演習 - Azure Policy を使用してデプロイを特定の場所に制限する

100 XP

8 分

この演習では、Azure リソースのデプロイを特定の場所に制限するポリシーを Azure Policy で作成します。 ポリシーに違反する場所にストレージ アカウントを作成してみることで、ポリシーを検証します。

Tailwind Traders は、リソースをデプロイできる場所を **米国東部** リージョンに制限したいと考えています。 それには次の 2 つの理由があります。

- **コスト追跡の向上**

  コストを追跡するため、Tailwind Traders では異なるサブスクリプションを使用して、それぞれのリージョンの場所へのデプロイを追跡しています。 このポリシーにより、すべてのリソースが **米国東部** リージョンにデプロイされます。

- **データ所在地とセキュリティ コンプライアンスへの準拠**

  Tailwind Traders は、顧客データを保存できる場所が示されているコンプライアンス規則に従う必要があります。 ここでは、顧客データを **米国東部** リージョンに保存する必要があります。

ポリシーは、管理グループ、単一のサブスクリプション、またはリソース グループに割り当てることができることを思い出してください。 ここでは、ポリシーが Azure サブスクリプション内の他のリソースに影響しないように、リソース グループにポリシーを割り当てます。

> **重要**
>
> このモジュールの演習を完了するには、自分の **Azure サブスクリプション**が必要です。 Azure サブスクリプションを持っていない場合でも、読み進めることはできます。

リソース グループを作成する

ここでは、**my-test-rg** という名前のリソース グループを作成します。 このリソース グループに、場所ポリシーを適用します。

学習が目的なので、前の演習で使用したものと同じリソース グループ名を使用します。 以前のリソース グループを削除したので、同じ名前を使用できます。

1. Azure portal に移動してサインインします。
2. [**リソースの作成**] を選択します。

3. 検索ボックスに「**リソース グループ**」と入力して、 `Enter` キーを押します。
4. 検索結果ペインが表示されたら、結果から [**リソース グループ**] を選択します。
5. **［作成］** を選択します 各設定に対して次の値を入力します。

設定	値
サブスクリプション	*(自分の Azure サブスクリプション)*
サブスクリプション > リソース グループ	**my-test-rg**
リージョン	**(米国) 米国東部**

6. [**確認と作成**] を選択し、次に [**作成**] を選択します。

定義済みのポリシーを調べる

場所のポリシーを構成する前に、定義済みのポリシーをいくつか簡単に見てみましょう。 例として、Azure Compute サービスに関連するポリシーを見てみます。

1. Azure portal のページの上部にある [**ホーム**] を選択して、スタート ページに戻ります。
2. ページの上部にある検索バーに「**ポリシー**」と入力します。 次に、結果の一覧から [**ポリシー**] を選択して Azure Policy にアクセスします。
3. [**作成**] で [**定義**] を選択します。
4. [**カテゴリ**] ドロップダウン リストから、[**コンピューティング**] のみを選択します。

   [**許可されている仮想マシン SKU**] 定義を使用すると、組織でデプロイできる仮想マシン SKU のセットを指定できることに注意してください。

オプションのステップとして、興味のある他のポリシーやカテゴリを調べてください。

場所のポリシーを構成する

ここでは、Azure Policy を使用して許可される場所のポリシーを構成します。 その後、そのポリシーをリソース グループに割り当てます。 そのためには次を行います。

