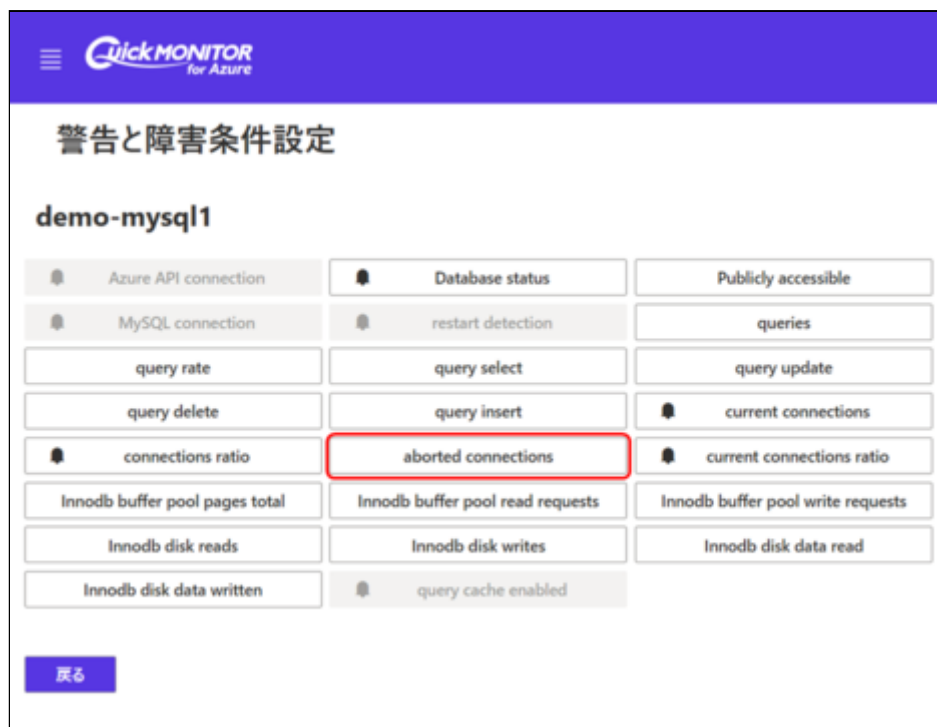
2. [警告と障害条件設定] をクリックします。



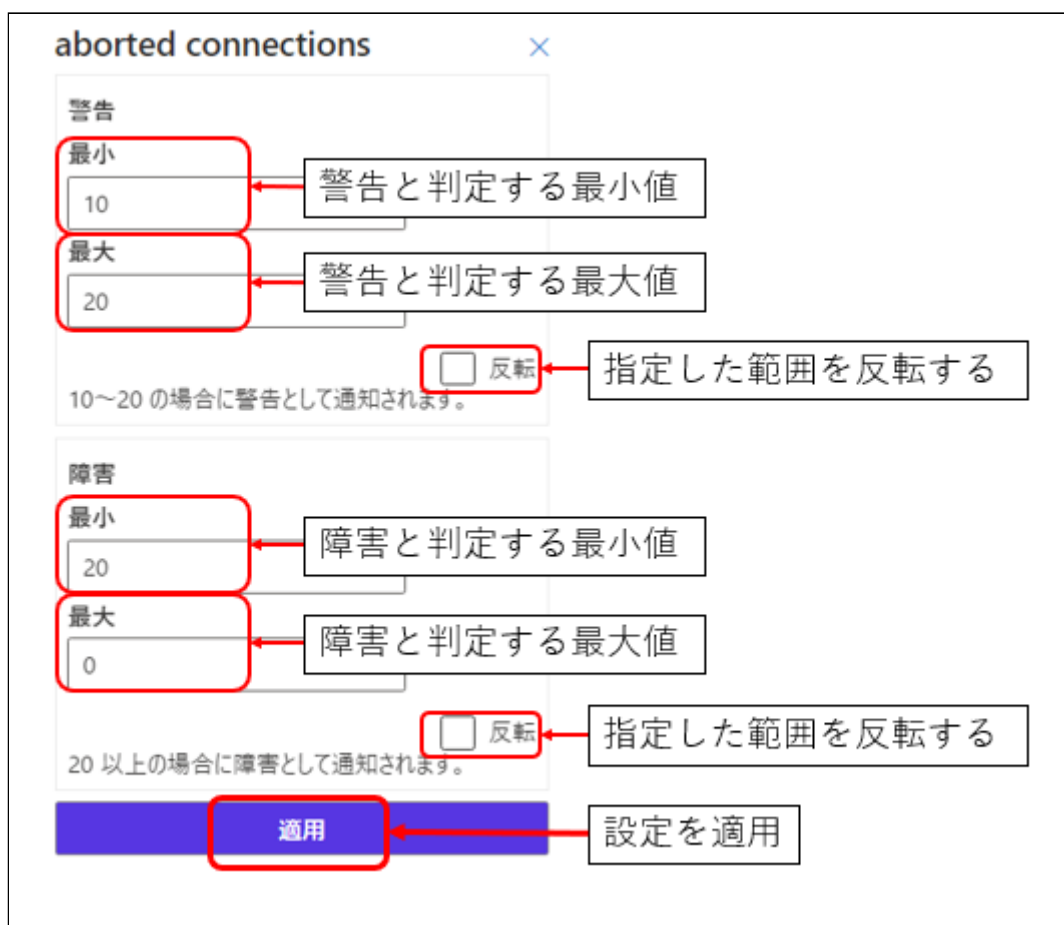
3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [aborted connections] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

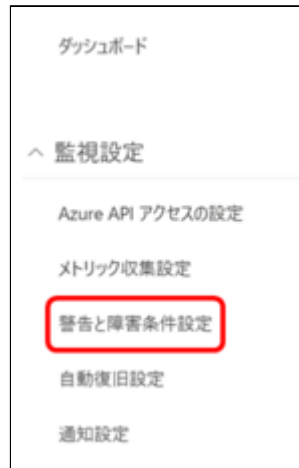


現在の接続占有率 (current connections ratio)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [current connections ratio] をクリックします。



QuickMONITOR
for Azure

警告と障害条件設定

demo-mysql1

 Azure API connection	 Database status	Publicly accessible
 MySQL connection	 restart detection	queries
query rate	query select	query update
query delete	query insert	 current connections
 connections ratio	aborted connections	 current connections ratio
Innodb buffer pool pages total	Innodb buffer pool read requests	Innodb buffer pool write requests
Innodb disk reads	Innodb disk writes	Innodb disk data read
Innodb disk data written	 query cache enabled	

戻る

5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

current connections ratio

警告

最小

85

警告と判定する最小値

最大

0

警告と判定する最大値

☐ 反転

指定した範囲を反転する

85 以上の場合に警告として通知されます。

障害

最小

90

障害と判定する最小値

最大

0

障害と判定する最大値

☐ 反転

指定した範囲を反転する

90 以上の場合に障害として通知されます。

適用

設定を適用

InnoDB バッファプールの合計サイズ (Innodb buffer pool pages total)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [Innodb buffer pool pages total] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

Innodb buffer pool pages total

警告

最小: 10 → 警告と判定する最小値

最大: 20 → 警告と判定する最大値

☐ 反転 → 指定した範囲を反転する

10～20 の場合に警告として通知されます。

障害

最小: 20 → 障害と判定する最小値

最大: 0 → 障害と判定する最大値

☐ 反転 → 指定した範囲を反転する

20 以上の場合に障害として通知されます。

適用 → 設定を適用

InnoDB バッファプールの読み取りリクエスト数、または書き込みリクエスト数 (Innodb buffer pool read requests / Innodb buffer pool write requests)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [Innodb buffer pool read requests] または [Innodb buffer pool write requests] をクリックします。

QuickMONITOR for Azure

警告と障害条件設定

demo-mysql1

Azure API connection	Database status	Publicly accessible
MySQL connection	restart detection	queries
query rate	query select	query update
query delete	query insert	current connections
connections ratio	aborted connections	current connections ratio
Innodb buffer pool pages total	Innodb buffer pool read requests	Innodb buffer pool write requests
Innodb disk reads	Innodb disk writes	Innodb disk data read
Innodb disk data written	query cache enabled	

戻る

5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

Innodb buffer pool read requests

警告

最小: 10 → 警告と判定する最小値

最大: 20 → 警告と判定する最大値

☐ 反転 → 指定した範囲を反転する

10～20 の場合に警告として通知されます。

障害

最小: 20 → 障害と判定する最小値

最大: 0 → 障害と判定する最大値

☐ 反転 → 指定した範囲を反転する

20 以上の場合に障害として通知されます。

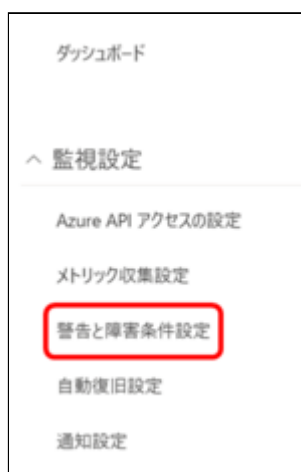
適用 → 設定を適用

データ読み取り、または書き込みの合計数 (Innodb disk reads / Innodb disk writes)

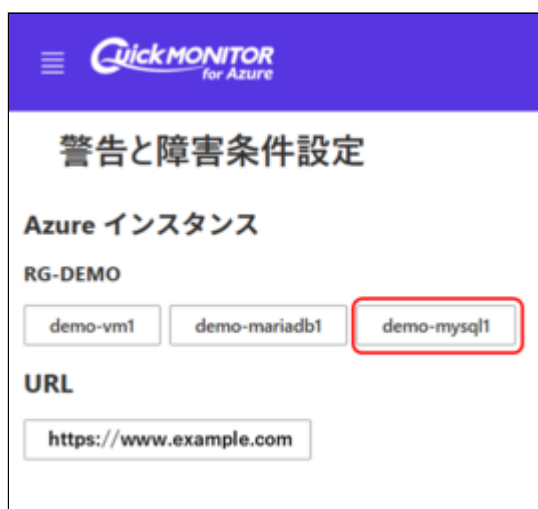
1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [Innodb disk reads] または [Innodb disk writes] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

The screenshot shows the 'InnoDB disk reads' configuration window. It is divided into two main sections: '警告' (Warning) and '障害' (Error). Each section has input fields for '最小' (Minimum) and '最大' (Maximum) values, a checkbox for '反転' (Invert), and a blue '適用' (Apply) button at the bottom.