1. **[ポリシー]** ペインの **[作成]** で、**[割り当て]** を選択します。

割り当ては、特定のスコープ内で実行するように割り当てられたポリシーです。 たとえば、サブスクリプションのスコープに定義を割り当てることができます。

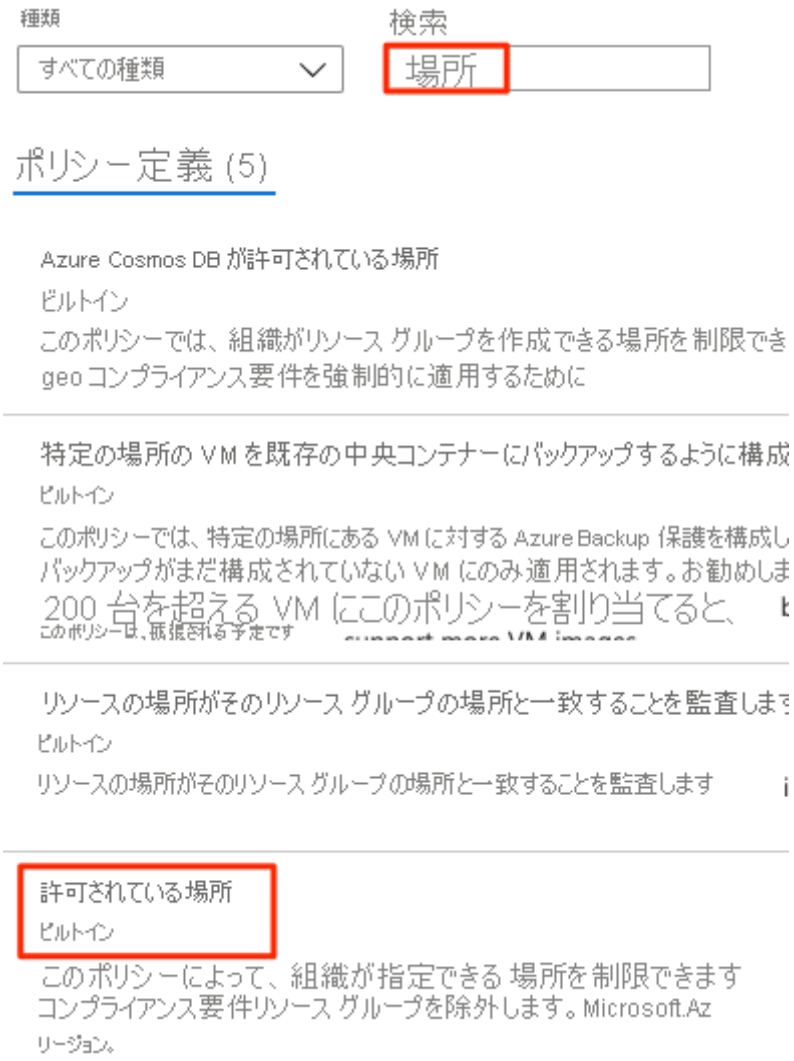
2. **[ポリシーの割り当て]** を選択します。

[ポリシーの割り当て] ペインが表示されます。

3. **[スコープ]** で、省略記号を選択します。

表示されるダイアログ ボックスで、次のように設定します。
   a. **[サブスクリプション]** フィールドにご自分の Azure サブスクリプションを設定します。
   b. **[リソース グループ]** フィールドに **my-test-rg** を設定します。
   c. **[選択]** を選択します。

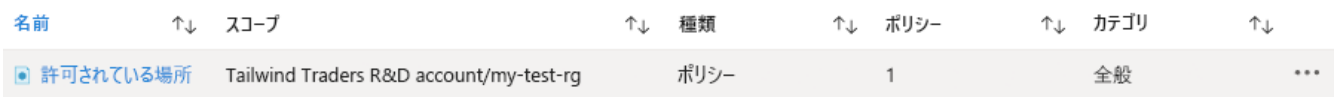
4. **[ポリシー定義]** で、省略記号を選択します。
   a. 検索バーに「場所」と入力します。
   b. **[許可されている場所]** の定義を選択します。
   c. **[選択]** を選択します。



このポリシー定義では、すべてのリソースをデプロイする必要がある場所を指定します。 別の場所を選択すると、デプロイは失敗します。

5. [**次へ**] を選択して、[**パラメーター**] タブに移動します。
6. [**許可されている場所**] ドロップダウン リストから [**米国東部**] を選択します。
7. [**確認と作成**] を選択し、次に [**作成**] を選択します。

[**許可されている場所**] ポリシー割り当てが、[**ポリシーの割り当て**] ペインの一覧に表示されます。 これにより、**my-test-rg** リソース グループに対してポリシーが適用されます。