警告 (Warning) Section:

- 最小 (Minimum):** The value is 10. An annotation points to this field with the text '警告と判定する最小値' (Minimum value for warning determination).
- 最大 (Maximum):** The value is 20. An annotation points to this field with the text '警告と判定する最大値' (Maximum value for warning determination).
- 反転 (Invert):** The checkbox is unchecked. An annotation points to it with the text '指定した範囲を反転する' (Invert the specified range).
- Text below checkbox:** '10～20 の場合に警告として通知されます。' (Notification is sent as a warning when the range is 10 to 20).

障害 (Error) Section:

- 最小 (Minimum):** The value is 20. An annotation points to this field with the text '障害と判定する最小値' (Minimum value for error determination).
- 最大 (Maximum):** The value is 0. An annotation points to this field with the text '障害と判定する最大値' (Maximum value for error determination).
- 反転 (Invert):** The checkbox is unchecked. An annotation points to it with the text '指定した範囲を反転する' (Invert the specified range).
- Text below checkbox:** '20 以上の場合に障害として通知されます。' (Notification is sent as an error when the value is 20 or above).

適用 (Apply) Button: A blue button at the bottom. An annotation points to it with the text '設定を適用' (Apply settings).

これまでに読み取られたデータの量、または書き込まれたデータの量 (Innodb disk data read / Innodb disk data written)

1. 画面左上のメニューアイコンをクリックします。



2. [警告と障害条件設定] をクリックします。



3. 設定を変更したいインスタンス名のボタンをクリックします。



4. [Innodb disk data read] または [Innodb disk data written] をクリックします。

QuickMONITOR for Azure

警告と障害条件設定

demo-mysql1

Azure API connection	Database status	Publicly accessible
MySQL connection	restart detection	queries
query rate	query select	query update
query delete	query insert	current connections
connections ratio	aborted connections	current connections ratio
Innodb buffer pool pages total	Innodb buffer pool read requests	Innodb buffer pool write requests
Innodb disk reads	Innodb disk writes	Innodb disk data read
Innodb disk data written	query cache enabled	

戻る

5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

Innodb disk data read

警告

最小: 10 → 警告と判定する最小値

最大: 20 → 警告と判定する最大値

☐ 反転 → 指定した範囲を反転する

10～20 の場合に警告として通知されます。

障害

最小: 20 → 障害と判定する最小値

最大: 0 → 障害と判定する最大値

☐ 反転 → 指定した範囲を反転する

20 以上の場合に障害として通知されます。

適用 → 設定を適用

URL

HTTP応答コード (HTTP Status Code)

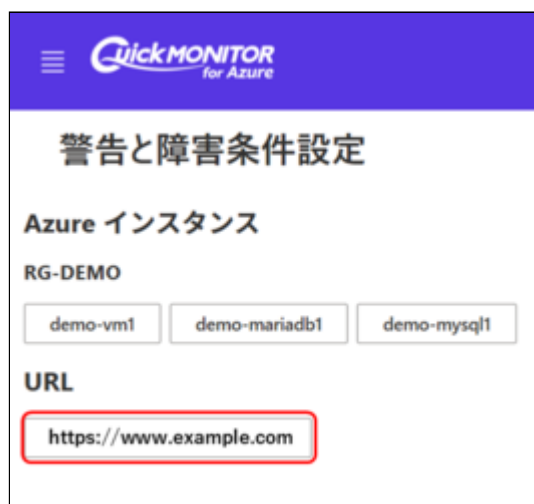
1. 画面左上のメニューアイコンをクリックします。



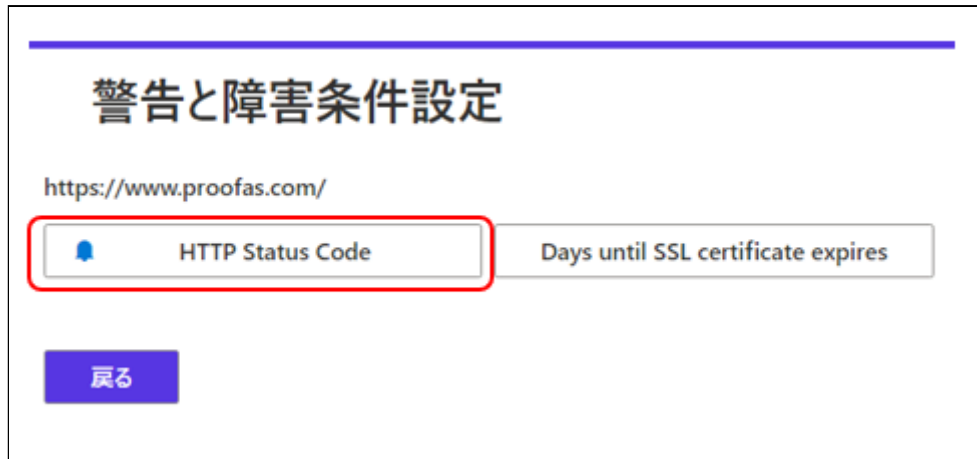
2. [警告と障害条件設定] をクリックします。



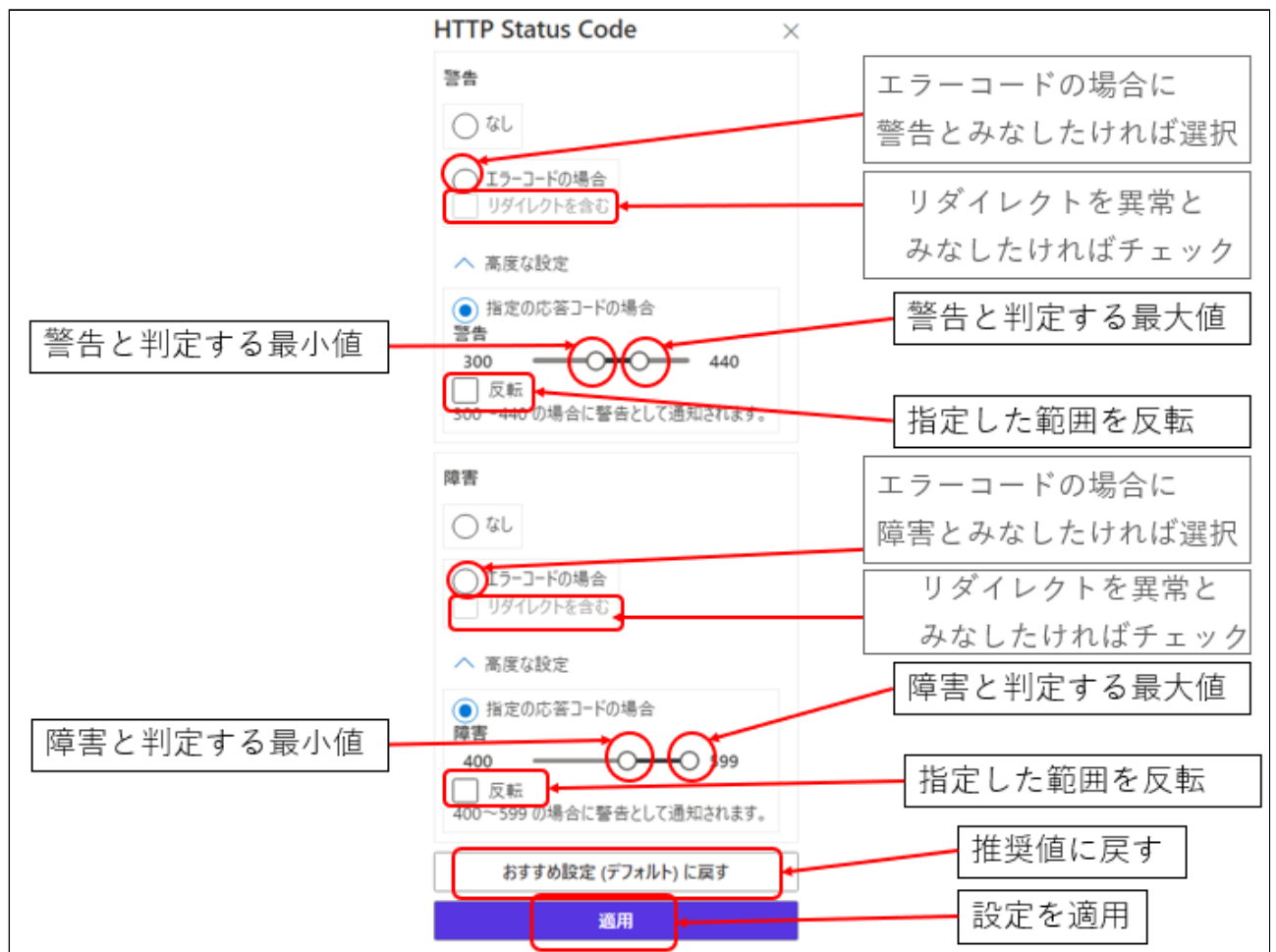
3. 設定を変更したい URL のボタンをクリックします。



4. [HTTP Status Code] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。



SSLサーバー証明書期限までの日数 (Days until SSL certificate expires)