場所のポリシーを確認する

ここでは、場所のポリシーに違反している場所にあるストレージ アカウントをリソース グループに追加してみます。

1. Azure portal のページの上部にある [**ホーム**] を選択して、スタート ページに戻ります。

2. [**リソースの作成**] を選択します。

3. 検索ボックスに「**ストレージ アカウント**」と入力して、 `Enter` キーを押します。

4. 検索結果ペインが表示されたら、結果から [**ストレージ アカウント**] を選択します。

5. **［作成］** を選択します 各設定に対して次の値を入力します。

   注意

   NNN は一連の数字に置き換えます。 この数字は、ストレージ アカウント名を確実に一意にするのに役立ちます。

設定	値
サブスクリプション	*(自分の Azure サブスクリプション)*
サブスクリプション > **リソース グループ**	**my-test-rg**
Storage account name (**ストレージ アカウント名**)	**mysaNNN**
場所	**(アジア太平洋) 東日本**
パフォーマンス	**Standard**
アカウントの種類	**StorageV2 (汎用 v2)**
レプリケーション	**ローカル冗長ストレージ (LRS)**
アクセス層 (既定)	**ホット**

   前に場所のポリシーで [**東日本**] を選択した場合は、一覧から別のリージョンを選択します。

6. [**確認と作成**] を選択し、次に [**作成**] を選択します。

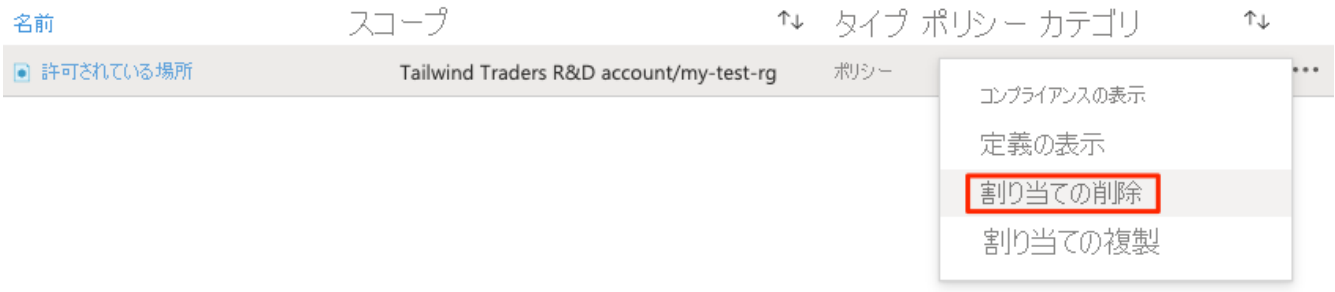
   ポリシー違反のためにデプロイが失敗したことを示すメッセージが表示されます。 デプロイの詳細も表示されます。

   mysa1234 という名前のストレージ アカウントに対して表示されるデプロイの詳細の例を次に示します。

ポリシーの割り当てを削除する

ポリシーの割り当てが不要になりました。 ここでは、サブスクリプションからそれを削除します。

1. Azure portal から、**[ホーム]** > **[ポリシー]** を選択します。
2. **[作成]** で **[割り当て]** を選択します。
3. **[許可されている場所]** の行で、省略記号を選択します。 次に、**[割り当ての削除]** を選択します。 メッセージが表示されたら **[はい]** を選択します。



[許可されている場所] ポリシー割り当てが存在しなくなったことがわかります。

オプションのステップとして、ストレージ アカウントをもう一度作成し、ポリシーが無効になっていることを確認できます。

リソース グループを削除します

リソース グループが不要になりました。 ここでは、サブスクリプションからそれを削除します。

1. Azure portal から、**[ホーム]** > **[リソース グループ]** > **my-test-rg** を選択して、リソース グループにアクセスします。
2. **[概要]** を選択し、**[リソース グループの削除]** を選択します。
3. プロンプトで「**my-test-rg**」と入力し、**[OK]** を選択します。

   削除操作が完了するまでにしばらくかかる場合があります。
4. 操作が完了したら、**[ホーム]** > **[リソース グループ]** を選択します。

my-test-rg リソース グループがアカウントに存在しなくなったことがわかります。

上出来 Azure Policy を使用してポリシーを適用し、Azure リソースのデプロイを特定の場所に制限することができました。 これで、管理グループ、サブスクリプション、またはリソース グループのレベルで必要なポリシーを適用できます。