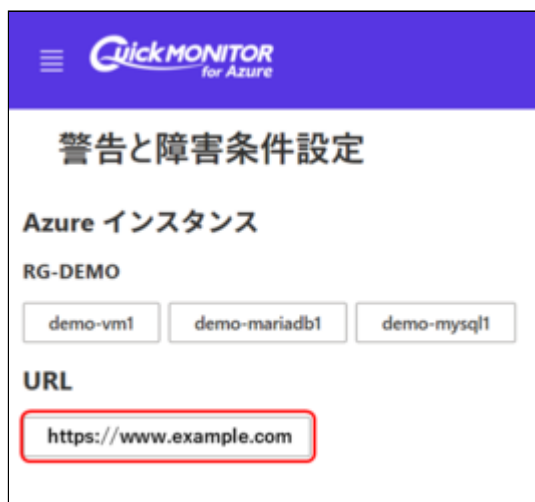
1. 画面左上のメニューアイコンをクリックします。



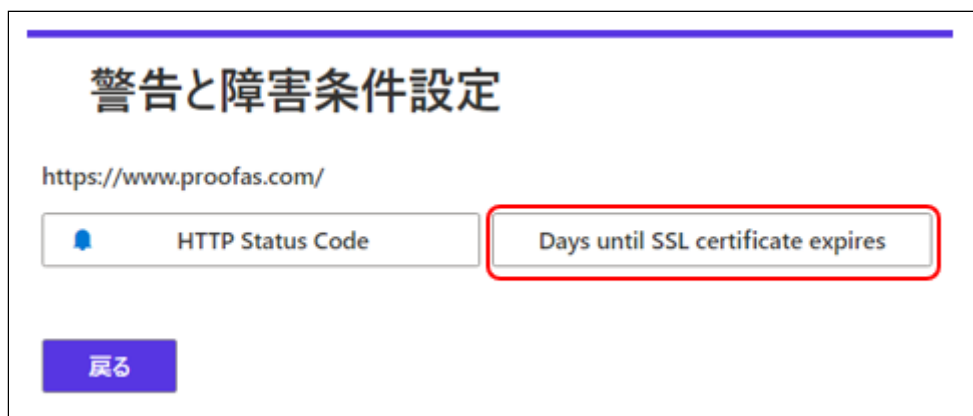
2. [警告と障害条件設定] をクリックします。



3. 設定を変更したい URL のボタンをクリックします。



4. [Days until SSL certificate expires] をクリックします。



5. 警告と障害条件を変更し、[適用] ボタンをクリックします。

×

Days until SSL certificate expires

警告

最小

14

警告と判定する最小値

最大

28

警告と判定する最大値

☐ 反転

指定した範囲を反転する

14～28 の場合に警告として通知されます。

障害

最小

0

障害と判定する最小値

最大

13

障害と判定する最大値

☐ 反転

指定した範囲を反転する

0～13 の場合に障害として通知されます。

適用

設定を適用

共通

監視間隔の変更

1. 画面左上のメニューアイコンをクリック



2. "メトリック収集設定" をクリック



3. 監視間隔を変更したいメトリックをクリック



4. インターバルの選択をする

メトリック収集設定

リージョンとインスタンス
対象インスタンスの上限まで残り: 6
対象インスタンス

R

RG-DEMO/demo-vm1

×

クリックしてインスタンスを追加

R

RG-DEMO/demo-vm4

R

RG-DEMO/demo-vm5

R

RG-DEMO/demo-vm2

R

RG-DEMO/demo-vm3

適用

監視インターバルを選択

インターバル

☐ 1 時間

☐ 30 分

☒ 5 分

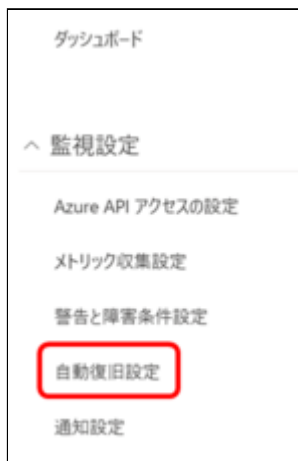
設定を適用

自動復旧設定の変更

1. 画面左上のメニューアイコンをクリックします。



2. "自動復旧の設定をする" をクリック



3. 自動復旧を有効にしたいインスタンスのボタンをクリックして有効化し、[Save] をクリックします。



通知設定の変更

1. 画面左上のメニューアイコンをクリック



2. "通知設定" をクリック



3. [通知方法] をクリックし、通知方法を選択します。

通知方法によって、必要な設定内容が異なります。以下に、通知方法ごとの入力内容についてご案内します。

通知方法「メール」

入力項目

項目	入力内容
宛先	E-Mail アドレスをカンマ区切りで入力します。

入力画面

通知設定

通知方法

メール

宛先

適用

通知方法「Slack」

入力項目

項目	入力内容
Webhook URL	Incoming Webhook URL を入力します。
チャンネル	通知を送りたいチャンネル名を入力します。(例: #channel)

入力画面

通知設定

通知方法

Slack

Webhook URL

チャンネル

適用

通知方法「LINE」

入力項目

項目	入力内容
アクセストークン	LINE Developers で発行したアクセストークンを入力します。

入力画面

通知設定

通知方法

LINE

アクセストークン

適用

通知方法「Chatwork」

入力項目

項目	入力内容
API トークン	Chatwork で発行した API トークンを入力します。
ルーム ID	通知を送りたいルームの ID を入力します。

入力画面

通知設定

通知方法

Chatwork

API トークン

ルーム ID

適用

通知方法「Mattermost」

入力項目

項目	入力内容
Webhook URL	Mattermost で発行した Webhook URL を入力します。
チャンネル	通知を送りたいチャンネル名を入力します。(例: #channel)

入力画面

通知設定

通知方法

Mattermost

Webhook URL

チャンネル

適用

通知方法「Teams (テキスト)」

Webhook URL の具体的な発行方法は本書の「事前準備 - Teams を通知先として利用する場合の準備」をご確認ください。

入力項目

項目	入力内容
Webhook URL	Teams の Workflows アプリで発行した URL を入力します。

入力画面

通知設定

通知方法

Teams (Text) ▼

Webhook URL

適用

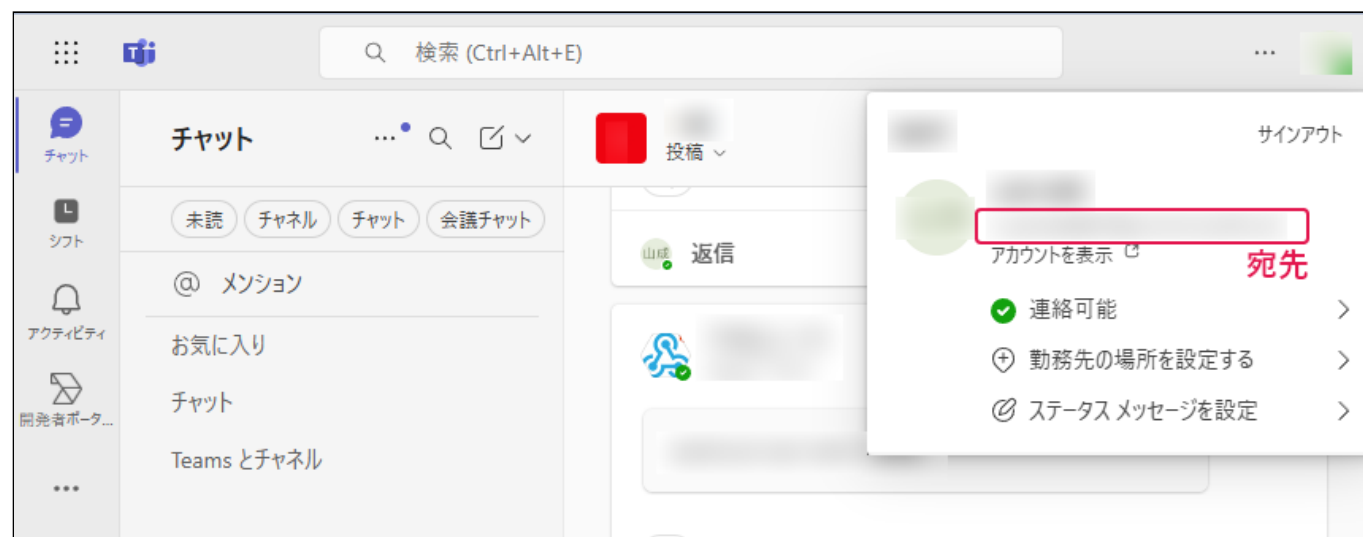
通知方法「Teams (音声)」

クライアントID、クライアントシークレット、テナント ID の具体的な発行方法は本書の「事前準備 - Teams を通知先として利用する場合の準備」をご確認ください。

入力項目

項目	入力内容
宛先	音声通知を送りたい Teams アカウントをカンマ区切りで入力します。(※1)
クライアントID	Teams Developer Portal および Azure Portal で登録・設定したアプリのクライアント ID を入力します。
クライアントシークレット	Teams Developer Portal および Azure Portal で登録・設定したアプリのクライアントシークレットを入力します。
テナント ID	Teams Developer Portal および Azure Portal で登録・設定したアプリのテナント ID を入力します。

※1 宛先として指定できるのは、Teams アカウントを表示したときに以下の部分に表示される情報です。



通知設定

通知方法

Teams (Call) 

宛先

クライアントID

クライアントシークレット

テナント ID

適用

AzureAPIアクセスの設定

AzureAPIアクセスの設定の変更

クライアントID や 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 の確認方法は別冊 [クイックスタート] の「2. Azure API 認証情報の用意」をご確認ください。

1. 画面左上のメニューアイコンをクリック



2. "Azure API アクセスの設定" をクリック




3. クライアントID と 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 を入力して [適用] をクリックします。

Azure API アクセスの設定

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

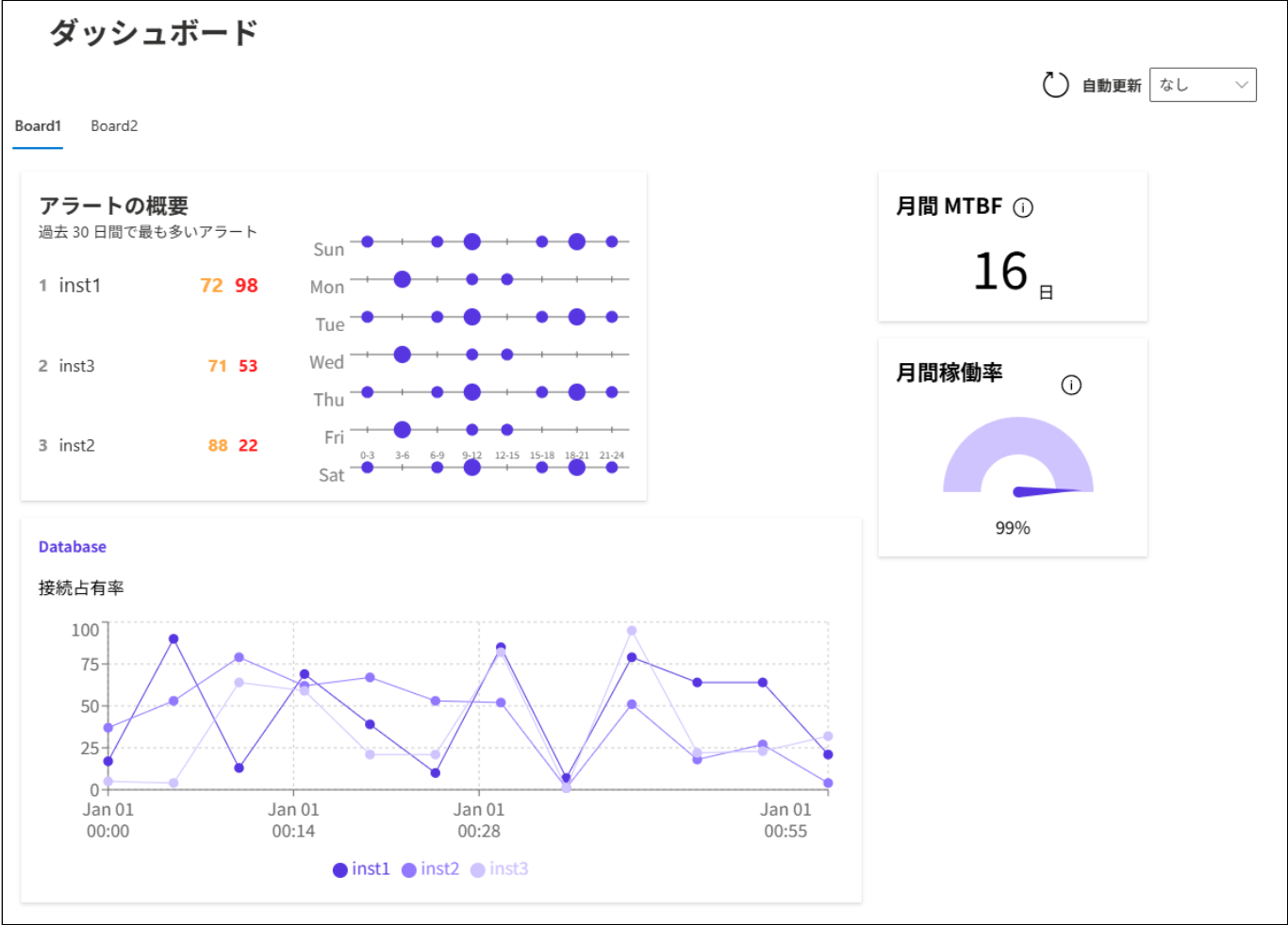
適用

ダッシュボード

Board1 (マネージャー向け)

監視中のシステムについて、稼働状況を俯瞰的に見ることを目的としたダッシュボードです。

ダッシュボードの表示例



アラートの概要

過去 30 日間で、最も警告条件または障害条件を満たした回数が多いインスタンスが上位 3 つまで表示されます。

また、過去 30 日間で何曜日のどの時間帯にアラートが多く発生していたかを示すチャートが表示されます。

月間 MTBF

インスタンスの平均連続稼働時間 (直近30日間) です。

計算式は別冊 [サービス仕様書] をご確認ください。

月間稼働率

インスタンスの稼働時間比率 (直近30日間) です。

計算式は別冊 [サービス仕様書] をご確認ください。

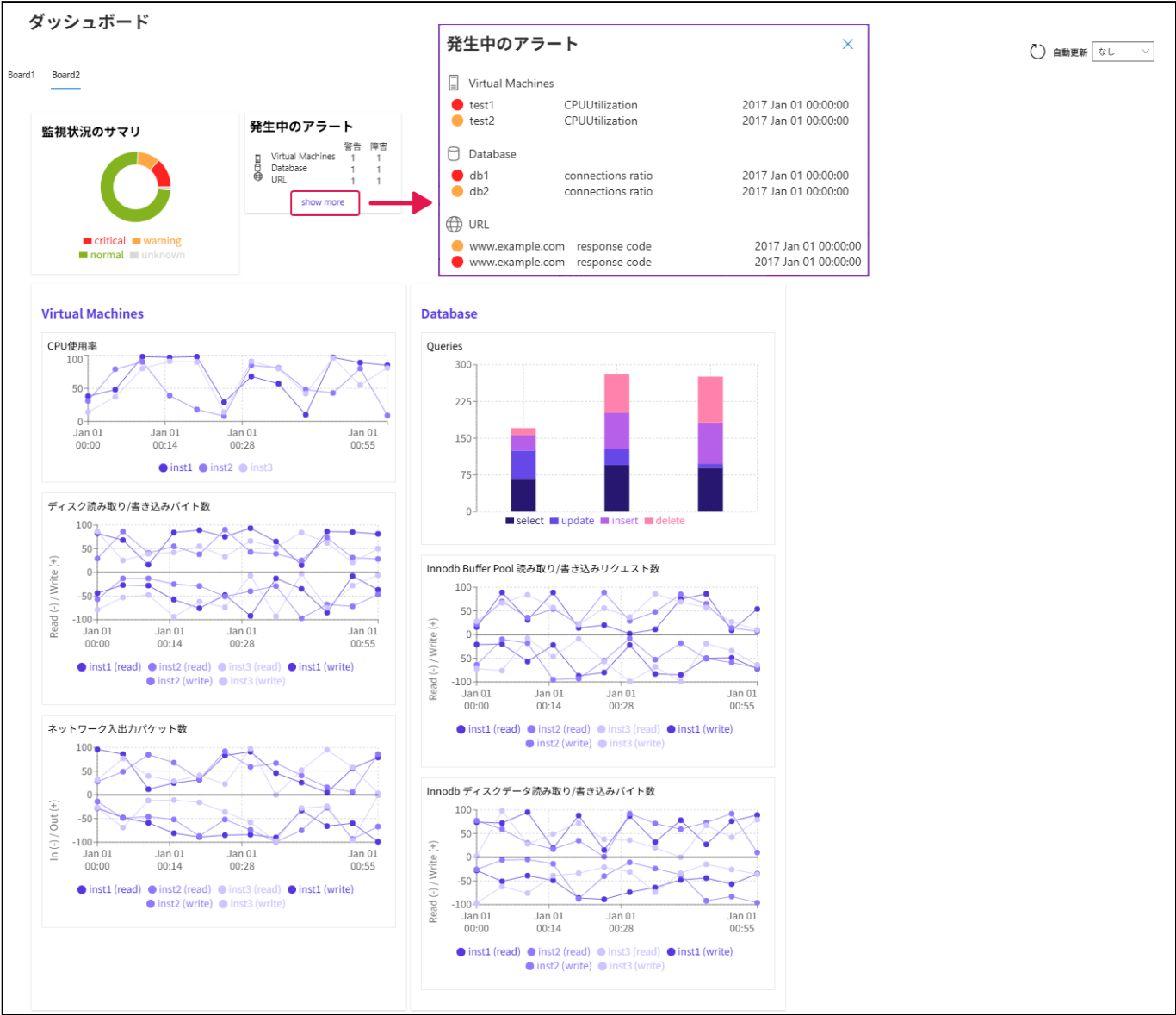
Database の接続占有率

直近 1 時間分の接続占有率の推移をあらわしたグラフです。

Board2 (監視オペレーター向け)

監視中のシステムについて、稼働状況の速報値を見ることを目的としたダッシュボードです。

ダッシュボードの表示例



監視状況のサマリ

現在のアラート状況をあらわした円グラフです。

凡例	説明
critical	障害条件を満たしている項目の数
warning	警告条件を満たしている項目の数
normal	正常な項目の数
unknown	何らかの理由で正常に監視できていない項目の数

発生中のアラート

警告または障害条件を満たしている項目の概要を一覧できます。

例えば、Virtual Machines の test1 インスタンスでは現在 CPUUtilization が警告と障害条件のいずれも満たしている状態、と読みます。

Virtual Machines の CPU使用率

直近1時間分の CPU使用率の推移をあらわしたグラフです。

Virtual Machines のディスク読み取り/書き込みバイト数

直近1時間分のディスク読み取り/書き込みバイト数をあらわしたグラフです。

Virtual Machines のネットワーク入出力パケット数

直近1時間分のネットワーク入出力パケット数をあらわしたグラフです。

Database の Queries

直近1時間分のデータベースに対するクエリ数をクエリの種別ごとにあらわしたグラフです。

Database の Innodb Buffer Pool 読み取り/書き込みリクエスト数

直近1時間分の Innodb Buffer Pool 読み取り/書き込みリクエスト数をあらわしたグラフです。

Database の Innodb デスクデータ読み取り/書き込みバイト数

直近1時間分の Innodb デスクデータ読み取り/書き込みバイト数をあらわしたグラフです。

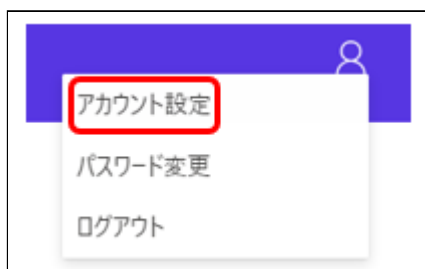
その他

言語の変更

1. 画面右上のメニューアイコンをクリック



2. "アカウント設定" をクリック



3. "言語" のプルダウンメニューから選択する

The screenshot shows the 'アカウント設定' (Account Settings) page. The '言語' (Language) dropdown menu is open, showing options: 日本語 (Japanese), Catalan, English (UK), Español, Français, 日本語 (highlighted with a red box), Русский, and 簡化字. Below the dropdown, the '適用' (Apply) button is highlighted with a red box. A red arrow points from the '適用' button to a box labeled '設定を反映する' (Reflect settings).

アカウント設定

ログインID
user-ja
[パスワード変更](#)

表示名
日本語ユーザー

言語
日本語 ▼
Catalan
English (UK)
Español
Français
日本語
Русский
簡化字

電話番号
0123-456-789

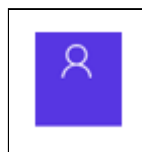
適用

設定を反映する

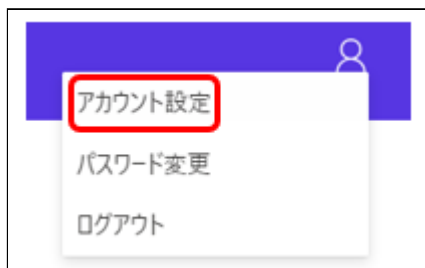
タイムゾーンの変更

タイムゾーンは、ダッシュボードで表示されるグラフなどの日時表示に影響します。

1. 画面右上のメニューアイコンをクリック



2. "アカウント設定" をクリック



3. タイムゾーンを選択し、[適用] をクリックします。

アカウント設定

ログインID
[パスワード変更](#)

表示名

言語

▼

タイムゾーン

Asia/Tokyo ▼

メールアドレス

電話番号

コメント

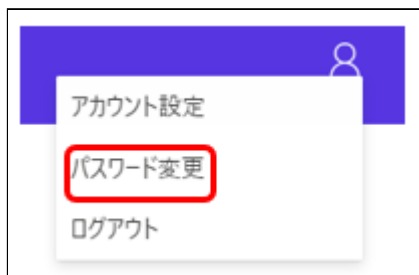
適用

パスワードの変更

1. 画面右上のメニューアイコンをクリック



2. "パスワード変更" をクリック



3. 現在のパスワードと新しいパスワードを記述する

パスワード変更

現在のパスワード

.....

新しいパスワード

.....

適用

設定を反映する

ログアウト

1. 画面右上のメニューアイコンをクリック



2. "ログアウト" をクリック

